



Junos Space

Junos Space Network Application Platform User Guide

Release

11.4



Published: 2014-05-26

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2014, 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 Application Platform User Guide

11.4

Copyright © 2014, 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	xxvii
	Documentation and Release Notes	xxvii
	Documentation Conventions	xxvii
	Documentation Feedback	xxix
	Requesting Technical Support	xxx
	Self-Help Online Tools and Resources	xxx
	Opening a Case with JTAC	xxx
Part 1	Junos Space User Interface	
Chapter 1	Getting Started	3
	Logging In to Junos Space	3
	Changing User Passwords	4
	Using the Getting Started Assistants	5
	Accessing Help	6
	Logging Out of the Junos Space System	6
Chapter 2	Understanding the Junos Space User Interface	9
	Application Chooser Overview	9
	Parts of the Application Chooser	9
	Application Icons	9
	Shortcut Icons	10
	Login User Name	11
	Application Chooser Actions	11
	Junos Space User Interface Overview	11
	Parts of the System User Interface	12
	Banner	12
	Application Chooser	13
	Application Dashboard	13
	Workspace Statistics	14
	Inventory Page	14
	Navigating the Junos Space User Interface	16
	Navigating Applications Using the Application Chooser	16
	Navigating Applications Using the Application Switcher	16
	Navigating Application Workspaces and Tasks Using the Navigation Ribbon	17
	Navigating to the Dashboard of an Application	18
	Navigating to a Workspace from a Task	18
	Network Application Platform Overview	18

	Platform Dashboard Overview	19
	Parts of Platform Dashboard	20
	Workspace Navigation Ribbon	20
	Dashboard Gadgets	21
	Viewing Dashboard Statistics	23
	Viewing System Health Statistics	23
	Viewing the Job Information	25
	Workspace Statistics Pages Overview	26
	Inventory Pages Overview	28
	Parts of the Inventory Page	29
	View Controls	31
	Sorted By Indicator	32
	Show or Hide Columns	32
	Zoom Slider	32
	Search and Filter Field	33
	Actions Drawer	33
	Paging Controls	34
Part 2	Devices	
Chapter 3	Discovering Devices	39
	Device Discovery Overview	39
	Discovering Devices	40
	Specifying Device Targets	41
	Specifying Probes	43
	Specifying Credentials	45
	Specifying Device Targets	48
	Specifying SNMP Probes	49
Chapter 4	Adding Deployed Devices	51
	Add Deployed Devices Wizard Overview	51
	Adding Deployed Devices	52
	Managing Deployed Devices	54
	Viewing the Details of a Task Instance	55
	Viewing the Device Status	55
	Deleting a Task Instance	55
	Downloading Management CLI Commands	55
Chapter 5	Device Management Overview	57
	Device Management Overview	57
	Viewing Device Statistics	58
	Viewing the Number of Devices by Platform	59
	Viewing Connection Status for Devices	59
	Viewing Devices by Junos OS Release	60
	Device Inventory Management Overview	62

Chapter 6	Managing Devices	63
	Viewing Managed Devices	63
	Viewing Devices as Graphics	64
	Viewing Devices in a Table	65
	Editing Device Configuration Overview	68
	Selecting the Device and the Configuration Perspective	69
	Editing Device Configuration Options	70
	Finalizing Device Configuration Changes	72
	Viewing Change Requests	74
	Viewing Change Requests	74
	Adding, Modifying, or Deleting a Change Request	75
	Viewing Hardware Inventory for Devices	75
	Viewing Physical Interfaces for Devices	78
	Deleting Devices	79
	Resynchronizing Managed Devices	80
	Changing Login Credentials for Managed Devices	82
	Displaying Service Contract and EOL Data in the Physical Inventory Table	84
	Exporting Device Inventory Information	87
	Viewing and Exporting Device License Inventory	91
	Troubleshooting Devices	94
	Understanding How Junos Space Automatically Resynchronizes Managed Devices	96
Chapter 7	Adding Devices and Connection Profiles	99
	Add Devices Overview	99
	Adding Devices	101
	Creating a Deployment Instance	102
	Adding a Deployment Instance by Importing a CSV File	103
	Adding a Deployment Instance Manually	104
	Working with Rows and Columns	105
	Working with Configlets	107
	Deploying Device Instances	108
	Viewing the Details of a Deployment Instance	108
	Viewing the Device Status	108
	Deleting a Deployment Instance	109
	Downloading Configlets	109
	Searching for a Deployment Instance	110
	Connection Profiles Overview	111
	Creating Connection Profiles	113
	Managing Connection Profiles	116
	Viewing the Details of a Connection Profile	117
	Modifying a Connection Profile	118
	Deleting a Connection Profile	118
	Copying a Connection Profile	119
	Searching for a Connection Profile	119

Chapter 8	Secure Console	121
	Connecting to a Device	121
	Secure Console Overview	121
	Connecting to a Device From Secure Console	121
	Connecting to a Managed Device	122
	Connecting to an Unmanaged Device	123
	Configuring SRX Device Clusters in Junos Space	126
	Configuring a Standalone Device from a Single-node Cluster	126
	Configuring a Standalone Device from a Two-Node Cluster	128
	Configuring a Primary Peer in a Cluster from a Standalone Device . . .	129
	Configuring a Secondary Peer in a Cluster from a Standalone Device	130
Chapter 9	Device Adapters	133
	Installation/Management	133
	Screen OS Software Adapter Overview	133
	Installing the ScreenOS Software Adapter for Managing Non-DMI Security Devices	134
	Uploading the SOS Adapter Image	134
	Installing the ScreenOS Adapter	134
	Verifying the SOS Adapter Installation	135
	Adding Screen OS Devices to Junos Space	136
	Uploading the Device Management Commands	139
	Deleting a ScreenOS Adapter	140
	Worldwide Junos OS Adapter Overview	140
	Installing the Worldwide Junos OS Adapter	141
	Installing the wwadapter Image	141
	Connecting to ww Junos OS Devices	143
Chapter 10	Discovering Topologies	145
	Topology Discovery Overview	145
	Discovering a Topology	148
	Managing Device Targets	149
	Managing SNMP Probes	151
Part 3	Device Templates	
Chapter 11	Overview	157
	Device Templates Overview	158
	Device Templates Workflow Overview	159
Chapter 12	Device Template Definitions	161
	Managing Device Template Definitions Overview	162
	Importing Device Template Definitions Overview	162
	Device Template Definition Workflow	163
	Creating a Device Template Definition Overview	164
	Junos OS Configuration Hierarchy Reference	164
	Defining the Operator's View	167
	Selecting the Device Family and Naming a Device Template Definition	169

	Creating Configuration Pages for a Device Template Definition	170
	Finding Configuration Options	174
	Filling in the General Tab	176
	Filling in the Description Tab	178
	Defining the Content the Operator Enters	179
	Filling in the Validation Tab	181
	Composing Error Messages	184
	Filling in the Advanced Tab	185
	Using Rules Overview	186
	Managing CSV Files	187
	Working with Rules	188
	Specifying Device-Specific Data in Definitions	190
	Specifying Default Values for Configuration Options	194
	Publishing and Unpublishing a Device Template Definition	196
	Modifying a Device Template Definition	197
	Cloning a Device Template Definition	198
	Deleting a Device Template Definition	199
	Importing a Device Template Definition	200
	Exporting a Device Template Definition	201
Chapter 13	Device Templates	203
	Managing Device Templates Overview	203
	Template States	203
	Filtering and Searching Templates	204
	Device Template Detailed Information	204
	Template Actions	205
	Creating a Device Template Overview	206
	Creating a Device Template	206
	Selecting a Device Template Definition	207
	Naming and Describing a Device Template	207
	Entering Data and Finishing the Device Template	208
	Deploying the Device Template	209
	Deploying a Device Template	209
	Modifying a Device Template	210
	Deleting a Device Template	211
	Viewing Device Template Inventory	212
	Viewing Device Template Statistics	212
Chapter 14	Troubleshooting	215
	Changing Device Template Definition States	215
	User Privileges in Device Templates	215
Part 4	Device Images and Scripts	
Chapter 15	Overview	219
	Device Images and Scripts Overview	219
	User Roles	220
Chapter 16	Device Images	223
	Device Images Overview	223

Chapter 17	Scripts	225
	Scripts Overview	225
Chapter 18	Operations	229
	Operations Overview	229
Chapter 19	Script Bundles	231
	Script Bundles Overview	231
Chapter 20	Configuration: Device Images	233
	Uploading Device Images to Junos Space	233
	Staging Device Images	234
	Verifying the Checksum	235
	Viewing and Deleting MD5 Validation Results	236
	Viewing the MD5 Validation Results	236
	Deleting the MD5 Validation Results	237
	Deploying Device Images	238
	Viewing Device Image Deployment Results	243
	Deleting Device Images	243
	Modifying Device Image Details	244
Chapter 21	Configuration: Scripts	247
	Importing a Script	247
	Modifying a Script	248
	Modifying Script Types	249
	Comparing Script Versions	250
	Deleting Scripts	251
	Deploying Scripts on Devices	252
	Verifying the Checksum of Scripts on Devices	253
	Enabling Scripts on Devices	255
	Removing Scripts from Devices	256
	Executing Scripts on Devices	257
Chapter 22	Configuration: Operations	259
	Creating an Operation	259
	Modifying an Operation	262
	Running an Operation	263
	Copying an Operation	264
	Deleting an Operation	265
Chapter 23	Configuration: Script Bundles	267
	Creating a Script Bundle	267
	Modifying a Script Bundle	268
	Deleting Script Bundles	270
	Deploying Script Bundles on Devices	270
	Executing Script Bundles on Devices	271
Chapter 24	Administration: Scripts	275
	Viewing Script Details	275
	Viewing Verification Results	277
	Exporting Scripts in Tar Format	278

Chapter 25	Administration: Operations	279
	Viewing Operations Results	279
Part 5	Network Monitoring	
Chapter 26	Network Monitoring UI	283
	Network Monitoring Workspace	283
	Network Monitoring Workspace Overview	284
	Network Monitoring Reports Overview	286
	Resource Graphs	286
	Key SNMP Customized (KSC) Performance Reports, Node Reports, and Domain Reports	286
	Database Reports	286
	Statistics Reports	286
	Viewing the Node List	287
	Resyncing Nodes	288
	Searching in the Network Monitoring Workspace	288
	Tracking and Searching for Assets	289
	Viewing and Tracking Outages	290
	Viewing, Querying, and Acknowledging Events	291
	Events Landing Page	291
	Advanced Event Search	292
	Viewing the Events List	292
	Viewing Event Details	293
	Viewing and Acknowledging Alarms	294
	Viewing Alarms	295
	Acknowledging Alarms	296
	Clearing Alarms	296
	Escalating Alarms	297
	Unacknowledging Alarms	297
	Viewing Acknowledged Alarms	297
	Viewing, Configuring, and Searching for Notifications	297
	Notification Escalation	298
	Creating Reports	299
	Creating Key SNMP Customized Performance Reports, Node Reports, Domain Reports	299
	Creating a New KSC Report from an Existing Report	299
	Viewing Reports	300
	Viewing Resource Graphs	300
	Viewing Key SNMP Customized (KSC) Performance Reports, Node Reports, Domain Reports	301
	Viewing Database Reports	301
	Sending Database Reports	302
	Viewing Pre-run Database Reports	303
	Viewing Statistics Reports	303
	Generating a Statistics Report for Export	303
	Deleting Reports	304
	Deleting Key SNMP Customized Reports	304
	Deleting Pre-run Database Reports	304

	Viewing Charts	305
	Admin: Configuring Network Monitoring	305
	Configuring Users, Groups, and Roles	305
	OpenNMS System: System Information	309
	OpenNMS System: Instrumentation Log Reader	310
	Notification Status	311
	Configuring SNMP Community Names by IP	311
	Configuring SNMP Data Collection per Interface	312
	Managing and Unmanaging Interfaces and Services	313
	Managing Thresholds	313
	Creating Thresholds	313
	Modifying Thresholds	316
	Deleting Thresholds	317
	Configuring Notifications	317
	Configuring Event Notifications	317
	Configure Destination Paths	319
	Configure Path Outages	320
	Configuring Scheduled Outages	321
Part 6	Device Configuration Files	
Chapter 27	Managing Configuration Files	325
	Managing Configuration Files Overview	326
	Viewing Configuration File Statistics and Inventory	327
	Backing Up Configuration Files	328
	Deleting Configuration Files	330
	Restoring Configuration Files	331
	Comparing Configuration Files	332
	Editing Configuration Files	334
	Exporting Configuration Files	336
	Tagging, Viewing Tags, and Untagging Configuration Files	337
	User Privileges in Configuration File Management	337
Part 7	Job Management	
Chapter 28	Overview	341
	Job Management Overview	341
Chapter 29	Administration	345
	Viewing Your Jobs	345
	Viewing Scheduled Jobs	347
	Changing the View	347
	Viewing Job Types	348
	Viewing Job Status Indicators	348
	Viewing Job Details, Status, and Results	349
	Performing Manage Jobs Commands	350
	Viewing Statistics for Scheduled Jobs	350
	Viewing the Types of Jobs That Are Run	351
	Viewing the State of Jobs That Have Run	351

	Viewing Average Execution Times for Jobs	352
	Canceling a Job	352
	Viewing Job Recurrence	353
Part 8	Audit Logs	
Chapter 30	Overview	357
	Junos Space Audit Logs Overview	357
Chapter 31	Administration	359
	Viewing Audit Logs	359
	Viewing Audit Log Statistics	361
	Converting the Audit Log File UTC Timestamp to Local Time in Microsoft Excel	363
	Archiving and Purging Audit Logs	364
	Archiving Audit Logs To a Local Server and Purging the Database	365
	Archiving Audit Logs To a Remote Server and Purging the Database	366
	Exporting Audit Logs	367
Part 9	Users	
Chapter 32	Role-Based Access Control	371
	Role-Based Access Control Overview	371
	Authentication	371
	RBAC Enforcement	371
	Enforcement by Workspace	371
	RBAC Enforcement Not Supported for Getting Started Page	372
	Understanding How to Configure Users to Manage Objects in Junos Space	372
	Predefined Administrator Roles	373
Chapter 33	User Accounts	381
	Creating Users	381
	Creating a New User Account	382
	Disabling and Enabling Users	385
	Viewing Users	386
	Changing Views	386
	Viewing User Details	386
	Performing Manage User Commands	387
	Modifying a User	387
	Deleting Users	389
	Changing User Passwords	389
	Clearing User Local Passwords	390
	Viewing User Statistics	391
	Viewing the Number of Users Assigned by Role	391
Chapter 34	User Roles	393
	Managing Roles Overview	393
	Managing Roles	394
	Creating a User-Defined Role	395
	Modifying User-Defined Roles	397
	Deleting User-Defined Roles	397

Part 10	Administration	
Chapter 35	Overview	401
	Junos Space Administrators Overview	401
	Maintenance Mode Overview	402
	Maintenance Mode Access and System Locking	403
	Maintenance Mode User Administration	403
Chapter 36	Fabric	405
	Fabric Management	405
	Fabric Management Overview	405
	Single Node Functionality	406
	Multinode Functionality	407
	Node Function Availability	409
	Adding a Node to an Existing Fabric	409
	Adding a Fabric Node	411
	Adding a Fabric Node	411
	Viewing Nodes in the Fabric	412
	Changing Views	412
	Viewing Fabric Node Details	413
	Performing Fabric Node Actions	415
	Configuring Node Network Settings	415
	Network Settings Configuration Guidelines	416
	Changing the VIP Interface in the Same Subnet	416
	Changing the Node Management IP in the Same Subnet	416
	Changing the Default Gateway	417
	Changing the Management IP to a Different Network	417
	Adding the Device Management IP Address	417
	Changing the Device Management IP Address in the Same Subnet	418
	Changing the Device Management IP Address to a Different Network	418
	Deleting a Device Management IP Address	418
	Changing the VIP Interface to a Different Network	419
	Changing the Node Management IP Address of All Nodes in the Fabric to the Same Subnet	419
	Changing the VIP interface of a Multi-Node Fabric to a Different Network	419
	Shutting Down or Rebooting a Node From Junos Space	420
	Deleting a Node	421
	Understanding Overall System Condition and Fabric Load	422
	System Condition	422
	Fabric Load	424
	Monitoring Nodes in the Fabric	424
	Creating a System Snapshot	425
	Deleting a System Snapshot	428
	Restoring the System to a Snapshot	428

Chapter 37	Manage Databases	431
	Database Backup and Restore Overview	431
	Backing up a Database	432
	Restoring a Database	432
	Backing Up the Database	433
	Backing Up the Database to a Local Directory	433
	Backing Up the Database to a Remote Host	434
	Restoring a Database in the User Interface	437
	Restoring a Local Database	438
	Restoring a Database from a Remote Host	439
	Restoring a Database in Maintenance Mode	440
	Viewing Database Backup Files	442
	Changing Views	442
	Viewing Database Details	442
	Manage Database Commands	443
	Deleting Database Backup Files	443
	Viewing Job Recurrence	444
Chapter 38	Manage Licenses	445
	Generating and Uploading the Junos Space License Key File	445
	Generating the License Key File	445
	Uploading the License Key File Contents	446
	Viewing Licenses	447
	Changing the View	448
	Viewing Manage License Details	449
Chapter 39	Manage Applications	451
	Application Management Overview	451
	Managing Junos Space Applications	452
	Changing The View	453
	Viewing Detailed Application Information	453
	Performing Manage Application Actions	454
	Modifying Application Settings	454
	Configuring Network Application Platform Application Settings	456
	Configuring Network Activate Application Settings	457
	Adding a Junos Space Application	458
	Upgrading a Junos Space Application	460
	Junos Space Software Upgrade Overview	461
	Upgrading Junos Space Software	462
	Junos Space 11.4 Release Highlights	462
	Before You Begin	463
	Upgrading Junos Space Release 11.2 or 11.3 to Release 11.4	463
	Upgrading the Network Application Platform	463
	Uninstalling a Junos Space Application	467

Chapter 40	System Troubleshooting	469
	System Status Log File Overview	469
	System Status Log File	469
	Customizing Status Log File Content	470
	Downloading System Log Files For an Appliance	470
	Customizing Log Files To Download	470
	Customizing Node System Status Log Checking	471
	Customizing Node Log Files To Download	472
	Downloading the Troubleshooting Log File from the UI	472
	Downloading the Troubleshooting Log File In Maintenance Mode	474
	Downloading Troubleshooting System Log Files Using the CLI	475
	Downloading a System Log File Using a USB Device	475
	Downloading System Log File Using SCP	476
Chapter 41	Authentication Servers	479
	Managing Remote Authentication Servers	479
	Remote Authentication Overview	479
	Understanding Junos Space Authentication Modes	480
	Local Authentication	480
	Remote Authentication	480
	Remote-Local Authentication	481
	Configuring Remote Authentication Method Workflows	481
	Configuring Local Authentication	481
	Configuring Remote Only Authentication	482
	Configuring Local-Remote Authentication	482
	Managing Remote Authentication Servers	483
	Creating a Remote Authentication Server	484
	Modifying Authentication Settings	486
	Junos Space Log In Behavior with Remote Authentication Enabled	486
Chapter 42	Managing Tags	491
	Overview	491
	Managing Tags Overview	491
	Managing Tags	492
	Managing Tags	492
	Sharing a Tag	493
	Renaming Tags	494
	Deleting Tags	495
	Tagging an Object	495
	Viewing Tags	496
	Untagging Objects	497
	Filtering Inventory Using Tags	497
	Creating Tags	498
	Creating a Tag	498
Chapter 43	Managing Permission Labels	499
	Managing Permission Labels Overview	499
	Working With Permission Labels	501
	Creating Permission Labels	501
	Assigning Permission Labels to Users	502

	Attaching Permission Labels to Objects	503
Chapter 44	Managing DMI Schemas	505
	Managing DMI Schemas Overview	506
	Updating a DMI Schema	508
	Creating a tgz File for Updating a DMI Schema	511
	Setting a Default DMI Schema	513
	Troubleshooting DMI Schema Management	514
Part 11	Index	
	Index	519

List of Figures

Part 1	Junos Space User Interface	
Chapter 1	Getting Started	3
	Figure 1: Junos Space System Login Screen	4
Chapter 2	Understanding the Junos Space User Interface	9
	Figure 2: Junos Space Banner	12
	Figure 3: Application Chooser	13
	Figure 4: Platform Dashboard	13
	Figure 5: Workspace Statistics	14
	Figure 6: Inventory Page: Thumbnail View	15
	Figure 7: Inventory Page: Tabular View	15
	Figure 8: Application Chooser	16
	Figure 9: Application Switcher Menu	17
	Figure 10: Navigation Ribbon: Workspaces	17
	Figure 11: Navigation Ribbon: Tasks	17
	Figure 12: Navigation Ribbon: Subtasks	18
	Figure 13: Platform Application Icon	18
	Figure 14: Platform Dashboard	20
	Figure 15: Platform System Health Gadget	23
	Figure 16: Fabric Monitoring Page	24
	Figure 17: Manage Users Page	25
	Figure 18: Job Information Gadget	25
	Figure 19: Manage Jobs Page	26
	Figure 20: Workspace Statistics Pages	26
	Figure 21: Manage Devices Inventory Page	27
	Figure 22: Manage Devices Page	28
	Figure 23: Manage Devices Inventory Page: Thumbnail View	30
	Figure 24: Manage Devices Inventory Page: Tabular View	30
	Figure 25: Sorting Tables	32
	Figure 26: Showing or Hiding Columns in Tables	32
	Figure 27: Search	33
	Figure 28: Page Information Bar	34
Part 2	Devices	
Chapter 3	Discovering Devices	39
	Figure 29: Specify Probes Dialog Box	43
	Figure 30: Add SNMP Settings Dialog Box (SNMP V1/V2C)	44
	Figure 31: Add SNMP Settings Dialog Box (SNMP V3)	44
	Figure 32: Specify Credentials Dialog Box	45

	Figure 33: Add Device Login Credential	45
	Figure 34: Discovery Status Report	46
	Figure 35: Device Discovery Detailed Report	47
	Figure 36: Job Report: Discover Network Elements Job	47
	Figure 37: Specify Device Targets	48
	Figure 38: Specify SNMP Probes	50
Chapter 4	Adding Deployed Devices	51
	Figure 39: Add Devices Dialog Box	52
	Figure 40: Selecting a CSV File to Upload	53
Chapter 5	Device Management Overview	57
	Figure 41: Device Count by Platform Report	59
	Figure 42: Device Status Report	60
	Figure 43: Device Count by OS Report	61
Chapter 6	Managing Devices	63
	Figure 44: Inventory Page: SRX Chassis Cluster	65
	Figure 45: Table Icon	65
	Figure 46: Device Table	65
	Figure 47: Selecting Columns	67
	Figure 48: Device Inventory: Single Chassis	76
	Figure 49: Device Inventory: Chassis Cluster	76
	Figure 50: Device Inventory: Service Information	76
	Figure 51: Device Inventory: Physical Interfaces	78
	Figure 52: Delete Devices Dialog Box	80
	Figure 53: Resynchronize Devices Dialog Box	81
	Figure 54: Resynchronization Information Status Message	81
	Figure 55: Change Credentials Dialog Box	83
	Figure 56: Change Credentials Dialog Box	83
	Figure 57: Physical Inventory with Service Contract Data	84
	Figure 58: Physical Inventory with Column Display Filters	85
	Figure 59: Service Now Service Detail Page	86
	Figure 60: Service Insight Exposure Analyzer Record with EOL Data	87
	Figure 61: Manage Devices Inventory Table	88
	Figure 62: Manage Devices Actions Drawer	88
	Figure 63: Physical Inventory View	89
	Figure 64: Physical Inventory View with Expanded Details	89
	Figure 65: Export Inventory Dialog Box	90
	Figure 66: Export Inventory Job Status Report	90
	Figure 67: Resynchronization Process	96
Chapter 7	Adding Devices and Connection Profiles	99
	Figure 68: Deploy Devices Inventory	102
	Figure 69: Device Details dialog box	102
	Figure 70: Selecting a CSV File to Upload	103
	Figure 71: Specifying Device Details	104
	Figure 72: Specifying Connectivity Details	104
	Figure 73: Specifying Configlet Options	107
	Figure 74: Deployment Instance Details Report	108

	Figure 75: Delete Deployment Instance Dialog Box	109
	Figure 76: Download Configlets Dialog Box	110
	Figure 77: Searching for a Configlet	110
	Figure 78: Connection Profiles Inventory	113
	Figure 79: Creating a Connection Profile	113
	Figure 80: PPPoA Connection Settings	115
	Figure 81: PPPoE Connection Settings	116
	Figure 82: Viewing the Details of a Connection Profile	117
	Figure 83: Modifying a Connection Profile	118
	Figure 84: Searching for a Connection Profile	119
Chapter 8	Secure Console	121
	Figure 85: Secure Console Window	122
	Figure 86: Secure Console Dialog Box	124
Chapter 10	Discovering Topologies	145
	Figure 87: Discover Topology	146
	Figure 88: Discovery Job Details Report	147
	Figure 89: Specify Device Targets	148
	Figure 90: Specify SNMP Probes	149
	Figure 91: Add Device Target Dialog Box	150
	Figure 92: Add SNMP V1/V2C Settings Dialog Box	152
	Figure 93: Add SNMP V3 Settings Dialog Box	152
Part 3	Device Templates	
Chapter 11	Overview	157
	Figure 94: Workflow for Device Template Definition and Template Creation	159
Chapter 12	Device Template Definitions	161
	Figure 95: Template Definition Workflow	163
	Figure 96: Create Definition Dialog Box	171
	Figure 97: General Tab	173
	Figure 98: Browsing the	174
	Figure 99: Specify Default Values Page	194
	Figure 100: Specify Default Values Page	195
	Figure 101: Unpublish Template Definition	197
Chapter 13	Device Templates	203
	Figure 102: Template Status Report	204
Part 4	Device Images and Scripts	
Chapter 17	Scripts	225
	Figure 103: Manage Scripts page	226
Chapter 19	Script Bundles	231
	Figure 104: Manage Script Bundles Page	231
Chapter 20	Configuration: Device Images	233
	Figure 105: Upload Image Dialog Box	233
	Figure 106: Validation Results Page	237

	Figure 107: View Deploy Results Page	243
	Figure 108: Modify Device Image Details	245
Chapter 21	Configuration: Scripts	247
	Figure 109: Import Scripts Dialog Box	248
	Figure 110: Modify Script Dialog Box	249
	Figure 111: Compare Scripts Dialog Box	250
	Figure 112: Compare Scripts Window	251
	Figure 113: Delete Device Scripts Dialog Box	252
	Figure 114: Deploy Scripts On Device(s) Dialog Box	253
	Figure 115: Verify Checksum of Scripts on Device(s) Dialog Box	254
	Figure 116: Enable Scripts on Device(s) Dialog Box	256
	Figure 117: Execute Script on Device(s) Dialog Box	258
Chapter 22	Configuration: Operations	259
	Figure 118: Create Operation-Edit Script Dialog Box	260
	Figure 119: Create Operation-Edit Image Dialog Box	261
	Figure 120: Create Operation-Add Operation Dialog Box	261
	Figure 121: Run Operation Page	264
Chapter 23	Configuration: Script Bundles	267
	Figure 122: Create Script Bundle page	267
	Figure 123: Modify Script Bundle page	269
	Figure 124: Deploy Script Bundle On Device(s) Dialog Box	271
	Figure 125: Execute Script Bundle On Devices(s) Dialog Box	272
Chapter 24	Administration: Scripts	275
	Figure 126: Script Details Dialog Box	276
	Figure 127: Script Verification Results Dialog Box	277
Chapter 25	Administration: Operations	279
	Figure 128: View Operation Results Page	280
Part 7	Job Management	
Chapter 29	Administration	345
	Figure 129: My Jobs Report	346
Part 10	Administration	
Chapter 35	Overview	401
	Figure 130: Maintenance Mode Actions Menu	403
Chapter 36	Fabric	405
	Figure 131: Fabric Nodes	406
	Figure 132: Fabric with One Node	407
	Figure 133: Fabric with Two Nodes	408
	Figure 134: Fabric with Three Nodes	408
	Figure 135: Add Fabric Node Dialog Box	410
Chapter 37	Manage Databases	431
	Figure 136: Maintenance Mode Dialog Box	440

	Figure 137: Authentication Required Dialog Box	440
	Figure 138: Maintenance Actions	441
	Figure 139: Selection Box	441
	Figure 140: Confirmation Message	441
Chapter 38	Manage Licenses	445
	Figure 141: Administration: Upload Licence Dialog Box	446
	Figure 142: License Information Upload Success Message	447
	Figure 143: Manage Licenses Inventory Page	447
	Figure 144: License File	449
Chapter 40	System Troubleshooting	469
	Figure 145: Maintenance Mode Page	474

List of Tables

	About the Documentation	xxvii
	Table 1: Notice Icons	xxviii
	Table 2: Text and Syntax Conventions	xxviii
Part 1	Junos Space User Interface	
Chapter 2	Understanding the Junos Space User Interface	9
	Table 3: Junos Space Application Icons	10
	Table 4: Junos Space Shortcut Icons	11
	Table 5: Global Action Icons	12
	Table 6: Workspace Icons	21
	Table 7: Gadget Mouse-Over and Double-Click Operations	22
	Table 8: Table Paging and Refreshing Controls	34
Part 2	Devices	
Chapter 4	Adding Deployed Devices	51
	Table 9: Icons to View or Download Management CLI Commands	54
Chapter 6	Managing Devices	63
	Table 10: Device Connection Status Icon	64
	Table 11: Fields in the Manage Devices Table	66
	Table 12: Device Inventory Fields	77
	Table 13: Physical Interfaces Columns	78
	Table 14: License Usage Summary Fields	92
	Table 15: License Feature or SKU Fields	93
	Table 16: Additional Fields in CSV Files	93
	Table 17: Commands Available in the Troubleshoot Device Dialog Box	94
Chapter 7	Adding Devices and Connection Profiles	99
	Table 18: Icons in the Rapid Deployment dialog box	106
	Table 19: Fields Manually Entered in the Rapid Deployment Dialog Box	107
	Table 20: IP Assignment Types	114
Chapter 10	Discovering Topologies	145
	Table 21: Discover Topology Landing Page Field Name and Descriptions	146
	Table 22: Discovery Job Details Field Names and Descriptions	147
Part 3	Device Templates	
Chapter 12	Device Template Definitions	161
	Table 23: Junos OS Configuration Hierarchy Guide Reference	165

	Table 24: Data Types and Tabs	167
	Table 25: Data Types and Validation Parameters	167
	Table 26: Template Definition States	196
Chapter 13	Device Templates	203
	Table 27: Device Template State Icon Indicators	204
	Table 28: Descriptive Information	204
Part 4	Device Images and Scripts	
Chapter 15	Overview	219
	Table 29: Device Images and Scripts User Roles	220
Chapter 16	Device Images	223
	Table 30: Manage Images Page	223
Chapter 17	Scripts	225
	Table 31: Manage Scripts Page Fields Description	226
Chapter 20	Configuration: Device Images	233
	Table 32: Stage Image On Devices Dialog Box Fields Descriptions	235
	Table 33: Validation Results Page Field Descriptions	237
	Table 34: Routing Platforms and Software Releases Supporting ISSU	238
	Table 35: Common Deployment Options Description	241
	Table 36: Conventional Deployment Options Description	241
	Table 37: ISSU Deployment Options Description	241
	Table 38: Advanced Deployment Options Description	242
	Table 39: Select Devices Table Field Descriptions	242
Chapter 22	Configuration: Operations	259
	Table 40: Create Operation Dialog Box Icon Descriptions	262
Chapter 23	Configuration: Script Bundles	267
	Table 41: Create Script Bundle Dialog Box Icon Descriptions	268
	Table 42: Modify Script Bundle Dialog Box Icon Descriptions	269
Chapter 24	Administration: Scripts	275
	Table 43: Script Details Dialog Box Fields	276
	Table 44: Script Verification Results Page Fields	277
Part 5	Network Monitoring	
Chapter 26	Network Monitoring UI	283
	Table 45: Information Displayed in the Alarms List	295
Part 7	Job Management	
Chapter 28	Overview	341
	Table 46: Junos Space Job Types Per Application	342
Chapter 29	Administration	345
	Table 47: Job Icon Status Indicators	348
	Table 48: Job Details and Columns in the Manage Jobs Table	349

Part 8	Audit Logs	
Chapter 31	Administration	359
	Table 49: Detailed Audit Logs Information and View Audit Log Table	
	Columns	360
	Table 50: Audit Log Table Details for Recurring and Non-recurring Jobs	360
Part 9	Users	
Chapter 32	Role-Based Access Control	371
	Table 51: Predefined Roles for the Network Application Platform	374
	Table 52: Predefined Roles for Network Activate Application	377
	Table 53: Predefined Roles for Service Now Application	379
	Table 54: Predefined Roles for Ethernet Design Application	380
Chapter 33	User Accounts	381
	Table 55: Users Detailed Information and Columns in the Manage Users	
	Table	386
Part 10	Administration	
Chapter 35	Overview	401
	Table 56: Junos Space Administrators	401
Chapter 36	Fabric	405
	Table 57: Fields for the Fabric Monitoring Inventory Page	413
Chapter 37	Manage Databases	431
	Table 58: Fields in the Manage Databases Table	442
Chapter 38	Manage Licenses	445
	Table 59: Manage Licenses Details	449
Chapter 39	Manage Applications	451
	Table 60: Application Information	453
	Table 61: Network Application Platform Application Settings	456
	Table 62: Network Activate Application Settings	457
Chapter 40	System Troubleshooting	469
	Table 63: Log Files included in the troubleshoot File	470
	Table 64: Data and Log Files in troubleshoot.zip File	473
Chapter 41	Authentication Servers	479
	Table 65: Remote Authentication Server Settings	484
Chapter 42	Managing Tags	491
	Table 66: Tag Information	493

About the Documentation

- Documentation and Release Notes on page xxvii
- Documentation Conventions on page xxvii
- Documentation Feedback on page xxix
- Requesting Technical Support on page xxx

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 xxviii 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 xxviii 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 send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number

- Software release version (if applicable)

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

Junos Space User Interface

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

CHAPTER 1

Getting Started

- [Logging In to Junos Space on page 3](#)
- [Changing User Passwords on page 4](#)
- [Using the Getting Started Assistants on page 5](#)
- [Accessing Help on page 6](#)
- [Logging Out of the Junos Space System on page 6](#)

Logging In to Junos Space

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



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



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

To access and log in to Junos Space:

1. In the address field of your browser window, type
https://<1.1.1.1>/mainui/
where <1.1.1.1> is the Web IP address for Web access to Junos Space.
2. Press Enter or click **Search**.
The system login screen appears.

Figure 1: Junos Space System Login Screen

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

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

5. Click **Log In**.

The Junos Space Application Chooser appears.

Related Documentation

- [Logging Out of the Junos Space System on page 6](#)
- [Changing User Passwords on page 4](#)
- [Application Chooser Overview on page 9](#)
- [Junos Space User Interface Overview on page 11](#)
- [Junos Space Log In Behavior with Remote Authentication Enabled on page 486](#)

Changing User Passwords

Users that are logged in to Junos Space can change their account password using the User Preferences icon in the Junos Space banner. You do not have to have any user roles configured to change your password.



WARNING: If you have a local password for remote or remote-local authentication modes, changing your password does that locally only. The change does not affect any passwords that a user administrator might have configured for you on a remote authentication server.



WARNING: If a user does not have a local password set, that user will not be able to set or change it.

To change your user password, follow these steps:

1. Click the User Preferences icon in the Junos Space banner. The User Preferences – Change Password dialog box appears.
2. Type your old password.

3. Type your new password.

The password must be 6 to 31 characters long, including two numbers or symbols.

4. Retype your password to confirm it.
5. Click **Change**. You are logged out of the system.

You have to log in again using your new password. Any open sessions are disabled until you log in again.

- Related Documentation**
- [Creating Users on page 381](#)
 - [Logging In to Junos Space on page 3](#)

Using the Getting Started Assistants

The Getting Started assistants display steps and help on how to complete common tasks. Getting Started is a section in the sidebar that appears when you log in to the system if the Show Getting Started on Startup check box is selected. The Getting Started topics are context sensitive per application. Getting Started displays all the steps in a task. From a step in a task, you can jump that point in the user interface to actually complete it.

To use a Getting Started assistant:

1. In Application Chooser, select an application.
2. Click the Help icon . The sidebar appears.
3. In the sidebar, expand **Getting Started**.

A main Getting Started topic link appears in the sidebar.

4. Select a main topic.

For example, in the Network Activate application, click **Provision a Service**. A list of required steps appears in the sidebar. Each step contains a task link and a link to the Help.

5. Perform a specific step by clicking the link.

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

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

- Related Documentation**
- [Accessing Help on page 6](#)
 - [Application Chooser Overview on page 9](#)

Accessing Help

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

To access online Help:

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

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

3. Click a topic link to view its contents.

The Help topic appears in a separate window.

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

Related Documentation

- [Using the Getting Started Assistants on page 5](#)
- [Application Chooser Overview on page 9](#)
- [Platform Dashboard Overview on page 19](#)

Logging Out of the Junos Space System

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

To log out of the system:

1. Click the Log Out icon in the 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 60 minutes. You can change the setting in the Manage Applications inventory page. Select **Network Management Platform** and then select **Modify Application Settings** from the Actions drawer.

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

Related Documentation

- [Logging In to Junos Space on page 3](#)
- [Changing User Passwords on page 4](#)
- [Modifying Application Settings on page 454](#)
- [Application Chooser Overview on page 9](#)

- [Junos Space User Interface Overview on page 11](#)

CHAPTER 2

Understanding the Junos Space User Interface

- [Application Chooser Overview on page 9](#)
- [Junos Space User Interface Overview on page 11](#)
- [Navigating the Junos Space User Interface on page 16](#)
- [Network Application Platform Overview on page 18](#)
- [Platform Dashboard Overview on page 19](#)
- [Viewing Dashboard Statistics on page 23](#)
- [Workspace Statistics Pages Overview on page 26](#)
- [Inventory Pages Overview on page 28](#)

Application Chooser Overview

The Application Chooser provides a user interface within which you can view and manage installed applications in Junos Space. The Application Chooser appears when you first log in to the system.

Mouse over an application to view its title and description. Double-click an application icon to launch it and navigate to its dashboard.

Parts of the Application Chooser




The following sections describe the parts of the Application Chooser:

- [Application Icons on page 9](#)
- [Shortcut Icons on page 10](#)
- [Login User Name on page 11](#)

Application Icons

[Table 3 on page 10](#) lists the Application Chooser icons for the Junos Space base applications. You can install other applications using the Manage Applications workspace (see [“Application Management Overview” on page 451](#)).

Table 3: Junos Space Application Icons


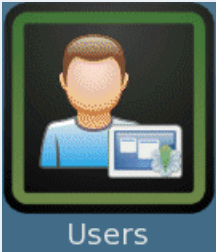
Application Icon/Name	For more information
 Platform	See "Platform Dashboard Overview" on page 19.
 Service Insight	See <i>Service Insight Overview</i> .
 Service Now	See <i>Service Now Overview</i> .

You can use the Application Switcher, accessed via the application banner, to switch to other applications. The Application Switcher displays the five most recently used applications or shortcuts.

Shortcut Icons

Table 4 on page 11 lists the Application Chooser icons for shortcuts. Shortcuts allow you to jump directly to a workspace without user interface navigation. For example, use the Devices shortcut to jump directly to the Devices workspace.

Table 4: Junos Space Shortcut Icons

Shortcut Icon/Name	For more information
	See “Viewing Managed Devices” on page 63.
	See “Viewing Users” on page 386.

Login User Name

Displays the username of the person currently logged in to the system.

Application Chooser Actions

The Application Chooser provides the following user actions:

- Change Application Chooser Views—To change the Application Chooser view, click the Thumbnail icon in the bottom-right Actions toolbar.
- Open Applications—To open an application, double-click its icon.
- Switch to Other Applications—To switch to other applications from the Application Chooser, select an application name in the Application Switcher. The Application Switcher is a global action to the right in the banner. The Application Switcher list displays the five most recently used applications or shortcuts. You must confirm whether you want to switch to that application.

Related Documentation

- Junos Space User Interface Overview on page 11
- Platform Dashboard Overview on page 19

Junos Space User Interface Overview

The Junos Space application design allows multiple users concurrent access to its user interface. Each user accesses the system using a Web browser.

Each user has access to the same systemwide database, which ensures that each user sees current information. User access to tasks and objects is controlled by permissions

assigned to the user. For example, a service provisioner will have full access to the tasks in the Service Provisioning workspace, but might not have access to Service Design tasks.

The Junos Space user interface is consistent across the Network Application Platform and other installed applications. The examples shown in this topic are from the Network Application Platform user interface. Other applications might have certain user interface design variations to fit the workflow.

Parts of the System User Interface

The following sections describe the major parts of the system user interface:

- [Banner on page 12](#)
- [Application Chooser on page 13](#)
- [Application Dashboard on page 13](#)
- [Workspace Statistics on page 14](#)
- [Inventory Page on page 14](#)

Banner






The banner displays the Junos Space application logo and name, the date and server time in the active time zone, and the global actions icons.

Figure 2: Junos Space Banner



The Junos Space application banner appears throughout each user interface page in the system. [Table 5 on page 12](#) describes the global action icons at the right in the banner.

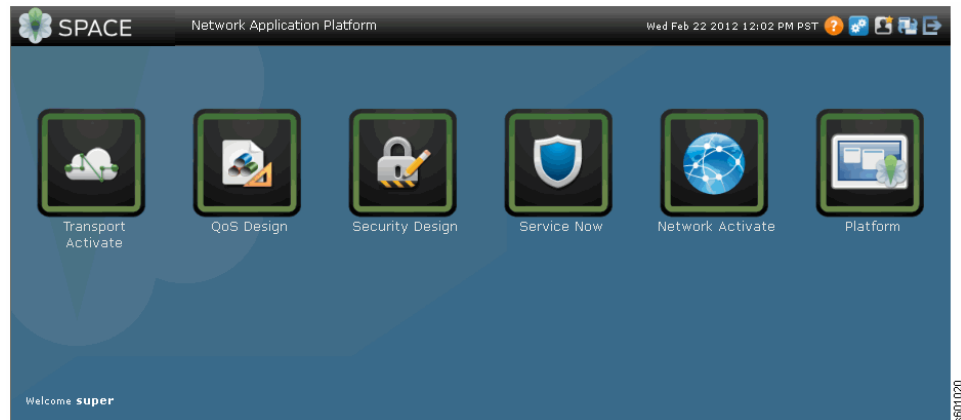
Table 5: Global Action Icons

Global Action Icon	Description
	Displays the application Help. To access workspace context-sensitive Help, click the Help icon after navigating to that workspace. See “Accessing Help” on page 6 .
	Displays the My Jobs dialog box from which you can view the progress and status of current managed jobs. See “Viewing Your Jobs” on page 345 .
	Displays the User Preferences dialog box from which you can change user preferences, such as the password. See “Changing User Passwords” on page 4 .
	Displays the Application Switcher list to switch between applications. The list displays the five most recently used applications or shortcuts. See “Application Chooser Overview” on page 9 .
	Logs you out of the system. See “Logging Out of the Junos Space System” on page 6 .

Application Chooser

When you log in to the system, you see the Application Chooser, shown in [Figure 3 on page 13](#). The Application Chooser displays the available applications and shortcuts. For more information, see [“Application Chooser Overview” on page 9](#).

Figure 3: Application Chooser

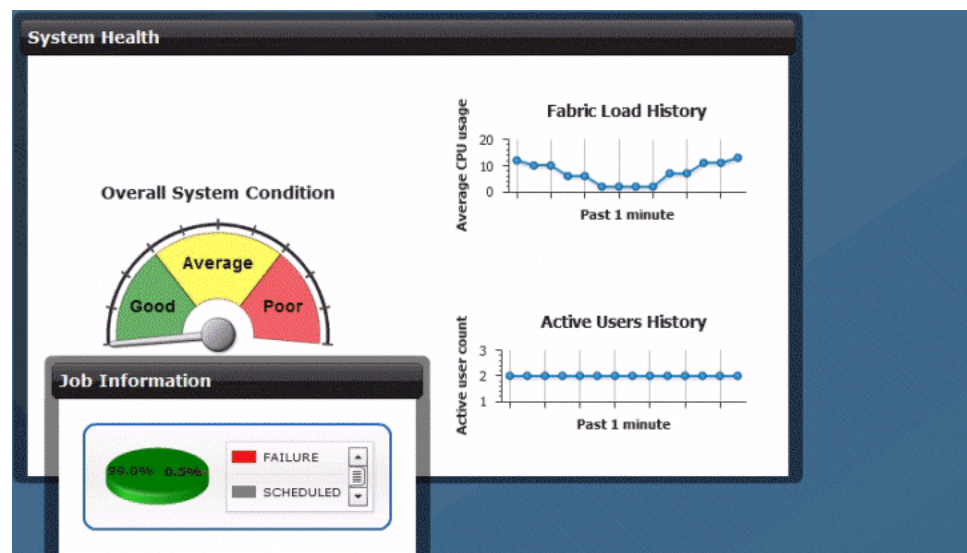


Application Dashboard

In the Application Chooser, click an application icon to view its dashboard. A dashboard displays graphical data about devices, jobs, users, administration, and so on.

[Figure 4 on page 13](#) shows the Platform dashboard. For more information, see [“Platform Dashboard Overview” on page 19](#).

Figure 4: Platform Dashboard



Workspace Statistics

In an application dashboard, click a workspace icon in the navigation ribbon to view its statistics page. The statistics page displays charts, graphics, and subtasks.

[Figure 5 on page 14](#) shows the statistics page for the Job Management workspace. For more information, see [“Workspace Statistics Pages Overview” on page 26](#).

Figure 5: Workspace Statistics



Inventory Page

Click a subtask in the workspace navigation ribbon to view its inventory page. Inventory pages display managed items in two views: thumbnail and tabular. [Figure 6 on page 15](#) shows the thumbnail view. [Figure 7 on page 15](#) shows the tabular view. For more information, see [“Inventory Pages Overview” on page 28](#).

Figure 6: Inventory Page: Thumbnail View

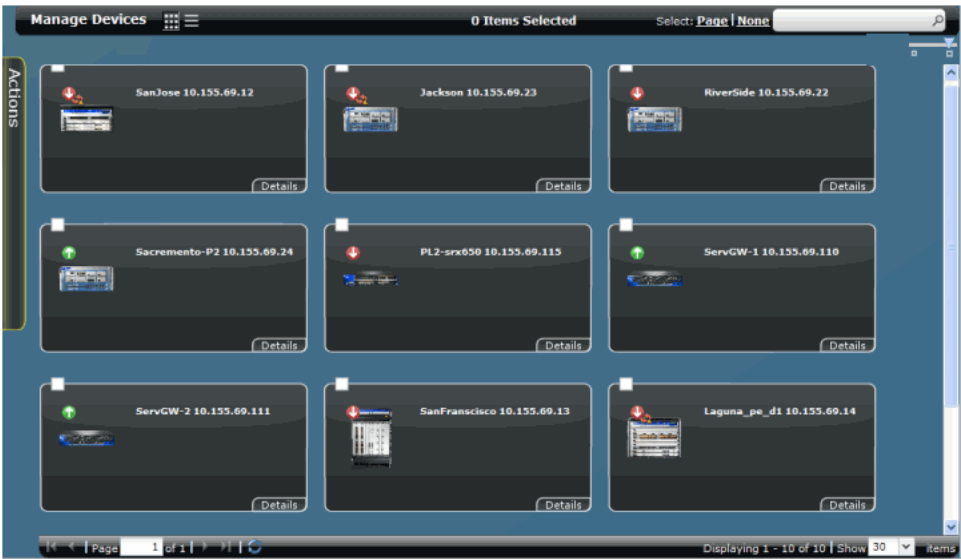


Figure 7: Inventory Page: Tabular View



- Related Documentation
- [Application Chooser Overview on page 9](#)
 - [Platform Dashboard Overview on page 19](#)
 - [Workspace Statistics Pages Overview on page 26](#)
 - [Inventory Pages Overview on page 28](#)

Navigating the Junos Space User Interface

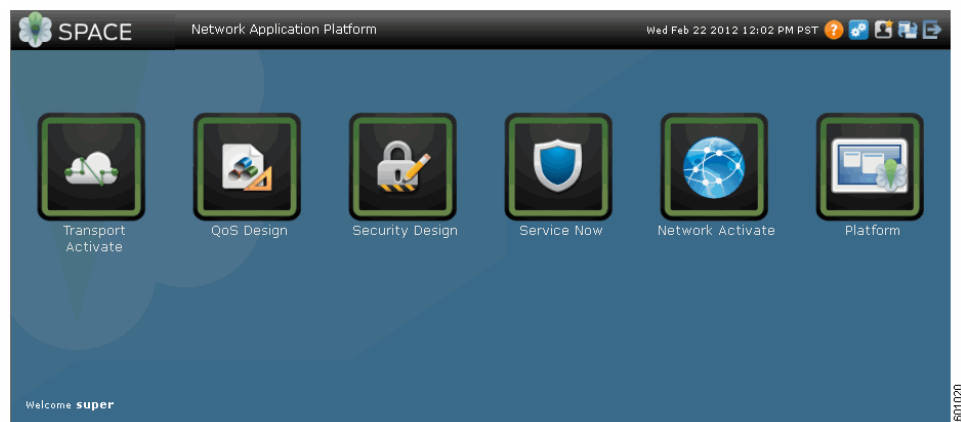
The following topics describe how to navigate the Junos Space user interface:

- [Navigating Applications Using the Application Chooser on page 16](#)
- [Navigating Applications Using the Application Switcher on page 16](#)
- [Navigating Application Workspaces and Tasks Using the Navigation Ribbon on page 17](#)
- [Navigating to the Dashboard of an Application on page 18](#)
- [Navigating to a Workspace from a Task on page 18](#)

Navigating Applications Using the Application Chooser

When you log in to Junos Space, the Application Chooser appears, as shown in [Figure 8 on page 16](#). The Application Chooser displays icons for installed applications and workspace shortcuts, such as Devices and Users.

Figure 8: Application Chooser



To navigate to an application in Application Chooser, click its icon.

Navigating Applications Using the Application Switcher

You use the Application Switcher global icon in the top-right corner of the Junos Space banner to navigate to applications or workspaces.

To navigate to an application or workspace:

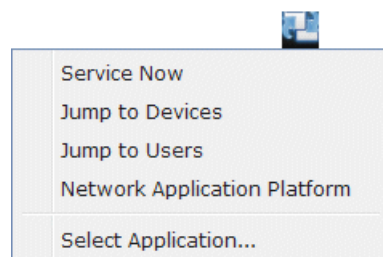
1. In the Junos Space banner, click the Application Switcher global icon.

The Application Switcher menu appears, as shown in [Figure 9 on page 17](#). The menu displays the five most recently used applications or shortcuts.

2. Select an application or workspace shortcut.

An application dashboard or workspace statistics page appears.

Figure 9: Application Switcher Menu



Navigating Application Workspaces and Tasks Using the Navigation Ribbon

Use the navigation ribbon to navigate application workspaces and tasks. When you start an application, all of the workspaces are displayed at the workspace level of the navigation ribbon.

To navigate using the application navigation ribbon:

1. In the Application Chooser, click an application icon.

The dashboard for the selected application appears. In addition, all of the workspaces are displayed in the navigation ribbon, as shown in [Figure 10 on page 17](#).

2. In the navigation ribbon, click a workspace.

Tasks related to the workspace are displayed in the navigation ribbon, as shown in [Figure 11 on page 17](#). The workspaces bank to the left in the navigation ribbon. The selected workspace is highlighted and appears to the right of the banked workspaces. The workspace tasks are displayed to the right of the workspace. Home appears rightmost in the navigation ribbon. Clicking Home takes you to the top level of the navigation ribbon where all workspaces are displayed.

3. In the navigation ribbon, click a task.

The inventory page containing objects on which to perform tasks appears. If a task has subtasks, the selected task is circled, and an arrow points to that task, as shown in [Figure 12 on page 18](#). The subtasks appear to right of the selected task.

4. In the navigation ribbon, click a subtask. The page for that subtask appears. An arrow points to the selected subtask.

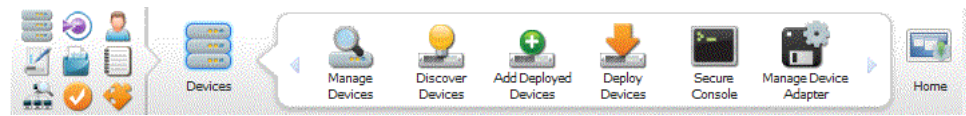
Figure 10: Navigation Ribbon: Workspaces



Figure 11: Navigation Ribbon: Tasks



Figure 12: Navigation Ribbon: Subtasks



Navigating to the Dashboard of an Application

To quickly navigate to the dashboard of an application where all workspaces appear, click Home at the right in the navigation ribbon. See [Figure 11 on page 17](#).

Navigating to a Workspace from a Task

To navigate to a workspace from a task or subtask, click the workspace icon banked at the left in the navigation ribbon. See [Figure 11 on page 17](#).

Related Documentation

- [Application Chooser Overview on page 9](#)
- [Junos Space User Interface Overview on page 11](#)

Network Application Platform Overview

The Junos Space Network Application Platform provides tools that enable automated device discovery and management, job operation management, audit logging, and network administration.

When you log into Junos Space, the Application Chooser displays icons for applications and shortcuts, including the Platform application icon shown in [Figure 13 on page 18](#). Mouse over the Platform application icon to display a brief description. Click the icon to display the Platform dashboard. The Platform dashboard displays the workspaces you can use to perform tasks.

Figure 13: Platform Application Icon



The Platform application includes the following components that enable you to automate network operations:

- **Devices**—Simplifies management of the devices running Junos OS software on your network, including discovery, deployment, and connection, and adapter management.
- **Device Templates**—Provides the tools to create custom Juniper Networks DMI schema device template definitions and templates deployable to devices on your network.

- **Topology Visualization**—Discovers network topology elements based on a device or subnet. You can view information about the devices and links in the discovered network.
- **Device Templates**—Manages Junos OS images for Juniper Networks devices so you can upload device images from your local file system to Junos Space and deploy these images onto a device or onto multiple devices of the same device family at once.
- **Scripts**—Uses configuration and diagnostic automation tools— commit, op, and event scripts—provided by the Junos OS to reduce network downtime and configuration complexity, automate common tasks, and decrease the time to problem resolution.
- **Configuration Files**—Maintains copies of device running, candidate, and backup configuration files within Junos Space, providing for device configuration recovery and maintaining configuration consistency across multiple devices.
- **Jobs**—Monitors the status of all jobs—for example, user-initiated actions performed on Junos Space objects, such as devices, services, or customers running in all Junos Space applications.
- **Audit Logs**—Monitors user login/logout activity, tracks device management tasks, and displays services that were provisioned on devices. Junos Space audit logging does not record non-user-initiated activities, such as device-driven activities, and is not designed for debugging purposes.
- **Administration**—Perform Junos Space system management tasks, including:
 - Manage Fabric
 - Manage Databases
 - Manage Licenses
 - Manage Applications
 - Troubleshoot Junos Space
 - Manage Tags
 - Manage DMI Schemas

**Related
Documentation**

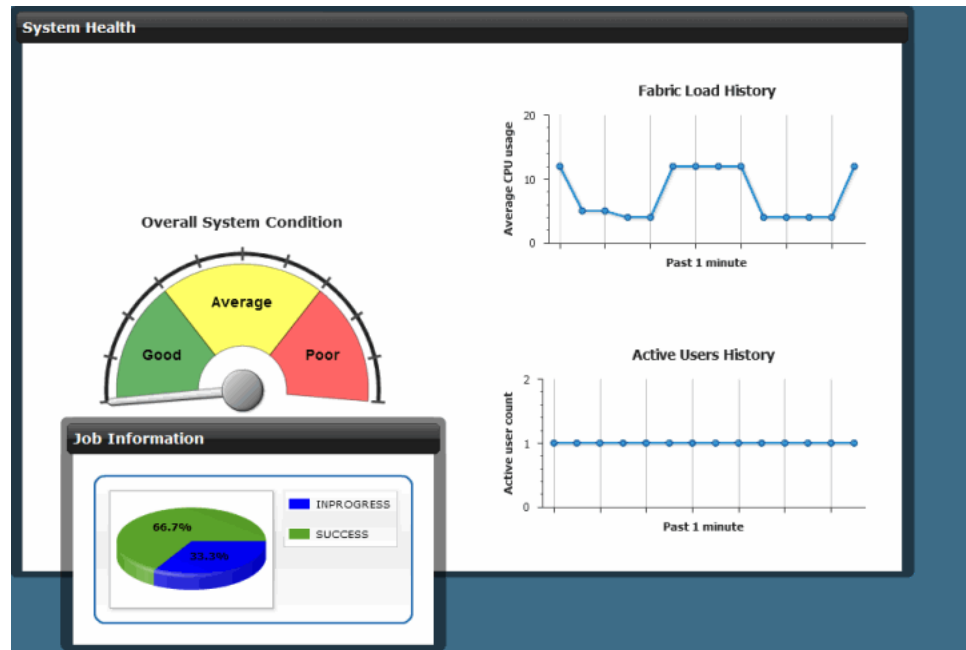
- [Application Chooser Overview on page 9](#)
- [Platform Dashboard Overview on page 19](#)
- *Network Activate Dashboard Overview*
- *Service Now Overview*
- *Ethernet Design Overview*

Platform Dashboard Overview

The dashboard provides a snapshot of the current status of objects managed and operations performed within a Junos Space application. For example, the Platform dashboard, shown in [Figure 14 on page 20](#), displays the system health of your network and the percentage of jobs run successfully and in progress. The Service Now dashboard

displays the number of platforms and devices with the most incidents. The dashboard appears when you click an application icon from Application Chooser or switch to it from the Application Switcher global icon menu.

Figure 14: Platform Dashboard



The following sections describe the parts of the Platform Dashboard:

Parts of Platform Dashboard

- [Workspace Navigation Ribbon on page 20](#)
- [Dashboard Gadgets on page 21](#)










Workspace Navigation Ribbon

Each Junos Space application has a navigation ribbon allowing you to visually navigate to the workspaces, tasks, and subtasks. To view a workspace, click its icon in the navigation ribbon. The tasks for that workspace appear in the navigation ribbon, and the statistics page for that workspace appears. For more information about using the navigation ribbon, see [“Navigating the Junos Space User Interface” on page 16](#).

When you want to leave a workspace, click Home to navigate you to all of the top-level navigation ribbon for that application. When you want to leave the application, use the Application Switcher list in the banner located in the top-right corner of the page.

[Table 6 on page 21](#) describes the Platform navigation ribbon workspaces.

Table 6: Workspace Icons

Icon	Workspace Name	Task
	Devices	Manage devices, including adding, discovering, importing, and updating them. See “Device Management Overview” on page 57 .
	Device Templates	Create configuration definitions and templates used to deploy configuration changes on multiple Juniper Networks devices. See “Device Templates Overview” on page 158 .
	Topology Visualization	Discover information about network elements and their interconnections based on the hostname or IP addresses of both Juniper-managed and non Juniper-managed devices. .
	Device Images	Download a device image from the Juniper Networks Software download site to your local file system, upload it into Junos Space, and deploy it on one or more devices at once. See “Device Images Overview” on page 223 .
	Scripts	Use Junos scripts (configuration and diagnostic automation tools) to deploy, verify, enable, disable, remove, and execute scripts deployed to devices.
	Job Management	Monitor the progress of ongoing jobs. See “Job Management Overview” on page 341 .
	Users	Add, manage, and delete users. See “Understanding How to Configure Users to Manage Objects in Junos Space” on page 372 .
	Audit Logs	View and filter system audit logs. See “Junos Space Audit Logs Overview” on page 357 .
	Administration	Add network nodes, backup your database, or troubleshoot. See “Adding a Fabric Node” on page 411 , “Database Backup and Restore Overview” on page 431 , “Downloading the Troubleshooting Log File from the UI” on page 472 , “Downloading the Troubleshooting Log File In Maintenance Mode” on page 474 , “Application Management Overview” on page 451 , “Viewing Tags” on page 496 .

Dashboard Gadgets

The Platform dashboard contains gadgets, such as graphs and charts, that display statistics that depict the overall health and functionality of that application. For example, the Platform dashboard gadgets provide an at-a-glance view of the system health, which includes the a gauge for the overall system condition and graphs that display the fabric load and active user history. For an explanation of the data shown in these gadgets, see [“Understanding Overall System Condition and Fabric Load” on page 422](#).

All dashboard gadgets are visible for all users.

Gadget information is updated automatically and immediately.

You can move gadgets on the dashboard or change the size of them. Changes in location or size of dashboard gadgets persist on returning to the dashboard, even after logging back into the system.

Click a gadget or gadget elements to drill down to more detailed information. Typically, clicking a gadget element takes you either to the statistics page of the associated workspace, or to an inventory page. Some gadgets let you filter information by selecting a specific segment or bar from a chart, or a specific line of a table. For example, if you select the red segment on the Status of Tasks run gadget, you navigate to the manage tasks inventory page, which displays only failed tasks.



NOTE: If you do not have user privileges to view certain application data, you will not be able to view more detailed information if you double-click a gadget.

Table 7 on page 22 describes the mouse-over and double-click operations you can perform on dashboard gadgets.

Table 7: Gadget Mouse-Over and Double-Click Operations

Gadget	Mouse-Over Information	Double-Click Navigation
Overall System Condition gauge	N/A	Double-click a graph data point to display the Administration workspace Manage Fabric > Fabric Monitoring page. Click Home to return to the Platform dashboard. For more information about fabric monitoring, see “Understanding Overall System Condition and Fabric Load” on page 422 .
Fabric Load History graph	Mouse over a graph data point to view the CPU Usage (average usage percentage)	Double-click a graph data point to display the Administration workspace Manage Fabric > Fabric Monitoring page. Click Home to return to the Platform dashboard. For more information about fabric monitoring, see “Viewing Nodes in the Fabric” on page 412 .
Active User History graph	Mouse over a graph data point to view the Active user (total count)	Double-click the graph data point display the Users workspace statistics page used to view the Number of Users by Assigned Role bar chart. Click Home to return to the Platform dashboard. For more information about the Users workspace, see “Viewing User Statistics” on page 391 .
Job information pie chart	Mouse over the pie chart to view the number of successful jobs.	Double-click the pie chart to display the Job Management Manage Jobs inventory page. Click Home to return to the Platform dashboard. For more information about the Job Management Manage Users inventory page, see “Viewing Scheduled Jobs” on page 347 .

Related Documentation

- [Viewing Dashboard Statistics on page 23](#)
- [Application Chooser Overview on page 9](#)
- [Junos Space User Interface Overview on page 11](#)
- [Understanding Overall System Condition and Fabric Load on page 422](#)
- [Viewing Nodes in the Fabric on page 412](#)
- [Viewing User Statistics on page 391](#)
- [Viewing Scheduled Jobs on page 347](#)

Viewing Dashboard Statistics

The dashboard appears when you select an application from the Application Chooser. It contains graphs and charts known as gadgets that provide high-level monitoring information for the system.

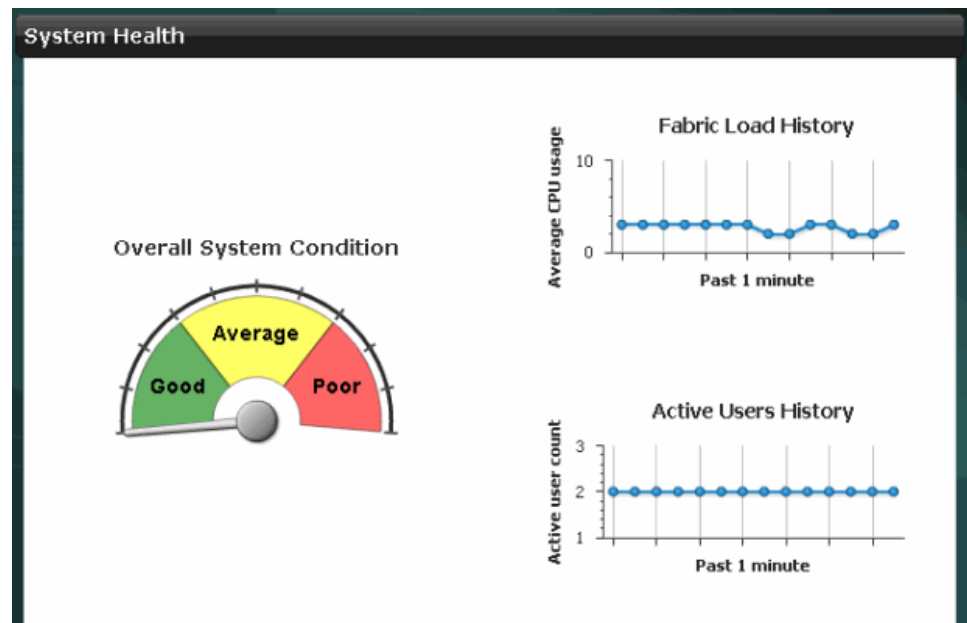
The following topics describe how to use and interpret dashboard gadgets:

- [Viewing System Health Statistics on page 23](#)
- [Viewing the Job Information on page 25](#)

Viewing System Health Statistics

The Network Application Platform dashboard system Health gadget displays real-time information about the overall health of the Junos Space system. It includes an overall system condition gauge and graphs that report the system load and number of users, as shown in [Figure 15 on page 23](#).

Figure 15: Platform System Health Gadget



The Overall System Condition gauge represents a combination of the health of the database, the application, and load-balancing software. If all these components are functional on all processors in the fabric, then the overall system condition is reported as good.

The Fabric Load History graph shows the trend of the average load of all CPUs in the fabric over the last minute. The Y axis shows the percentage of CPU use and scales dynamically so that useful information can be obtained at low loads. A new reading appears every 5 seconds.

To view the average CPU use at a specific data point, drag the mouse over the data point of interest. The fabric load is shown in parentheses in a tooltip.

To obtain more details about the status of the fabric, click any data point in the graph. The Fabric Monitoring page appears and shows detailed status of each node in the fabric, as shown in [Figure 16 on page 24](#). For more information, see [“Viewing Nodes in the Fabric” on page 412](#).

Figure 16: Fabric Monitoring Page

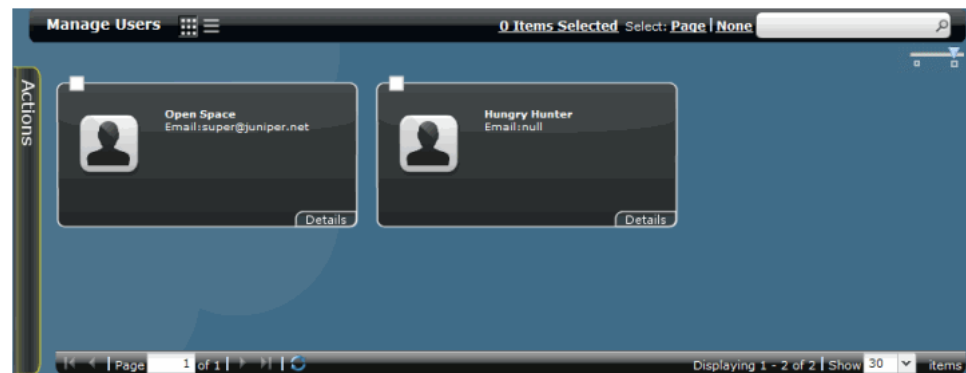


The Active Users History graph shows a history of the number of active users on the system for the previous minute.

To view the number of active users at a specific data point, drag the mouse over the data point of interest. The fabric load is shown in parentheses in a tooltip.

To obtain more details about active users, click any data point in the graph. The Manage Users inventory page appears filtered by the active users, as shown in [Figure 17 on page 25](#). For more information, see [“Viewing Users” on page 386](#).

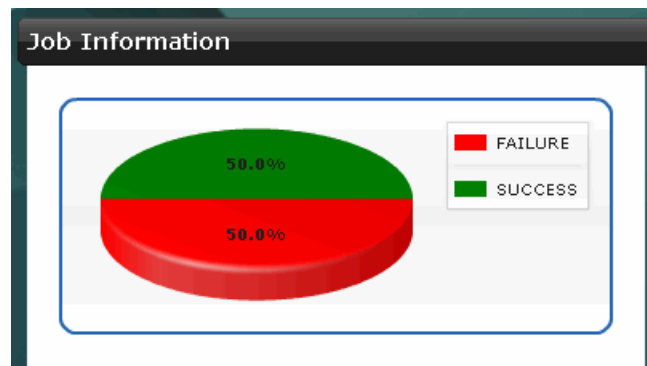
Figure 17: Manage Users Page



Viewing the Job Information

The Job Information gadget on the system dashboard provides real-time information about the proportion of tasks successfully completed, failed, or in some other state during in the logged-on user's current work session, as shown in [Figure 18 on page 25](#).

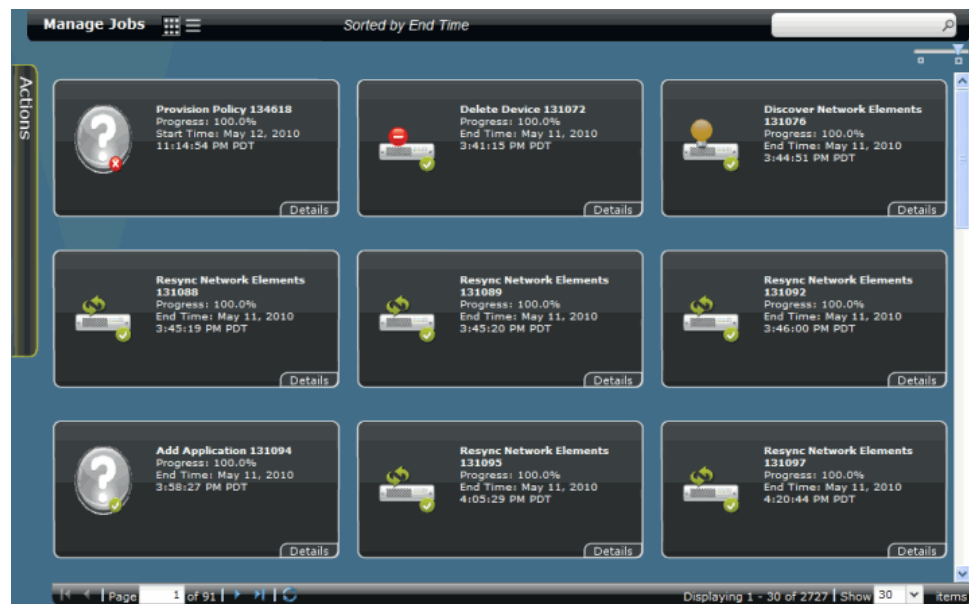
Figure 18: Job Information Gadget



To view the number of jobs in a specific state rather than the percentage, drag the mouse over the segment in the chart. The number of jobs appears in parentheses in a tooltip.

To view details about the jobs represented in the chart, click on the segment of interest. For example, click on the red segment to view details about failed jobs. The Manage Jobs page appears filtered by the job types selected, as shown in [Figure 19 on page 26](#). For more information, see [“Viewing Scheduled Jobs” on page 347](#).

Figure 19: Manage Jobs Page



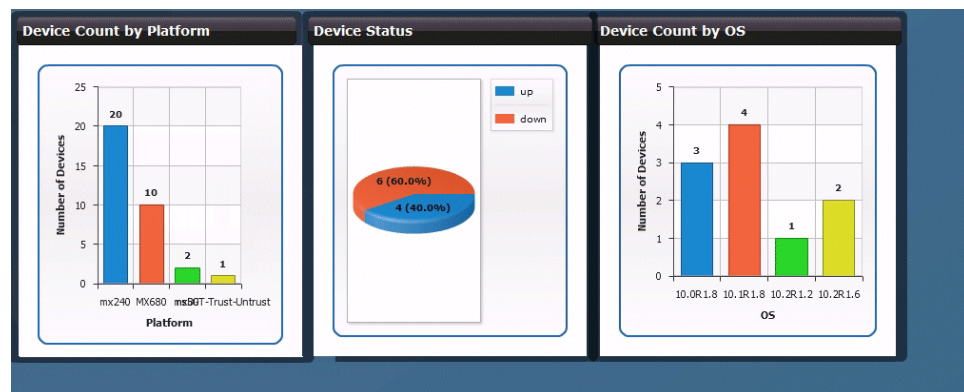
Related Documentation

- [Platform Dashboard Overview on page 19](#)
- [Understanding Overall System Condition and Fabric Load on page 422](#)

Workspace Statistics Pages Overview

When you select a workspace from an application dashboard navigation ribbon, Junos Space typically displays high-level statistics representing the status of managed objects in that workspace. [Figure 20 on page 26](#) shows the statistics page for the Devices workspace.

Figure 20: Workspace Statistics Pages



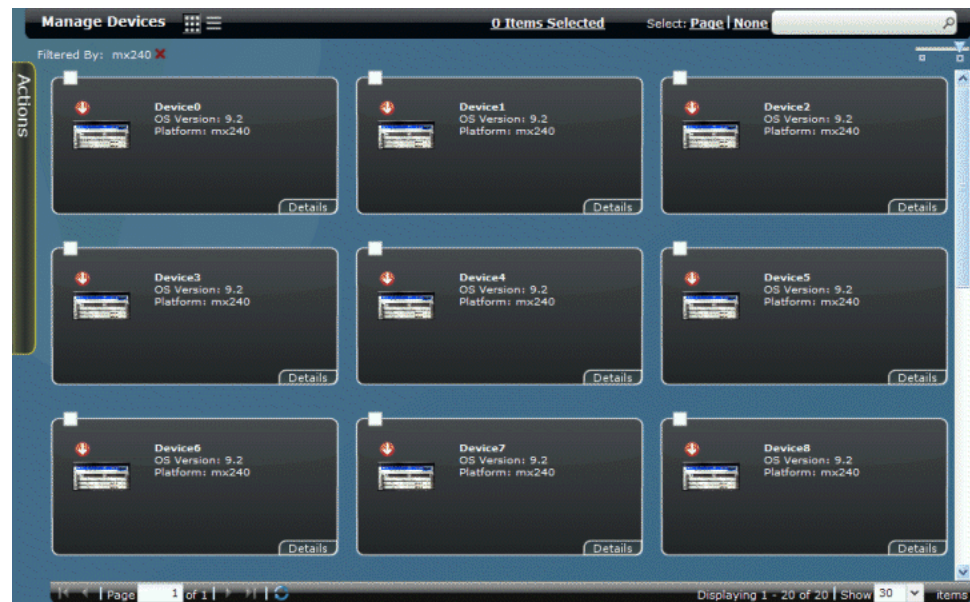
To print or save the statistics, right-click the graphic (bar chart or pie chart).

You can move charts and graphs on the screen or resize them. Changes in location or size of charts and graphs persist on returning to the statistics page, even after logging back into the system.

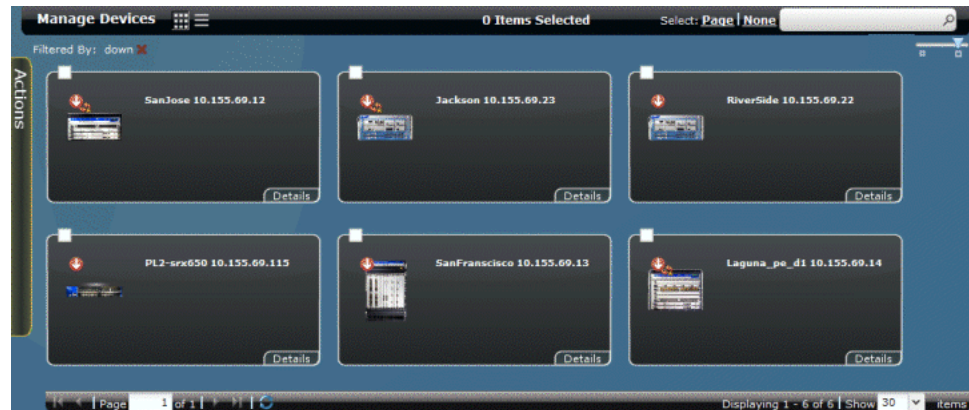
If a chart has more data points than can be viewed clearly at once, a scroll bar appears at the bottom of the chart for access to the remaining data.

Active links within the graphs and charts provide access to more details. For example, if you click a bar or pie-chart segment, you navigate to the corresponding inventory page filtered according to the bar or segment you selected. For example, if you click the MX240 devices bar in the Device Count by Juniper Networks device platform bar chart, you navigate to the Platform > Devices > Manage Devices inventory page, which displays all the MX240 devices on the network that are discovered and managed by Junos Space.

Figure 21: Manage Devices Inventory Page

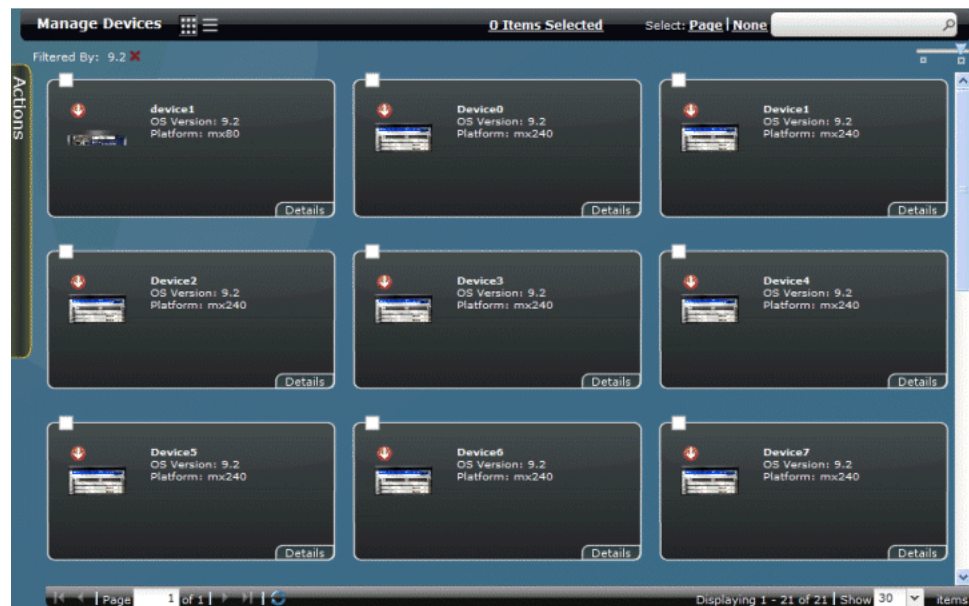


For example, if you click the slice in the Device Status pie chart that represents the number of devices that are down. You navigate to the Manage Devices inventory page that displays all of the devices on the network that are down.



For example, if you click a bar in the Device by OS Count, you navigate to the Manage Devices inventory page, which displays all of the devices that are running the Junos OS release that you selected.

Figure 22: Manage Devices Page



- Related Documentation**
- [Junos Space User Interface Overview on page 11](#)
 - [Device Management Overview on page 57](#)

Inventory Pages Overview

Application workspace inventory pages allow you to view and manipulate managed objects individually or collectively, including devices, logs, users, jobs, clients, software,

licenses, and so forth. You can browse, zoom, filter, tag, and sort objects. You can select one, several, or all objects and perform actions on them using the actions in the Actions drawer or by right-click actions.

Throughout the Junos Space user interface, you navigate to an inventory page by selecting an application from Application Chooser, selecting an application workspace in the navigation ribbon, then selecting a managing task, such as Manage Devices, Manage Users, or Manage Jobs. For example, to view the Manage Devices inventory page, select Platform > Devices > Manage Devices.

On the inventory page, managed objects are represented by unique icons. Object status is represented by superimposed icons with colors. You can mouse over objects to view the name.

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

By default, inventory pages appear in thumbnail view. You can also display them in tabular.



NOTE: The function and implementation of individual inventory pages in both thumbnail and tabular views depend on the Junos Space application design.

Parts of the Inventory Page

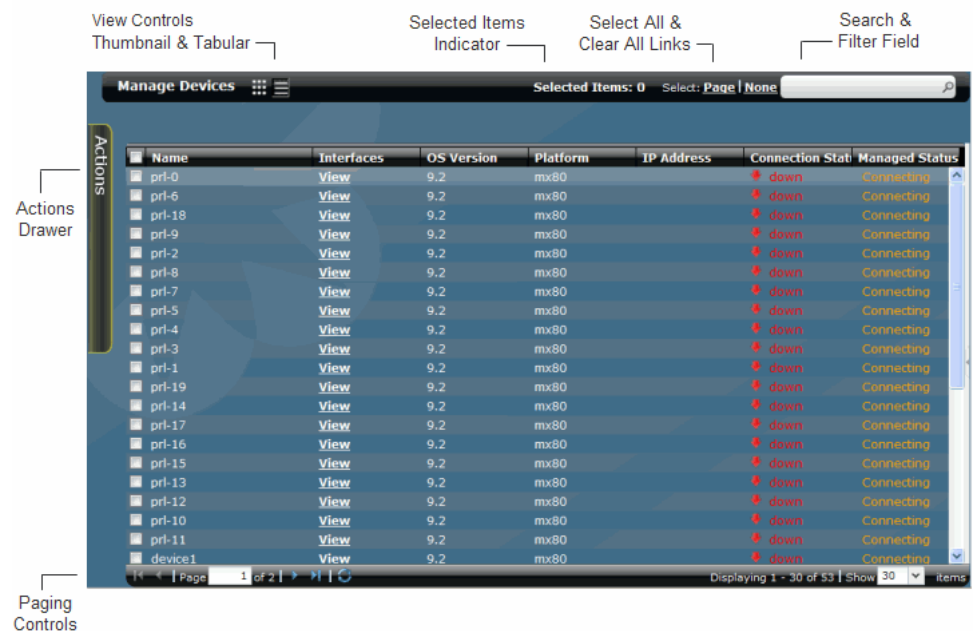
Figure 23 on page 30 shows the parts of the Manage Devices inventory page user interface in thumbnail view.

Figure 23: Manage Devices Inventory Page: Thumbnail View



Figure 24 on page 30 shows the parts of the Manage Devices inventory page user interface in tabular view.

Figure 24: Manage Devices Inventory Page: Tabular View



The following sections describe the parts of the inventory page user interface in more detail:

- [View Controls on page 31](#)
- [Sorted By Indicator on page 32](#)
- [Show or Hide Columns on page 32](#)
- [Zoom Slider on page 32](#)
- [Search and Filter Field on page 33](#)
- [Actions Drawer on page 33](#)
- [Paging Controls on page 34](#)

View Controls

The following sections describe the view controls in the inventory pages:

- [Thumbnail View on page 31](#)
- [Tabular View on page 31](#)

Thumbnail View

The default inventory page view—thumbnail view—displays icons of managed objects. Icons also include visual elements that display item status, type, operation, and so forth. For example in the Platform > Devices > Manage Devices inventory page, the green up arrow indicates the device is up; a red arrow indicates the device is down. In the Manage Service Definitions inventory page, a visual element in the object icon indicates whether a service definition is standard or custom.

Each object includes a title. You can also mouse over an object to see its title.

You must select an object to perform an action on it. Select objects by clicking the selection check box. You can select objects in a sequence or randomly. Use the Select Page or None links to select all or clear the selection of all objects at once.

Double-clicking an object in thumbnail view provides more detailed information. You can use the zoom slider to the right-most position to see more detailed information. The zoom slider provides three levels of information.

Tabular View

Tabular view displays managed objects on an inventory page as rows in a table. Data about each managed object appears in the table columns.

You must select an object to perform an action on it. Select objects by clicking the row check box. You can select objects in a sequence or randomly. Use the Select Page or None links to select all or clear the selection of all objects at once.

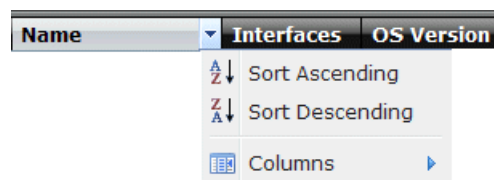
You can manipulate objects in tables by changing the width of columns, sorting columns, and hiding columns.

Sorted By Indicator

The Sorted by indicator in the inventory page banner displays how the objects are sorted in the tabular view. The Sorted by indicator appears in both the thumbnail and tabular views after you have sorted a column.

In tabular view, you can sort inventory data using the Sort Ascending and Sort Descending commands in the column header drop-down menu. Click the down arrow on a table header to view the sort menu. In [Figure 25 on page 32](#), the device inventory is sorted by the Name column.

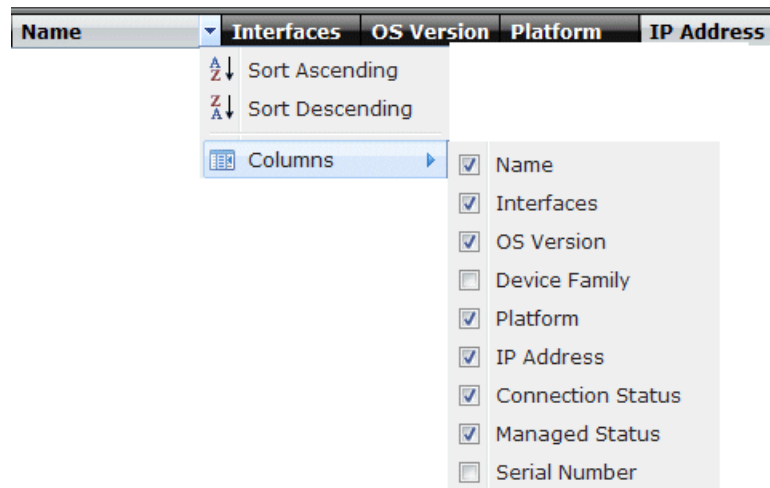
Figure 25: Sorting Tables



Show or Hide Columns

Hide table columns by deselecting the column name in the Columns Cascading menu, as shown in [Figure 26 on page 32](#). Only selected column names appear in the inventory table.

Figure 26: Showing or Hiding Columns in Tables



Zoom Slider

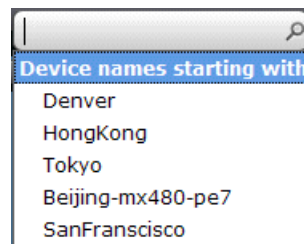
The zoom slider determines the size of the icons displayed on the screen and the amount of detailed information that appears. The zoom slider appears only in thumbnail view. The zoom slider provides two levels of zoom. The left level of zoom displays objects smaller on the inventory page and reduces the amount of paging. The right level of zoom provides detailed information about an object. The size of objects is persistent between work sessions.

Search and Filter Field

Use the Search and Filter text field on the right of the inventory page banner enables you to search for specific objects to display on the inventory page. Typing the first letter of an object displays the available names that start with that letter.

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

Figure 27: Search



You can create tags to categorize objects. For more information about tagging objects to select similar objects, see [“Tagging an Object” on page 495](#).

Clearing the contents in the Search box and pressing Enter, displays all the inventory objects on the page again.

Actions Drawer

You can perform actions on one or more selected items on an inventory page by using the Actions drawer or by right-clicking items. To use the actions in the Actions drawer, select one or more objects, mouse over the Actions drawer to open it, and select an action. The drawer opens and the actions that can be performed are displayed as shown. For example, to delete a device from the inventory, select that device in the Manage Devices inventory page, mouse over the Actions drawer, then click the Delete link. Move the cursor from the drawer to close it.

You can also select one or more items, then right-click. The right-click menu appears, which has the same action as the Actions drawer.



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

To ensure you can use the right-click menu:

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

Paging Controls

Figure 28 on page 34 shows the paging controls that appear at the bottom of the inventory page. You can use these controls to browse the inventory when the inventory is too large to fit on one page.

Figure 28: Page Information Bar



The Page box lets you jump to a specific page of managed objects. Type the page number in the Page box and press Enter to jump to that field. The Show box enables you to customize the number of objects displayed per page. Table 8 on page 34 describes other table controls.

Table 8: Table Paging and Refreshing Controls

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

- Related Documentation**
- [Junos Space User Interface Overview on page 11](#)
 - [Tagging an Object on page 495](#)

PART 2

Devices

- [Discovering Devices on page 39](#)
- [Adding Deployed Devices on page 51](#)
- [Device Management Overview on page 57](#)
- [Managing Devices on page 63](#)
- [Adding Devices and Connection Profiles on page 99](#)
- [Secure Console on page 121](#)
- [Device Adapters on page 133](#)
- [Discovering Topologies on page 145](#)

CHAPTER 3

Discovering Devices

- [Device Discovery Overview on page 39](#)
- [Discovering Devices on page 40](#)
- [Specifying Device Targets on page 48](#)
- [Specifying SNMP Probes on page 49](#)

Device Discovery Overview

You use device discovery to add devices to Junos Space. *Discovery* is the process of finding a device and then synchronizing the device inventory and configuration with the Junos Space database. To use device discovery, Junos Space must be able to connect to the device.

To discover network devices, Junos Space uses the SSH and SNMP protocols. Device authentication 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 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 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 uses Juniper Network's Device Management Interface (DMI), which is an extension to the NETCONF network configuration protocol.

When discovery succeeds, Junos Space creates an object in the Junos Space database to represent the physical device and maintains a connection between the object and the physical device so their information is linked.

When configuration changes are made in Junos Space, for example, when you deploy service orders to activate a service on your network devices, the configuration is pushed to the physical device.

When configuration changes are made on the physical device (out-of-band CLI commits and change-request updates), Junos Space automatically resynchronizes with the device so that the device inventory information in the Junos Space database matches the current device inventory and configuration information.

The following device inventory and configuration data is captured and stored in relational tables in the Junos Space 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 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
- Loopback interface

Other device configuration data is stored in the Junos Space database as binary large objects, and is available only to northbound interface (NBI) users.

Related Documentation

- [Discovering Devices on page 40](#)
- [Viewing Managed Devices on page 63](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 96](#)
- [Resynchronizing Managed Devices on page 80](#)
- [Device Management Overview on page 57](#)
- [Device Inventory Management Overview on page 62](#)
- [Managing DMI Schemas Overview on page 506](#)

Discovering Devices

You use device discovery to automatically discover and synchronize Junos OS devices in Junos Space. Device discovery is a three-step process in which you specify target devices, a probe method (ping or SNMP or both, or none), and credentials to connect to each device.



.....

NOTE: The values that you enter to specify the targets, probe method, and credentials are persistent from one discovery operation to the next, so you do not have to reenter information that is the same from one operation to the next.

.....

During device discovery, device license information is imported and stored in the Junos Space database, including:

- 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



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 manages the device and the redundancy. If the master Routing Engine fails, the backup Routing Engine takes over and Junos Space manages the transition automatically without bringing down the device.



NOTE: When you initiate discovery on a device, Junos Space automatically enables SSH and the NETCONF protocol over SSH by pushing the following commands to the device:

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

To discover and synchronize devices, complete the following tasks:

1. [Specifying Device Targets on page 41](#)
2. [Specifying Probes on page 43](#)
3. [Specifying Credentials on page 45](#)

Specifying Device Targets

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

1. From the navigation ribbon, select the **Devices** workspace.
2. From the navigation ribbon, click the Discover Devices icon.
Junos Space displays discovery status for discovery targets that are already processed.
3. From the navigation ribbon, click the Discover Targets icon.

The Discover Targets dialog box appears.

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 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.

4. 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.

5. Click **Browse**.

The CSV File Upload dialog box appears.

6. 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.

7. Click **Upload** to upload the selected CSV file.

8. 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.

9. 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.

10. 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 to discover, click **Add**.

The Discover Targets Dialog box displays the addresses of the configured device targets.

11. Click **Discover** from the Discover Targets dialog box.



NOTE: You need to navigate through the Specify Probes and Specify Credentials dialog boxes before you click the **Discover** button.

In the next task, you specify a probe method to connect to and discover the device targets.

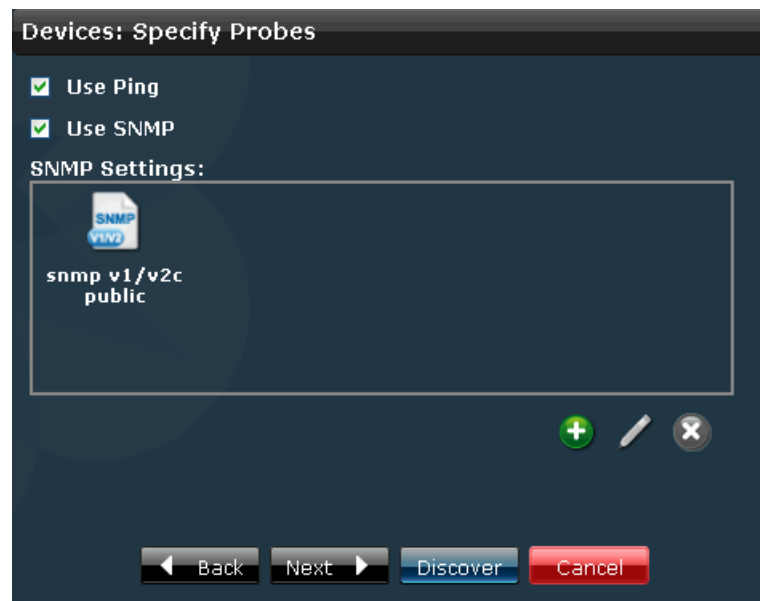
Specifying Probes

To configure the method Junos Space uses to discover the device targets:

1. From the navigation ribbon, select the **Devices** workspace, and then click the Discover Devices icon.
2. From the navigation ribbon, click the Specify Probes icon.

The Specify Probes dialog box appears, as shown in [Figure 29 on page 43](#).

Figure 29: Specify Probes Dialog Box



3. 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 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 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 can discover the target device more quickly, if the device is pingable and SNMP is enabled on the device.

4. Click the Add icon (+).

An Add SNMP Settings dialog box appears.

5. [Figure 30 on page 44](#) shows the Add SNMP Settings dialog box when you select **SNMP V1/V2C**. If you make this selection, specify a community string, which can be **public**, **private**, or a predefined string.

Figure 30: Add SNMP Settings Dialog Box (SNMP V1/V2C)

[Figure 31 on page 44](#) shows the Add SNMP Settings dialog box when you select **SNMP V3**.

Figure 31: Add SNMP Settings Dialog Box (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.

Click **Add** to save the SNMP settings, or click **Add More** to add additional configurations. After using **Add More**, click **Add** to save the settings and close the dialog box.

The Specify Probes dialog box (Figure 29 on page 43) displays the configured SNMP settings.

6. Click **Discover** in the Specify Probes dialog box.

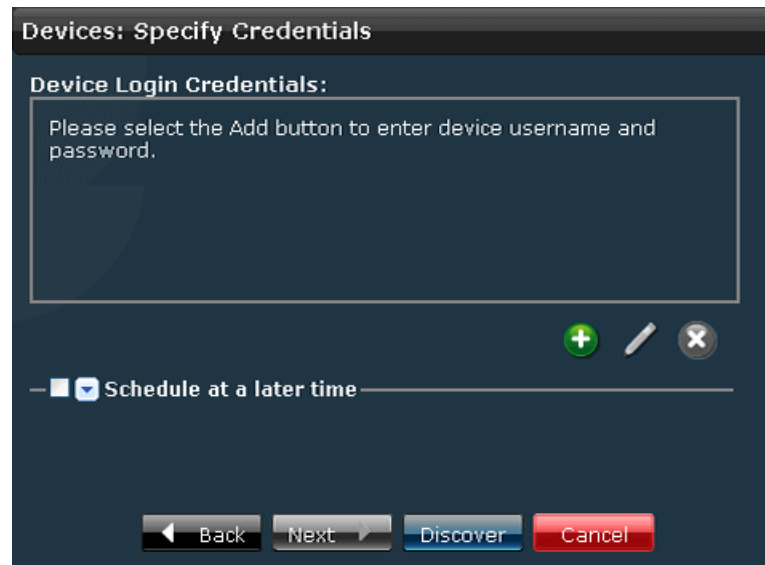
Specifying Credentials

Specify an administrator name and password to establish the SSH connection for each target device that you configured:

1. From the navigation ribbon, select the **Devices** workspace, and then click the Discover Devices icon.
2. From the navigation ribbon, select the Specify Credentials icon.

The Specify Credentials dialog box appears, as shown in Figure 32 on page 45.

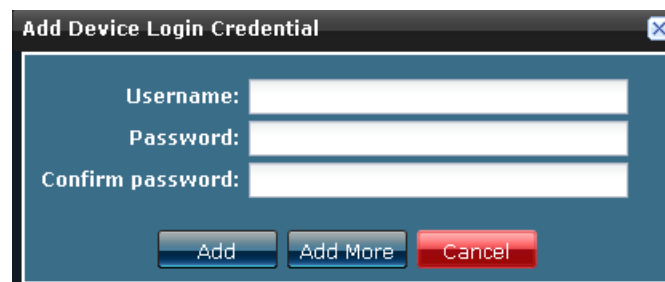
Figure 32: Specify Credentials Dialog Box



3. Click the Add icon.

The Add Device Login Credential dialog box appears, as shown in Figure 33 on page 45.

Figure 33: Add Device Login Credential



4. 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 clicking **Add** or **Add More** to add another username and password. If you use Add More, click **Add** after you have finished adding all login credentials.

The Credential dialog box displays the administrator user names that you configured.

5. 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.

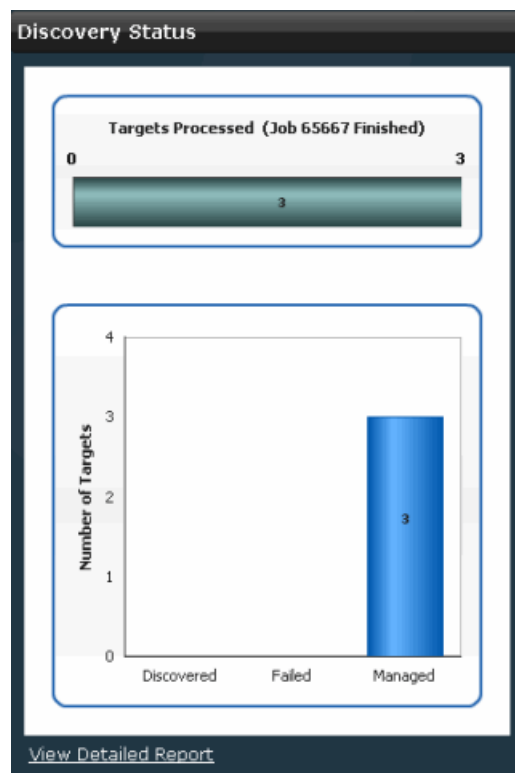


NOTE: The selected time in the scheduler corresponds to Junos Space server time but is mapped to the local time zone of the client computer.

6. Click **Discover** to start the discovery job.

The Discovery Status report appears, as shown in [Figure 34 on page 46](#). 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.

Figure 34: Discovery Status Report



7. To view device discovery details, click **View Detailed Report**.

The report, shown in [Figure 35 on page 47](#), displays the IP address, hostname, and discovery status for discovered devices.

Figure 35: Device Discovery Detailed Report

Devices			
IP Address	Hostname	Status	Description
10.155.69.22	Tokyo	Device Managed	
10.155.69.23	HongKong	Device Managed	
10.155.69.24	Denver	Device Managed	

Page 1 of 1 | Displaying 1 - 3 of 3



NOTE: If the discovery operation fails, the Description column in the Detailed Report table indicates the cause of failure.

You can also view the device discovery job in the Jobs workspace.

To view device discovery from the Jobs workspace:

1. From the navigation ribbon, select the Jobs workspace.
2. From the navigation ribbon, select the Manage Jobs icon.
3. From the Job Manager inventory page, enter **Discover Network Elements** in the search box to view device discovery jobs. [Figure 36 on page 47](#) shows a table view of Discover Network Elements jobs.

Figure 36: Job Report: Discover Network Elements Job

Manage Jobs					
Sorted by Job Type					
Percent	State	Job Type	ID	Summary	Scheduled Start Time
100.0	SUCCESS	Discover Network Elements	13107	Number of scanned IP: 1 Number of Discovery succeeded: 1 Number of Add Device failed: 0 Number of Already Managed: 0 Number of Skipped: 0 Number of Device Managed: 1	Mar 6, 2010 12:07:22 AM PST
100.0	SUCCESS	Discover Network Elements	65536	Number of scanned IP: 1 Number of Already Managed: 0 Number of Skipped: 0 Number of Discovery succeeded: 1 Number of Device Managed: 1 Number of Juniper Device but Add device failed: 0	Mar 5, 2010 6:03:56 PM PST

Page 1 of 1 | Displaying 1 - 7 of 7 | Show 30 items

Related Documentation

- [Viewing and Exporting Device License Inventory on page 91](#)
- [Viewing Managed Devices on page 63](#)

- [Viewing Scheduled Jobs on page 347](#)
- [Resynchronizing Managed Devices on page 80](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 96](#)
- [Viewing Hardware Inventory for Devices on page 75](#)
- [Viewing Physical Interfaces for Devices on page 78](#)
- [Managing DMI Schemas Overview on page 506](#)

Specifying Device Targets

To discover a topology using Junos Space Topology Discovery, you must first specify a device target. This device acts as a seed device in initiating a topology discovery. You can also begin a topology discovery by using subnets as targets or seeds.

To specify device targets:

1. From the navigation ribbon, select **Topology Visualization > Discover Topology > Specify Target**.

The Specify Targets dialog box appears, as shown in [Figure 37 on page 48](#).

2. Perform one or more of the following actions:
 - Select the **Include Managed Devices as Targets** check box if you want Junos Space to use Junos OS managed devices as the target devices for topology discovery.
 - Add, edit, or delete device targets. See “[Managing Device Targets](#)” on page 149.

Figure 37: Specify Device Targets



- Related Documentation**
- [Topology Discovery Overview on page 145](#)
 - [Specifying SNMP Probes on page 49](#)

Specifying SNMP Probes

Junos Space uses SNMP to discover network elements that are connected to the specified seed devices and subnets. The Junos Space server contacts the targeted devices in the specified subnets and gets the relevant management information base (MIB) information that is needed for computing the topology.

You can also specify a hop count to limit the number of routers from the seed device that you want Junos Space to discover. If the hop count is 1, the Junos Space server takes the IP addresses present in the IP routing tables of all the initially targeted devices and considers them for further discovery. This process is repeated based on the hop count value that you specified.

For example, if a device X is targeted for discovery with hop count as 1, then all the IP addresses present in the routing table of device X are targeted for discovery. If the hop count is 2, then all the IP addresses present in the routing tables of the devices whose IP addresses were in the routing table of device X are also targeted for discovery.

To use SNMP to probe devices as part of topology discovery, make sure that SNMP is enabled on the devices in the network with appropriate read-only version 1, version 2, or version 3 credentials.

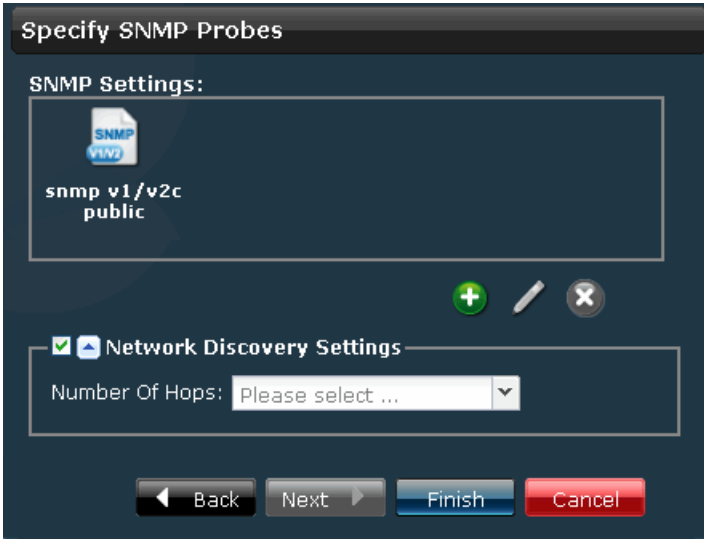
To configure SNMP settings:

1. From the navigation ribbon, select **Topology Visualization > Discover Topology > Specify SNMP Probes**.

The **Topology Visualization Workspace: SNMP Probes** dialog box appears, as shown in [Figure 38 on page 50](#).

2. Perform one or more of the following actions:
 - Add, edit, or delete SNMP probes that specify how Junos Space discovers the network. For more information, see [“Managing SNMP Probes” on page 151](#).
 - Specify a hop count to limit the number of routers from the target that Junos Space tries to discover. Select the **Network Discovery Settings** check box and select the number of hops from the Number of Hops list.

Figure 38: Specify SNMP Probes



The dialog box titled "Specify SNMP Probes" contains the following elements:

- SNMP Settings:** A section with a dark blue background containing an SNMP icon and the text "snmp v1/v2c" and "public".
- Network Discovery Settings:** A section with a light blue background containing a checked checkbox, a small icon, and the text "Network Discovery Settings". Below this is a label "Number Of Hops:" followed by a dropdown menu showing "Please select ...".
- Buttons:** At the bottom are four buttons: "Back" (with a left arrow), "Next" (with a right arrow), "Finish" (in blue), and "Cancel" (in red).

- Related Documentation**
- [Topology Discovery Overview on page 145](#)
 - [Specifying Device Targets on page 48](#)

CHAPTER 4

Adding Deployed Devices

- [Add Deployed Devices Wizard Overview on page 51](#)
- [Adding Deployed Devices on page 52](#)
- [Managing Deployed Devices on page 54](#)

Add Deployed Devices Wizard Overview

Network devices deployed on the network can be easily managed by Junos Space using the Discover Devices task. However, for security devices, SSH and ping are disabled on the device interface for any incoming traffic. Hence, security devices cannot communicate with Junos Space. In such instances, you can use the Add Deployed Devices Wizard to enable communication between security devices and Junos Space. The Add Deployed Devices Wizard creates a Task Instance that you can use to obtain management CLI commands related to these devices. These CLI commands can be pasted on the device console, enabling the device to connect to Junos Space for further management.

You can create Task Instances either manually or by uploading a comma-separated values (CSV) file. You need to specify the following details to create a Task Instance:

- Device name
- Device platform
- OS version
- Device count
- Authentication details

You can store the management CLI commands obtained from a Task Instance and paste it on the device console or on a command-line session on the device.

**NOTE:**

If you are using Internet Explorer to download the management CLI commands, you must customize the browser settings to download them. Perform the following steps to customize the Internet Explorer settings:

1. Open Internet Explorer and select **Tools > Internet Options**.
2. Click the **Security** tab and select the **Custom Level** tab.
3. In the Automatic prompting for file downloads section, click the **Enable** option button.

Related Documentation

- [Adding Deployed Devices on page 52](#)
- [Managing Deployed Devices on page 54](#)
- [Managing DMI Schemas Overview on page 506](#)

Adding Deployed Devices

To create a Task Instance:

1. From the navigation ribbon, select **Devices > Add Deployed Devices**.

The Add Deployed Devices inventory page displays icons for all the Task Instances.

2. From the navigation ribbon, select the Add Device icon. You can use this to add branch ScreenOS devices.

The Add Devices dialog box appears, as shown in [Figure 39 on page 52](#).

Figure 39: Add Devices Dialog Box

3. In the Name box, enter a name for the new Task Instance.
4. In the Description box, enter a description for the new Task Instance.
5. You can add a new Task Instance either by importing a CSV file or manually.

To add a new Task Instance by importing a CSV file:

- a. Select the **Import to CSV** option button.
- b. Select the **View Sample CSV** link in the Import section to see a sample of the CSV file that should be uploaded.
- c. Save the sample CSV file to your storage location.
- d. Make necessary changes in this CSV file and rename it with an appropriate name.

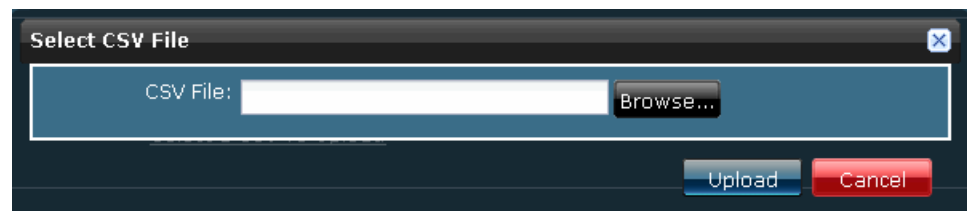


NOTE: Do not add or delete any columns in the CSV file. You cannot upload the CSV file successfully if you add or delete any columns.

- e. Select the **Select a CSV To Upload** link in the Import section.

The **Select CSV File** dialog box appears, as shown in [Figure 40 on page 53](#).

Figure 40: Selecting a CSV File to Upload



- f. Click **Browse** and upload the CSV file from your storage location.
- g. If the CSV file is successfully uploaded, a Green mark appears next to the Select a CSV To Upload link.

The Upload dialog box appears.

- h. Click **OK**.

To add a new Task Instance manually:

- a. Select the **Add Manually** option button.
- b. Enter the following details in the Device Details section:
 - From the Platform list, select an appropriate platform.
 - From the OS Version list, select an appropriate OS version.
 - In the Number of devices box, enter the number of devices with the same platform and OS version.





NOTE: If you add multiple devices, a unique numerical identifier is appended at the end of each device name.

- c. In the Authentication Details section:

- In the Username box, choose an appropriate user name.
 - In the Password box, enter a password.
 - In the Re-enter Password box, reenter the password.
6. Click **Next**.
 7. This wizard page displays rows that make up the configured Task Instance. Select a row or rows and use the icons described in [Table 9 on page 54](#) to view or download management CLI commands.

Table 9: Icons to View or Download Management CLI Commands

Icon	Description
	View the management CLI commands.
	Download the management CLI commands.

8. Click **Finish**.
The new Task Instance you have added appears in the Add Deployed Devices inventory page. A new job is created and the job ID appears in the Job Information dialog box.
9. Click the job ID to view more information about the job created.
This action directs you to the Job Management workspace.

Related Documentation

- [Add Deployed Devices Wizard Overview on page 51](#)
- [Managing Deployed Devices on page 54](#)
- [Managing DMI Schemas Overview on page 506](#)

Managing Deployed Devices

Task Instances are listed in the Add Deployed Devices inventory page. You can view or download the management CLI commands associated with Task Instances. You can also view the device instance status or delete Task Instances.

This topic describes the following tasks related to Task Instances and management CLI commands:

- [Viewing the Details of a Task Instance on page 55](#)
- [Viewing the Device Status on page 55](#)
- [Deleting a Task Instance on page 55](#)
- [Downloading Management CLI Commands on page 55](#)

Viewing the Details of a Task Instance

To view the details of a Task Instance:

1. From the navigation ribbon, select **Devices > Add Deployed Devices**.
The Add Deployed Devices inventory page appears.
2. Double-click the icon for the Task Instance whose details you intend to view.
The details of the Task Instance are displayed in the Add Instance Details dialog box.
3. Click **Close** to close the Add Instance Details dialog box.

Viewing the Device Status

To view the device status:

1. From the navigation ribbon, select **Devices > Add Deployed Devices**.
The Add Deployed Devices inventory page appears.
2. Select the Task Instance you intend to view the device status for and click the **View Device Status** link from the Actions drawer in the top-left corner of the inventory page.
A new dialog box displays the connection status and managed status of the devices.
3. Click **Back** on the top-left corner to return to the inventory page.

Deleting a Task Instance

To delete a Task Instance you have created:

1. From the navigation ribbon, select **Devices > Add Deployed Devices**.
The Add Deployed Devices inventory page appears.
2. Select the Task Instance you intend to delete and click the **Delete** link from the Actions drawer in the top-left corner of the inventory page.
The Delete Instance dialog box appears.
3. Select the Task Instance you want to delete and click **Delete**.

Downloading Management CLI Commands

To download management CLI commands from the Task Instance you have created:

1. From the navigation ribbon, select **Devices > Add Deployed Devices**.
The Add Deployed Devices inventory page appears.
2. Select the Task Instance containing the management CLI commands you intend to download and click the **Download Management CLIs** link from the Actions drawer in the top-left corner of the inventory page.
The Download Management CLIs dialog box appears.

3. Click the **Download Management CLIs** link.
4. Save the .zip file in your local host.

**Related
Documentation**

- [Add Deployed Devices Wizard Overview on page 51](#)
- [Adding Deployed Devices on page 52](#)
- [Managing DMI Schemas Overview on page 506](#)

CHAPTER 5

Device Management Overview

- [Device Management Overview on page 57](#)
- [Viewing Device Statistics on page 58](#)
- [Device Inventory Management Overview on page 62](#)

Device Management Overview

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

From the Devices workspace, you use device discovery to discover devices and synchronize device configurations with the Junos Space database. You can use device discovery to discover one or many devices at a time. After Junos Space discovers your network devices, you can perform the following tasks to monitor and configure devices from Junos Space:

- 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.
- Resynchronize a managed device to resynchronize the device configuration in the Junos Space database with the physical device.
- Deploy service orders to activate a service on your network devices.
- Troubleshoot devices.

Related Documentation

- [Device Discovery Overview on page 39](#)
- [Device Inventory Management Overview on page 62](#)
- [Discovering Devices on page 40](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 96](#)
- [Viewing Managed Devices on page 63](#)

- [Viewing and Exporting Device License Inventory on page 91](#)
- [Troubleshooting Devices on page 94](#)

Viewing Device Statistics

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

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

To view device statistics, select the Platform > Devices workspace.

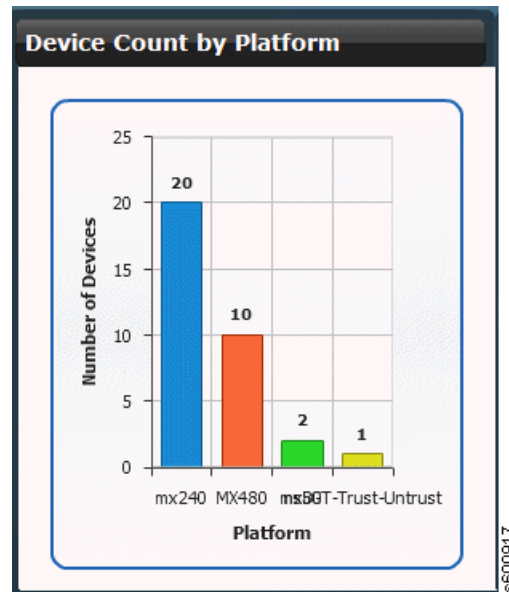
This topic includes the following tasks:

- [Viewing the Number of Devices by Platform on page 59](#)
- [Viewing Connection Status for Devices on page 59](#)
- [Viewing Devices by Junos OS Release on page 60](#)

Viewing the Number of Devices by Platform

Figure 41 on page 59 shows the Device Count by Platform report. The bar chart shows the number of Juniper Networks devices on the y axis discovered by platform type on the x axis. Each vertical bar in the chart displays the number of managed devices for a platform.

Figure 41: Device Count by Platform Report



To view more detailed information about devices per platform:

- Click a bar in the bar graph. The Manage Devices inventory page appears filtered by the device type you selected. See [“Viewing Managed Devices” on page 63](#).

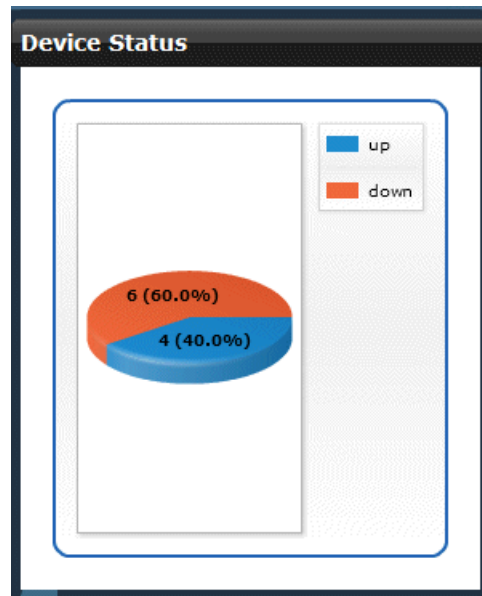
To save the bar chart as an image or to print for presentations or reporting:

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

Viewing Connection Status for Devices

Figure 42 on page 60 shows the Device Status report. The pie chart displays the percentage and number of devices that are connected and disconnected on the network. The up or down status is expressed as a percentage of the total number of devices.

Figure 42: Device Status Report



To view more detailed device status information:

- Click a slice in the pie chart. The Manage Devices inventory page appears filtered by the devices that are up or down. See "[Viewing Managed Devices](#)" on page 63.

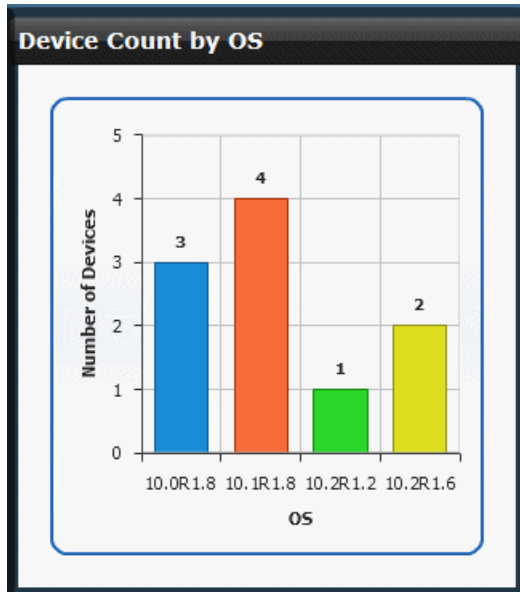
To save the pie chart as an image or to print for presentations or reporting:

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

Viewing Devices by Junos OS Release

Figure 43 on page 61 shows the Device Count by OS report. The bar chart shows the number of Juniper Networks devices on the network (the y axis) categorized by running a certain Junos OS release (the x axis).

Figure 43: Device Count by OS Report



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

- Click a bar in the chart. The Manage Devices inventory page appears. See [“Viewing Managed Devices” on page 63](#).

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

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

Related Documentation

- [Viewing Managed Devices on page 63](#)
- [Viewing Hardware Inventory for Devices on page 75](#)
- [Discovering Devices on page 40](#)

Device Inventory Management Overview

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

- List the device inventory to view information about the hardware and software components of each device that Junos Space manages.
- View information about the service contract or end-of-life status for a part.
- View the operational and administrator status for the physical interfaces on which devices are run.
- Change credentials for a device.
- Export the device inventory information for use in other applications, such as those used for asset management.
- Troubleshoot a device.
- Resynchronize the network devices managed by Junos Space.

The device inventory in the Junos Space database is generated when the device is first discovered and synchronized in Junos Space. After a device is synchronized, the device inventory in the Junos Space 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 database. However, Junos Space automatically triggers a resync job when a configuration change request commit or out-of-band CLI commit occurs on a managed device.

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

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

Related Documentation

- [Device Management Overview on page 57](#)
- [Device Discovery Overview on page 39](#)
- [Viewing Hardware Inventory for Devices on page 75](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 96](#)
- [Resynchronizing Managed Devices on page 80](#)
- [Exporting Device Inventory Information on page 87](#)
- [Viewing and Exporting Device License Inventory on page 91](#)
- [Troubleshooting Devices on page 94](#)

CHAPTER 6

Managing Devices

- [Viewing Managed Devices on page 63](#)
- [Editing Device Configuration Overview on page 68](#)
- [Selecting the Device and the Configuration Perspective on page 69](#)
- [Editing Device Configuration Options on page 70](#)
- [Finalizing Device Configuration Changes on page 72](#)
- [Viewing Change Requests on page 74](#)
- [Viewing Hardware Inventory for Devices on page 75](#)
- [Viewing Physical Interfaces for Devices on page 78](#)
- [Deleting Devices on page 79](#)
- [Resynchronizing Managed Devices on page 80](#)
- [Changing Login Credentials for Managed Devices on page 82](#)
- [Displaying Service Contract and EOL Data in the Physical Inventory Table on page 84](#)
- [Exporting Device Inventory Information on page 87](#)
- [Viewing and Exporting Device License Inventory on page 91](#)
- [Troubleshooting Devices on page 94](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 96](#)

Viewing Managed Devices

You can view operating system, platform, IP-address, license, and connection status information for all the managed devices in your network. Device information can be viewed graphically or in a table. By default, Junos Space displays thumbnail representations of devices.

You can also view managed devices from the Network Monitoring workspace, via the Node List (see [“Viewing the Node List” on page 287](#)). The Network Monitoring workspace also enables you to resync your managed devices (see [“Resyncing Nodes” on page 288](#)).

- [Viewing Devices as Graphics on page 64](#)
- [Viewing Devices in a Table on page 65](#)

Viewing Devices as Graphics

You can view thumbnails, summary information, and detailed information about the devices managed by Junos Space.




To view the managed devices:

1. From the navigation ribbon, select the **Devices** workspace.
2. From the navigation ribbon, select the Manage Devices icon.

The inventory page displays thumbnails of managed devices by name and IP address.

Above each thumbnail, an icon indicates whether the device is connected (up) or down. [Table 10 on page 64](#) describes the connection status icons.

Table 10: Device Connection Status Icon

Icon	Description
	<p>Connection is up—The device is connected to Junos Space and is running properly.</p> <p>NOTE: Before you can update a device from Junos Space (deploy service orders), the device connection must be up.</p>
	<p>Out of sync—The device is connected to Junos Space but the device configuration in the Junos Space database is out of sync with the physical device.</p>
	<p>Connection is down—The device is not currently connected to Junos Space or an event has occurred, either manually by an administrator or automatically by the flow of a type of traffic, that has stopped the device from running.</p>

3. 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 summary information for a device, select the device in the inventory page and drag the zoom slider to the rightmost position.

Junos Space displays information about the selected device, including OS version, platform, IP address, connection status, and managed status.

For SRX Series devices that are configured as a chassis cluster, Junos Space displays a cluster icon and indicates whether the device is the primary or secondary device, as shown in the following example.

Figure 44: Inventory Page: SRX Chassis Cluster



- To view hardware inventory information for a device, double-click the thumbnail or select the device, and click **View Physical Inventory** from the Actions drawer.

Viewing Devices in a Table

To view configuration and run-time information for devices in a table:

- From the navigation ribbon, select the **Devices** workspace.
- Click the Table icon in the filter bar, as shown in the following example.

Figure 45: Table Icon



Junos Space displays a table of devices in the inventory page.

Figure 46: Device Table

Name	Interfaces	OS Version	Platform	IP Address	Connection Status	Managed Status
<input checked="" type="checkbox"/> SanFrancisco	View	10.1R1.1	MX960	10.155.69.13	up	In Sync
<input type="checkbox"/> SanJose	View	10.1R1.7	MX240	10.155.69.12	up	In Sync
<input type="checkbox"/> coyotes	View	9.6R3.2	J6350	10.155.77.217	up	In Sync

At the bottom of the table, there is a pagination bar showing 'Page 1 of 1', 'Displaying 1 - 3 of 3', and 'Show 30 items'.

Table 11 on page 66 describes the fields displayed in the inventory window.

Table 11: Fields in the Manage Devices Table

Field	Description
Name	The device configuration name.
Interfaces	Link to the view of physical interfaces for the device.
OS Version	Operating system firmware version running on the device.
Platform	Model number of the device.
IP Address	IP address of the device.
Connection Status	<p>Connection status of the device in Junos Space.</p> <ul style="list-style-type: none"> up—Device is connected to Junos Space. When connection status is up, the managed status is Out of Sync, Synchronizing, In Sync, or Sync Failed. down—Device is not connected to Junos Space. When Connection status is down, the managed status is None or Connecting.
Managed Status	<p>Current status of the managed device in Junos Space:</p> <ul style="list-style-type: none"> Connecting— Junos Space has sent connection RPC and is waiting for first connection from device. In Sync—Sync operation has completed successfully, and Junos Space and the device are synchronized. None—Device is discovered, but Junos Space has not yet sent connection RPC. Out of Sync—Device has connected to Junos Space, but the sync operation has not been initiated, or an out-of-band configuration change on the device was detected and auto-resync is disabled or has not yet started. 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.
Device Family (not displayed by default)	Device family of the selected device.
Serial Number (not displayed by default)	Serial number of the device chassis.

- 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**.

4. Show columns not in the default table view or hide columns as follows:
 - a. Mouse over any column header and click the down arrow.
 - b. Select **Columns** from the menu, as shown in the following example.

Figure 47: Selecting Columns



- c. Select the check boxes for columns that you want to view. Clear the check boxes for columns that you want to hide.
5. 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, double-click the table row for the device or select the row for the device, and click **View Physical Inventory** from the Actions drawer.
 - To view the physical interfaces for a device, select the row for the device, and click **View Interfaces** from the Actions drawer.

Related Documentation

- [Viewing Device Statistics on page 58](#)
- [Viewing Hardware Inventory for Devices on page 75](#)
- [Viewing and Exporting Device License Inventory on page 91](#)
- [Viewing Physical Interfaces for Devices on page 78](#)
- [Discovering Devices on page 40](#)
- [Viewing the Node List on page 287](#)
- [Resyncing Nodes on page 288](#)

Editing Device Configuration Overview

This action enables you to view and edit a device's configuration. You can deploy the new configuration immediately, save it as a change request, or schedule it for later.

To display all of a device's configuration options, Junos Space requires the DMI schema for that device type. To upload a DMI schema to Junos Space, see [“Managing DMI Schemas Overview” on page 506](#).

If Junos Space 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 to let you edit all of the device's configuration options. If Junos Space uses the default schema, it is possible that some already configured parameters on the device will not be displayed.

Junos Space checks for an exact match between device and DMI schema every time you edit the device's configuration.

Editing device configuration relates to three types of device configuration files:

- Running configuration—The current running configuration.
- Candidate configuration—The future running configuration, which is saved as a change request until you deploy it or create another candidate configuration. If you create a second candidate configuration, the first (undeployed,) candidate configuration, is overwritten.
- Backup configuration—The copy of the running configuration created by a commit command applied to a candidate configuration. All former running configurations are saved in the change request history.

When you edit a device configuration, you are creating a candidate configuration file. When you deploy the candidate, you are creating a new running-configuration file and a backup configuration file.

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

1. [Selecting the Device and the Configuration Perspective on page 69](#)
2. [Editing Device Configuration Options on page 70](#)
3. [Finalizing Device Configuration Changes on page 72](#)

Although Junos OS devices can maintain up to 49 copies of a configuration file, Junos Space also provides database management of configuration files.

Related Documentation

- [Managing Configuration Files Overview on page 326](#)
- [Viewing Change Requests on page 74](#)
- [Managing DMI Schemas Overview on page 506](#)

Selecting the Device and the Configuration Perspective

The Edit Device Configuration page shows the DMI schema applied by Junos Space to the selected device. If Junos Space has the same DMI schema as the device, then that schema will be applied. If Junos Space does not, then it displays the default schema for the selected device's type. The default schema does not necessarily show all of the configuration options available in the actual device schema. Therefore you cannot configure those options using Junos Space; you must go to the device itself. To avoid this situation, upload the device's schema to Junos Space using the DMI Schema management workspace (see [“Managing DMI Schemas Overview” on page 506](#)).

This topic describes how to view the device configuration before editing it.

To select the device and the perspective:

1. Navigate to **Devices > Manage Devices**, and select a single device.
2. Select **Edit Device Configuration** from the Actions drawer.

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

3. Explore the configuration details in the following ways:
 - Use the expander buttons (plus and minus) to explore the Junos OS statement hierarchy.
 - Mouse over the blue information icon next to each Junos OS statement to display explanatory text. The information is the same as that in the device CLI.
 - See which configuration options in the hierarchy are actually set by selecting **Configured Data** from the Perspective list on the top of the left pane next to the magnifying glass search icon.
 - Likewise, in the right pane, select the **Show configured data only** check box on the title bar at the right to display in the right pane only those options that are actually configured.
 - Search for a particular option. See [“Finding Configuration Options” on page 174](#). Although that topic deals with Device Templates, the principle is exactly the same.

Related Documentation

- [Editing Device Configuration Overview on page 68](#)
- [Editing Device Configuration Options on page 70](#)
- [Finalizing Device Configuration Changes on page 72](#)
- [Updating a DMI Schema on page 508](#)

Editing Device Configuration Options

This topic describes the individual operations in editing a device configuration after you have selected your device and the perspective.

To edit a configuration option:

1. Select a configuration option in 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 in the title bar on the right pane.

The way the parameters in a configuration option are displayed varies depending on the option's data type. 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.

For example, tables are shown as rows that can be manipulated as follows:

- Edited by selecting a row and clicking the diagonal pencil icon
- Added by clicking the plus icon
- Deleted by selecting a row and clicking 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 on the correlation between data types and validation methods, see [“Defining the Operator's View” on page 167](#). For more detailed instructions on how to handle entering your parameters, consult [“Specifying Default Values for Configuration Options” on page 194](#). Although both these topics deal with Device Templates instead of editing device configuration, both features use basically the same displays. Note that when editing a device configuration you are not entering a default value but the actual value.

A parameter available for configuration is usually displayed as a link called Click to Configure.

2. Click the appropriate link. Keep clicking until you arrive at the parameter you want to change.
3. Make your change(s).

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 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.

4. Continue to either make changes or to do any or none of the following tasks:

- (Optional) Click **Preview** to see how your changes would look on the device CLI.

The View Device Configuration Changes page appears, displaying in XML format all the parameters you changed.



NOTE: All changes are displayed, not just the one you are currently working on.

Click **Close** to return to the device configuration editor.

- (Optional) Click **Validate** to perform the configuration validation check.

The Validate Device Configuration Changes dialog box appears, asking that you wait while the configuration is being validated on the device. When it has finished, the device validation status appears, announcing success or failure.



TIP: To avoid not knowing which parameter in a complex configuration change caused the validation to fail, make your changes one by one, validating after each one.

Click **Close** to return to the device configuration editor.

- Click **Cancel** to cancel the editing operation without making any changes.

You can also use the Preview and Validate buttons for configurations that you have not changed.

5. Click **Finish**.

The Finalize Device Configuration Changes dialog box appears.

6. Choose one of the following:

- **Save as Change Request** (default setting).

Select this option and click **OK**.

The item appears in the Change Request list for that device. See [“Viewing Change Requests” on page 74](#).

- **Deploy now**

Select this option and click **OK**.

The Deploy Configuration Changes Job dialog box appears.

a. Click the job ID to view details.

The Manage Jobs dialog box appears, filtered to display your job. See [“Job Management Overview” on page 341](#).

b. Click **OK** to return to the Manage Devices page.

The Manage Devices page appears. The device you edited is now unselected.

- **Deploy later**

- a. Choose the date and time.

The time zone is determined by the setting on the Junos Space server. If you choose a time or date that is in the past, a little red exclamation mark icon appears. Mouse over it to see the warning.

- b. Click **OK**.

The Deploy Configuration Changes Job Information dialog box appears.

- Click the job ID to view details.

The Manage Jobs dialog box appears, filtered to display your job. See [“Job Management Overview” on page 341](#).

- Click **OK** to return to the Manage Devices page.

The Manage Devices page appears. The device you edited is now unselected.

**Related
Documentation**

- [Editing Device Configuration Overview on page 68](#)
- [Selecting the Device and the Configuration Perspective on page 69](#)
- [Finalizing Device Configuration Changes on page 72](#)
- [Managing DMI Schemas Overview on page 506](#)

Finalizing Device Configuration Changes

After editing your device configuration, you can finalize your changes.

To finalize your device configuration changes:

1. Do any, all, or none of the following tasks:

- (Optional) Click **Preview** to see how your changes would look on the device CLI.

The View Device Configuration Changes page appears, displaying in XML format all the parameters you changed.



NOTE: All changes are displayed, not just the one you are currently working on.

Click **Close** to return to the device configuration editor.

- (Optional) Click **Validate** to perform the configuration validation check.

The Validate Device Configuration Changes dialog box appears, asking that you wait while the configuration is being validated on the device. When it has finished, the device validation status appears, announcing success or failure.



TIP: To avoid not knowing which parameter in a complex configuration change caused the validation to fail, make your changes one by one, validating after each one.

Click **Close** to return to the device configuration editor.

- Click **Cancel** to cancel the editing operation without making any changes.

You can also use the Preview and Validate buttons for configurations that you have not changed.

2. Click **Finish**.

The Finalize Device Configuration Changes dialog box appears.

3. Choose one of the following:

- **Save as Change Request** (default setting).

Select this option and click **OK**.

The item appears in the Change Request list for that device. See [“Viewing Change Requests” on page 74](#).

- **Deploy now**

Select this option and click **OK**.

The Deploy Configuration Changes Job dialog box appears.

a. Click the job ID to view details.

The Manage Jobs dialog box appears, filtered to display your job. See [“Job Management Overview” on page 341](#).

b. Click **OK** to return to the Manage Devices page.

The Manage Devices page appears. The device you edited is now unselected.

- **Deploy later**

a. Choose the date and time.

The time zone is determined by the setting on the Junos Space server. If you choose a time or date that is in the past, a little red exclamation mark icon appears. Mouse over it to see the warning.

b. Click **OK**.

The Deploy Configuration Changes Job Information dialog box appears.

- Click the job ID to view details.

The Manage Jobs dialog box appears, filtered to display your job. See [“Job Management Overview” on page 341](#).

- Click **OK** to return to the Manage Devices page.

The Manage Devices page appears. The device you edited is now unselected.

- Related Documentation**
- [Editing Device Configuration Overview on page 68](#)
 - [Selecting the Device and the Configuration Perspective on page 69](#)
 - [Editing Device Configuration Options on page 70](#)
 - [Viewing Change Requests on page 74](#)

Viewing Change Requests

Change requests are generated when you edit a device configuration and save the edits instead of deploying them immediately or scheduling deployment. See [“Finalizing Device Configuration Changes” on page 72](#).

This topic includes the following tasks:

- [Viewing Change Requests on page 74](#)
- [Adding, Modifying, or Deleting a Change Request on page 75](#)

Viewing Change Requests

To view a change request:

1. Navigate to **Devices > Manage Devices**.

The list of managed devices appears on the Manage Devices inventory page. See [“Viewing Managed Devices” on page 63](#).

2. Select a single device, mouse over the Actions drawer, and select **View Change Requests**.

The list of change requests for the selected device appears in the form of a table.

The table displays the following column headings:

- **Checkbox**—When checked, it selects all entries in the table.
 - **Description**—The value of the changed parameter. Note that this value is likely to be ambiguous without the context of the parameter name and the schema path: for example, one schema path for the parameter name “Description” is “configuration/snmp/description.”
 - **Created By**—The name of the person who edited the configuration to produce the change request.
 - **Creation Time**—The time at which the change request was created.
 - **Last Updated By**—The name of the person who updated the original change request.
 - **Last Update Time**—The time at which the update was made.
 - **Schedule Status**—The status, including scheduled, unscheduled, or in progress.
3. Click **Return to Inventory View**.

Adding, Modifying, or Deleting a Change Request

To add a change request, click the green plus icon above the table.

The Edit Device Configuration page appears. See [“Editing Device Configuration Overview” on page 68](#).

To modify a change request, select it, then click the diagonal pencil icon above the table.

The Edit Device Configuration page appears. See [“Editing Device Configuration Overview” on page 68](#).

To delete a change request, select it, then click the red X icon above the table.



NOTE: Change requests in progress cannot be deleted. An error message appears if your change is in progress.

The Confirm Deletion of Change Request dialog box appears. It displays two columns, Description and Created By.

Confirm by clicking **Delete**.

An error message tells you if the delete action cannot be completed, and you return to the Confirm Deletion of Change Request dialog box.

Related Documentation

- [Editing Device Configuration Overview on page 68](#)
- [Selecting the Device and the Configuration Perspective on page 69](#)
- [Editing Device Configuration Options on page 70](#)
- [Finalizing Device Configuration Changes on page 72](#)

Viewing Hardware Inventory for Devices

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 displays hardware inventory by device name, based on data that Junos Space retrieves both from the device during discovery and resync operations, and from the data stored in the hardware catalog. For each managed device, the Junos Space 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 manages:

1. From the navigation ribbon, select the **Devices** workspace.
2. From the navigation ribbon, select the Manage Devices icon.

The Manage Devices inventory page displays the devices managed in Junos Space.

3. Double-click a device to display its inventory.

Figure 48 on page 76 shows the device inventory page for a single device.

Figure 48: Device Inventory: Single Chassis

Return to Inventory View				
Item	Model Number	Part Number	Serial Number	Description
San Francisco - MX960			JN111BEBEAF6	
Chassis	CHAS-BP-MX960-S	710-013698	JN111BEBEAF6	MX960
FPM Board	CRAFT-MX960-S	710-014974 (REV 03)	XE1330	Front Panel Display
PDM		740-013110 (REV 03)	QCS1243504A	Power Distribution Module
PEM 0		740-013682 (REV 04)	QCS1239402A	PS 1.7kW; 200-240VAC in
PEM 2		740-013682 (REV 04)	QCS123340EM	PS 1.7kW; 200-240VAC in
PEM 3		740-013682 (REV 04)	QCS123340F2	PS 1.7kW; 200-240VAC in
Routing Engine 0	RE-S-1300-2048-S	740-015113 (REV 07)	9009009811	RE-S-1300
Routing Engine 1	RE-S-1300-2048-S	740-015113 (REV 07)	9009009266	RE-S-1300
CB 0	SCB-MX960-S	710-021523 (REV 03)	XA5623	MX SCB
CB 1	SCB-MX960-S	710-021523 (REV 03)	XC0534	MX SCB
CB 2	SCB-MX960-S	710-021523 (REV 03)	XA5805	MX SCB
FPC 0	DPCE-R-40GE-SFP	750-021679 (REV 13)	XA6865	DPCE 40x 1GE R
CPU		710-022351 (REV 03)	XA1540	DPC PMB
PIC 0		BUILTIN	BUILTIN	10x 1GE(LAN)
Xcvr 0		740-013111 (REV 01)	7351693	SFP-T
Xcvr 1		740-013111 (REV 01)	7351258	SFP-T
Xcvr 2		740-013111 (REV 01)	7351312	SFP-T
Xcvr 3		740-013111 (REV 01)	7351640	SFP-T
Xcvr 4		740-013111 (REV 01)	7351358	SFP-T
Xcvr 5		740-013111 (REV 01)	7351448	SFP-T
Xcvr 6		740-013111 (REV 01)	7351265	SFP-T
Xcvr 7		740-013111 (REV 01)	7351369	SFP-T
Xcvr 8		740-013111 (REV 02)	9012993	SFP-T
Xcvr 9		740-013111 (REV 01)	7351299	SFP-T

Figure 49 on page 76 shows the device inventory for SRX Series chassis cluster devices. This inventory record shows information for both the primary and secondary device.

Figure 49: Device Inventory: Chassis Cluster

Return to Inventory View				
Item	Model Number	Part Number	Serial Number	Description
Cluster				
srx3400-bottom - SRX3400			AA2808AD0015	
Chassis (node1)	SRX3400-CHAS	710-015748	AA2808AD0015	SRX 3400
srx3400-top - SRX3400			AA2808AD0013	
Chassis (node0)	SRX3400-CHAS	710-015748	AA2808AD0013	SRX 3400

Figure 50 on page 76 shows the device inventory for a Junos Space Network Application Platform installation that includes Service Now and Service Insight. This inventory record includes columns related to service contracts and end-of-life status.

Figure 50: Device Inventory: Service Information

Return to Inventory View Export								
Item	Model Number	Part Number	Serial Number	Service SKU	Contract End	EOL Status	EOL Replacer	EOL Date
srx650_191 - SRX650			AJ4410AA0031					
Chassis		710-023875	AJ4410AA0031	PAR-1-AR1-AP-F1	07/31/2011			
System IO		710-023209 (REV 09)	AACV9484	SVC-JCS-XXX	09/30/2011			
Routing Engine		750-023223 (REV 22)	AACV1217	PA3-1-AR1-AP-E1	07/29/2011			
FPC 0								
PIC 0								
FPC 5		750-026182 (REV 08)	AACV9792	PAR-1-S0-SRX21	07/31/2011			
PIC 0								
Power Supply 0	SRX600-PWR-64	740-024283 (REV 03)	UH09309					

Table 12 on page 77 describes the information displayed in the device inventory page.

Table 12: Device Inventory Fields

Field	Description
Item	Chassis component. Depending on the device type, can include the midplane, backplane, power supplies, fan trays, Routing Engine, front panel module board, PDM, CIP, PEM, SCG, CB, FPCs, and PICs.
Model Number	Model number for the chassis component.
Part Number	Part number and revision level of the component (FRU). "BUILTIN" indicates the component is not a FRU.
Serial Number	Serial number of the component (FRU). "BUILTIN" indicates the component is not a FRU.
Service SKU	Stock-keeping unit (SKU) identifier for the service contract associated with the part. This data is populated by the Service Now Devices table. If Service Now is not installed, or if the table contains no data, this column is not displayed.
Contract End	End date for the service contract associated with the part. This data is populated by the Service Now Devices table. If Service Now is not installed, or if the table contains no data, this column is not displayed.
EOL Status	Indicates whether end-of-life (EOL) data is available for the part. This data is populated by the Service Insight Exposure Analyzer table. If Service Insight is not installed, or if the table contains no data, this column is not displayed.
EOL Replacement Part	Part number for the replacement part identified by the Juniper Networks support organization. This is the same information that would be published in an EOL announcement bulletin. For an example, see PSN-2011-07-315 . This data is populated by the Service Insight Exposure Analyzer table. If Service Insight is not installed, or if the table contains no data, this column is not displayed.
EOL Date	End-of-sale date reported in the EOL announcement bulletin. For an example, see PSN-2011-07-315 . This data is populated by the Service Insight Exposure Analyzer table. If Service Insight is not installed, or if the table contains no data, this column is not displayed.
Description	Description of the component or FRU.

- Click **Return to Inventory View** to return to the device inventory page.
- Click **Export** at the top of the inventory page to export the table in CSV format.

The Export Inventory Job Status dialog box appears, displaying the progress of the job and the job ID.
- Go to the Job Manager and click the download link to access the file.

Related Documentation

- [Displaying Service Contract and EOL Data in the Physical Inventory Table on page 84](#)
- [Viewing Managed Devices on page 63](#)
- [Viewing Physical Interfaces for Devices on page 78](#)
- [Resynchronizing Managed Devices on page 80](#)
- [Viewing and Exporting Device License Inventory on page 91](#)
- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 96](#)

Viewing Physical Interfaces for Devices

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

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

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

To view the physical interfaces for devices:

1. From the navigation ribbon, select the **Devices** workspace.
2. From the navigation ribbon, select the Manage Devices icon.
3. In the Manage Device inventory page, select the device for which you want to view the physical interfaces.
4. In the Actions drawer, click **View Interfaces**.

Junos Space displays the status of the physical interfaces for a device.

Figure 51: Device Inventory: Physical Interfaces

Return to Inventory View									
Device Name	Interface Name	Ip Address	MAC Address	Operational Sta	Admin Status	Encapsulation	Link Type	Speed (Mbps)	MTU
SanFrancisco	lo0	192.168.1.40		up	up				Unlimited
SanFrancisco	ge-0/0/0	10.1.10.30	00:22:83:d9:d8:1	up	up	Ethernet	full-duplex	1000	1514
SanFrancisco	ge-0/0/1		00:22:83:d9:d8:1	down	down	Ethernet		1000	1514
SanFrancisco	ge-0/0/2		00:22:83:d9:d8:1	up	up	52	full-duplex	1000	1522
SanFrancisco	ge-0/0/3		00:22:83:d9:d8:1	up	up	Ethernet	full-duplex	1000	1514
SanFrancisco	ge-0/0/4		00:22:83:d9:d8:1	up	up	Ethernet	full-duplex	1000	1514
SanFrancisco	ge-0/0/5		00:22:83:d9:d8:1	up	up	Ethernet	full-duplex	1000	1514
SanFrancisco	ge-0/0/6		00:22:83:d9:d8:1	up	up	Ethernet	full-duplex	1000	1514
SanFrancisco	ge-0/0/7		00:22:83:d9:d8:1	up	up	Ethernet	full-duplex	1000	1514
SanFrancisco	ge-0/0/8		00:22:83:d9:d8:1	up	up	Ethernet-VPLS	full-duplex	1000	1522
SanFrancisco	ge-0/0/9		00:22:83:d9:d8:1	up	up	Ethernet-VPLS	full-duplex	1000	1522
SanFrancisco	ge-0/1/0		00:22:83:d9:d8:1	up	up	Ethernet	full-duplex	1000	1514

Table 13 on page 78 describes the information displayed for the physical Interfaces.

Table 13: Physical Interfaces Columns

Field	Description
Device Name	Device configuration name.

Table 13: Physical Interfaces Columns (*continued*)

Field	Description
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.
Operational Status	Operational status of the interface: up or down.
Admin Status	Admin status of the interface: up or down.
Encapsulation	Encapsulation used on the physical interface.
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.

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

Related Documentation

- [Viewing Managed Devices on page 63](#)
- [Viewing Hardware Inventory for Devices on page 75](#)
- [Viewing and Exporting Device License Inventory on page 91](#)

Deleting Devices

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

To delete a device from Junos Space:

- From the navigation ribbon, select the **Devices** workspace.
- From the navigation ribbon, click the Manage Devices icon.

The Manage Devices inventory page displays thumbnails of the devices managed in Junos Space.

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

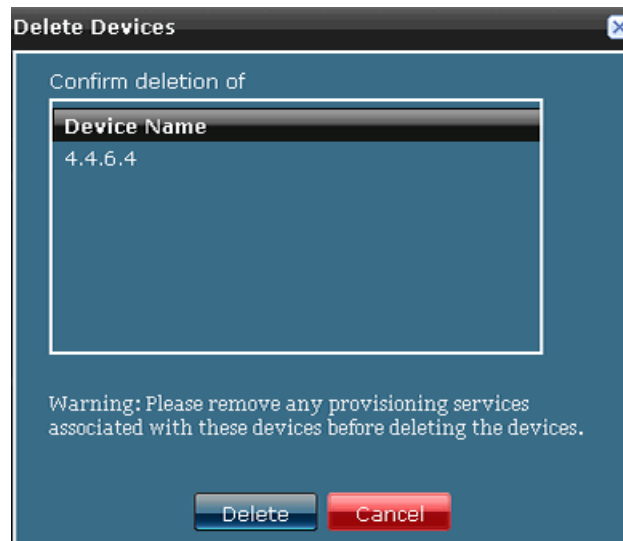
Junos Space displays basic device information, including name, OS version, platform, IP address, and connection status.

- From the Manage Devices inventory page, select one or more devices to delete.

5. If provisioning services are associated with a device that you want to delete, you must remove the provisioning services before deleting the device. See *Deleting a Service Order*.
6. Select **Delete** from the Actions drawer.

Junos Space displays the Delete Devices dialog box.

Figure 52: Delete Devices Dialog Box



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

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

Related Documentation

- [Viewing Managed Devices on page 63](#)
- [Viewing Hardware Inventory for Devices on page 75](#)
- [Viewing Physical Interfaces for Devices on page 78](#)
- [Discovering Devices on page 40](#)

Resynchronizing Managed Devices

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 database with the physical device.

To resynchronize a device:

1. From the navigation ribbon, select the **Devices** workspace icon.
2. From the navigation ribbon, select the Manage Devices icon.

The Manage Devices inventory page displays the list of managed devices by name and IP address.

3. From the Manage Devices inventory page, select one or more devices to resynchronize:
4. From the Actions drawer, click **Resynchronize with Network** to reimport the devices in Junos Space.

Junos Space displays the Resynchronize Devices dialog box, as shown in the following example.

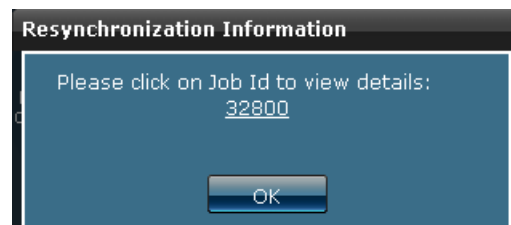
Figure 53: Resynchronize Devices Dialog Box



5. Click **Confirm**.

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

Figure 54: Resynchronization Information Status Message



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

When a resync job is scheduled to run but another resync job on the same device is in progress, Junos Space delays the scheduled resync job. The time delay is determined by the damper interval that you set from the application workspace. By default the time delay is 20 seconds. The scheduled job is delayed as long as the other resync job to the same device is in progress. When the job that is currently running finishes, the scheduled resync job starts. See [“Modifying Application Settings” on page 454](#).

**Related
Documentation**

- [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 96](#)
- [Device Inventory Management Overview on page 62](#)
- [Viewing Managed Devices on page 63](#)
- [Viewing Hardware Inventory for Devices on page 75](#)
- [Viewing Physical Interfaces for Devices on page 78](#)
- [Viewing and Exporting Device License Inventory on page 91](#)

Changing Login Credentials for Managed Devices

You can change the login credentials for any device that Junos Space manages. Changing the credentials for a managed device updates the credentials in Junos Space but not on the device itself. To change credentials on a device, you must access the device directly from the CLI.

We recommend that you bring down the managed device connection before you change the login credentials.

To change the login credentials for devices that Junos Space manages:

1. From the navigation ribbon, select the **Devices** workspace.
2. From the navigation ribbon, click the Manage Devices icon.

The Manage Devices inventory page displays the devices managed in Junos Space.



.....

NOTE: You can select one or more devices and apply the same login credentials to the selected devices.

.....

3. Change credentials for one or more managed devices for which the connection status is down as follows:
 - a. Select the device or devices for which you want to change login credentials.
 - b. Select **Change Credentials** from the Actions drawer.

The Change Credentials dialog box appears, as shown in the following example.

Figure 55: Change Credentials Dialog Box

Warning: Credentials will be changed within Junos Space only. Please update credentials on devices manually.

☒ Do not change device credentials in the database for devices currently connected to Junos Space

Confirm changing credentials of

Device Name	Connection Status
4.4.4.6	down
4.4.4.7	down

Username:

Password:

Confirm password:

- c. Enter a username and password, and reenter the password.
- d. Click **Confirm**.

The new login credentials for the selected devices are updated in the Junos Space database.

Change credentials for one or more managed devices for which the connection status is up.

- a. Select one or more devices for which you want to change the login credentials.
- b. Select **Change Credentials** from the Actions drawer.

The Change Credentials dialog box appears.

- c. Clear the **Do not change device credentials in the database for devices currently connected to Junos Space** check box.

The Change Credentials dialog box displays the selected devices that are connected to Junos Space, as shown in the following example.

Figure 56: Change Credentials Dialog Box

Change Credentials

Warning: Credentials will be changed within Junos Space only. Please update credentials on devices manually.

☐ Do not change device credentials in the database for devices currently connected to Junos Space

Confirm changing credentials of

Device Name	Connection Status
Laguna_pe_d1	up

Username:

Password:

Confirm password:

d. Enter a username and password, and reenter the password.

e. Click **Confirm**.

The new login credentials for the selected devices are updated in the Junos Space database.

Related Documentation

- [Connecting to a Device From Secure Console on page 121](#)

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. [Figure 57 on page 84](#) shows the Physical Inventory table with service contract data.

Figure 57: Physical Inventory with Service Contract Data

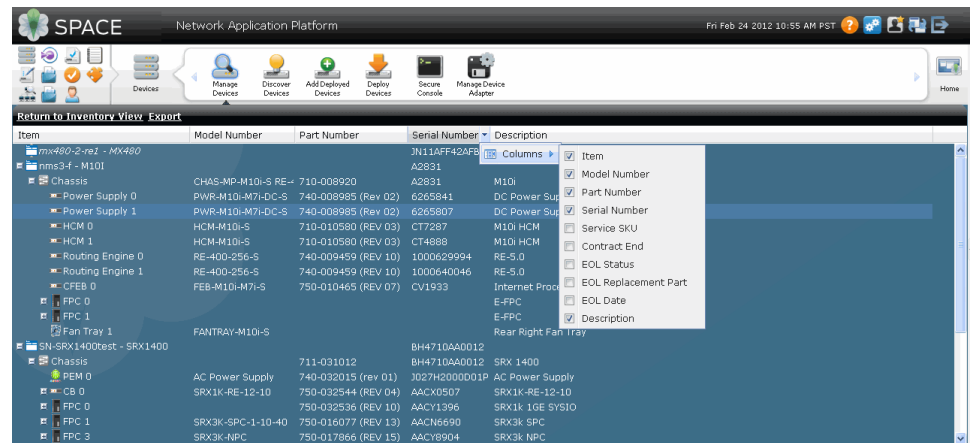
Item	Model Number	Part Number	Serial Number	Service SKU	Contract End	EOL Status	EOL Replacer	EOL Date	Description
SRX650_191 - SRX650									SRX650
Chassis		710-023875	AH410AA0031	PAR-1-AR1-AP-F1	07/31/2011				SRXSME System
System IO		710-023209 (REV 09)	AAC9484	SVC-JCS-XXX	09/30/2011				RE-SRXSME-SRE
Routing Engine		750-023223 (REV 22)	AACY1217	PA3-1-AR1-AP-E	07/29/2011				FPC
FPC 0									4x GE Base PIC
PIC 0									FPC
FPC 6		750-026182 (REV 08)	AACY9792	PAR-1-SD-SRX21	07/31/2011				16x GE gPIM
PIC 0									PS 645W AC
Power Supply 0		SRX600-PWR-645AC- 740-024283 (Rev 03)	UH09309						

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. [Figure 58 on page 85](#) shows the table column display filters.

Figure 58: Physical Inventory with Column Display Filters



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, including information about the service contract. [Figure 59 on page 86](#) shows the service contract information displayed in the Service Detail page.

Figure 59: Service Now Service Detail Page

The screenshot displays the 'Service Detail' page in Junos Space. The left sidebar shows the 'Service Now Devices' section with a list of devices under the 'Nandial' organization. The main content area shows details for a specific device, including its hostname, serial number, product, platform, OS version, and event profile. Below this, a table lists contracts. Two red circles highlight the 'SKU' and 'End Date' columns in the contract table.

Agreement Num	Agreement Sta	SKU	SKU Type	Start Date	End Date
C1-156261494E	Expired	PAR-1-AR1-AP-FWL	PAR	Jun 20, 2011 12:00:00 AM PDT	Jul 31, 2011 12:00:00 AM PDT
NContract	ACTIVE	SVC-JCS-XXX	SVC	May 29, 2011 12:00:00 AM PDT	Sep 30, 2011 12:00:00 AM PDT

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* in the Service Now documentation.
 - Service Now Device. See *Service Now Devices Overview* in the Service Now documentation.
 - Service Now Device Group. See *Associating Devices with a Device Group* in the Service Now documentation.
 - Service Now Event Profile. See *Event Profiles Overview* in the Service Now documentation.
3. Check the Service Insight Exposure Analyzer table for details about the devices managed with Junos Space, including information about EOL announcements. [Figure 60 on page 87](#) shows a Service Insight Exposure Analyzer record where EOL data is available.

Figure 60: Service Insight Exposure Analyzer Record with EOL Data

The screenshot displays the Junos Space Service Insight Exposure Analyzer. The main table lists exposure records with columns for Organization, Connected Member, Device Group, and EOL Status. A red circle highlights the 'EOL Status' column. The 'Device Detail' pane on the right shows information for a specific device, including its name, serial number, IP address, and EOL status. The 'EOL Status' is highlighted with a red circle and shows 'EOL Data available'.

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

Related Documentation

- [Viewing Hardware Inventory for Devices on page 75](#)

Exporting Device Inventory Information

From the Manage Devices application in the Junos Space Devices workspace, you can view the list of devices managed through Junos Space and export the device information to a comma-separated view (CSV) file. You can upload the CSV file that you create into other applications, such as those you use for asset management. The export task runs as a Junos Space job.

You can display the device inventory summary in table format from Manage Devices on the navigation ribbon, or in a detailed list form from the Actions drawer. You use both forms in the export device inventory process.

To export device inventory information:

1. Display the device inventory by selecting **Network Application Platform > Devices > Manage Devices**.

Figure 61: Manage Devices Inventory Table



Name	Interfaces	OS Version	Platform	IP Address	Connection...	Managed S...
10.155.70.222	View	10.2R1.8	SRX3400	10.155.70.222	down	In Sync
CE-1	View	9.6R3.8	M10	10.155.69.1	down	In Sync
CE2	View	9.3R4.4	M10	10.155.69.2	down	Connecting
Eureka-PE	View	10.1R1.8	M71	10.155.69.26	down	In Sync
Florence-PE	View	10.1R1.8	M71	10.155.69.27	down	In Sync
Laguna_pe_d1	View	10.2R1.3	MX480	10.155.69.14	down	In Sync
RioVista_pe_d1	View	10.2R2.3	MX240	10.155.69.25	down	In Sync
RiverSide	View	10.2R1.6	M101	10.155.69.22	down	In Sync
Sacramento-P2	View	10.1R1.8	M101	10.155.69.24	down	In Sync
SanDiego-P1	View	10.1R1.8	M101	10.155.69.15	down	In Sync
SanFrancisco	View	10.0R3.10	MX960	10.155.69.13	down	Connecting
SanJose	View	10.2R1.8	MX240	10.155.69.12	down	Connecting

2. Select the devices you want to include in the inventory report. See “[Inventory Pages Overview](#)” on page 28.
3. (Optional) Preview the details for the device selection.

You might want to preview the device information before you export to the CSV file. To display the device inventory details in list format, open the Actions drawer and click the **View Physical Inventory** task.

Figure 62: Manage Devices Actions Drawer



Name	Interfaces	OS Version	Platform	IP Address	Connection Status	Managed Status	Serial Nu...	Level 2 De...
10.155.69.12	View	10.1R1.8	junos	MX240	down	Connecting	JN1124E9	OS Version 10.1R1.8 Platform: MX240
10.155.69.14	View	10.2R1.3	junos	MX480	down	Connecting	JN115607	OS Version 10.2R1.3 Platform: MX480
10.155.69.13	View	10.0R3.10	junos	MX960	down	Connecting	JN1118E9	OS Version 10.0R3.10 Platform: MX960
10.155.69.25	View	10.0R2.10	junos	MX240	down	Connecting	JN119387	OS Version 10.0R2.10 Platform: MX240
10.155.69.27	View	10.1R1.8	junos	M71	down	Connecting	B5259	OS Version 10.1R1.8 Platform: M71
10.155.69.23	View	10.2R1.6	junos	M101	up	In Sync	B4203	OS Version 10.2R1.6 Platform: M101
10.155.69.22	View	10.2R1.6	junos	M101	up	In Sync	B4170	OS Version 10.2R1.6 Platform: M101

The following page appears.

Figure 63: Physical Inventory View

Return to Inventory View		Export		
Item	Model Number	Part Number	Serial Number	Description
[-] RioVista-pe-d1 - MX240			JN1193879AFC	
[-] SanFrancisco - MX960			JN1118E9EAFA	
[-] SanJose - MX240			JN112AE30AFC	
[-] Florence-PE - M7I			B5259	
[-] Sacramento-P2 - M10I			B3901	
[-] SanDiego-P1 - M10I			B4171	
[-] Laguna-pe-d1 - MX480			JN1156D73AFB	
[-] Jackson - M10I			B4203	
[-] RiverSide - M10I			B4170	
[-] CE-1 - M10			52839	

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.

Figure 64: Physical Inventory View with Expanded Details

Return to Inventory View		Export		
Item	Model Number	Part Number	Serial Number	Description
[-] space-EX2200 - EX2200-24T-4G			CW0210102867	
[-] Chassis	EX2200-24T-4G		CW0210102867	EX2200-24T-4G
[-] Routing Engine 0	EX2200-24T-4G	750-026468 (REV 11)	CW0210102867	EX2200-24T-4G
[-] FPC 0	EX2200-24T-4G	750-026468 (REV 11)	CW0210102867	EX2200-24T-4G
[-] CPU		BUILTIN	BUILTIN	FPC CPU
[-] PIC 0	EX2200-24T-4G	BUILTIN	BUILTIN	24x 10/100/1000 Base-T
[-] PIC 1	EX2200-24T-4G	BUILTIN	BUILTIN	4x GE SFP
[-] Xevr 0 (Empty)				
[-] Xevr 1 (Empty)				
[-] Xevr 2 (Empty)				
[-] Xevr 3 (Empty)				
[-] Power Supply 0				PS 100W AC
[-] Fan Tray				Fan Tray
[-] ft-sw1 - EX2200-24T			BH0205106206	
[-] ps2 - EX2200-24T			BM0208204486	
[-] CE1 - EX2200-48T			BP0208248984	

If the device information in this display is what you want to include in your report, click **Export** in the window header to create the CSV file. If you want to change the content of the report, click 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.

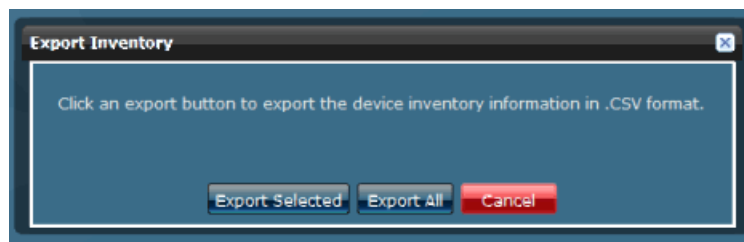
4. Export the device inventory information to the CSV file.

You can export information about selected devices or export information about all of the devices managed by Junos Space.

Once you are satisfied with your selection of devices to include in your report, open the Action drawer and click **Export Physical Inventory** to display the Export Inventory dialog box.

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

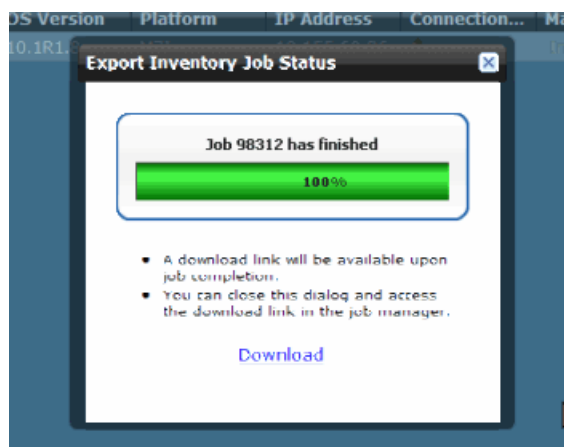
Figure 65: Export Inventory Dialog Box



Clicking an export button starts a Junos Space job that creates and saves the CSV report. When the job starts, the Export Inventory Job Status dialog box appears.

When the job is completed, the Export Inventory Job Status report indicates the job is 100% complete. Click the **Download** link in the Export Inventory Job Status report to display the CSV file.

Figure 66: Export Inventory Job Status Report



5. Download the resulting CSV file.

Now that you have the CSV report, you can import that CSV file into other applications such as those you use for asset management.

Related Documentation

- [Device Inventory Management Overview on page 62](#)
- [Viewing Managed Devices on page 63](#)
- [Inventory Pages Overview on page 28](#)
- [Viewing Hardware Inventory for Devices on page 75](#)
- [Device Management Overview on page 57](#)
- [Device Discovery Overview on page 39](#)

Viewing and Exporting Device 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 management.

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

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 itself, see [“Viewing Licenses” on page 447](#).

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, Junos Space automatically synchronizes with the managed device. You can also manually resynchronize the Junos Space license database with the device by using the Resynchronize with Network action. See [“Resynchronizing Managed Devices” on page 80](#).

Viewing device license inventory does not include pushing license keys to devices. You can, however, push licenses with the Configuration Editor to any device that has license keys in its configuration. See [“Editing Device Configuration Overview” on page 68](#). You can export device license inventory information to a CSV file for use in other applications.

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

To view license inventory for a device:

1. From the navigation ribbon, select the **Devices > Manage Devices**.

The Manage Devices inventory page displays the devices managed in Junos Space.

2. Select a device and click **View License Inventory** in the Actions drawer.

The License Inventory page displays the license information listed in [Table 14 on page 92](#).



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 15 on page 93](#).

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

5. (Optional) Click **Export** at the top of the inventory page, just below the navigation ribbon, 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 15 on page 93](#) and [Table 16 on page 93](#). 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 14: License Usage Summary Fields

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

Table 14: License Usage Summary Fields (*continued*)

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

Table 15: 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 16: 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 63](#)
 - [Resynchronizing Managed Devices on page 80](#)
 - [Understanding How Junos Space Automatically Resynchronizes Managed Devices on page 96](#)

Troubleshooting Devices

You can troubleshoot M Series or MX Series devices from Network Application Platform if you have Network Activate installed.

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

To check device configuration:

1. In the Network Application Platform navigation ribbon, select **Devices > Manage Devices**.

The Manage Devices inventory page appears, displaying all discovered devices on the network.

2. Select the device that you want to troubleshoot.
3. Open the Actions drawer and select **Troubleshoot**.

The Troubleshoot Device dialog box appears.



NOTE: This command is available only for M Series and MX Series devices.

4. Select any **show** command to view device-specific configuration information.

Table 17 on page 94 describes the show commands that you can run to check the configuration on a device.

Table 17: Commands Available in the Troubleshoot Device Dialog Box

Command	Description	Fields Displayed
show mpls lsp ingress	Display whether ingress LSP is up and running.	<ul style="list-style-type: none"> • Device name • LSP State • Destination Address
show mpls lsp egress	Display whether egress LSP is up and running.	<ul style="list-style-type: none"> • Device name • LSP State • Destination Address
show bgp summary	Display summary information about BGP and its neighbors to determine if routes are received from peers in the autonomous system (AS). When a BGP session is established, the peers exchange update messages.	<ul style="list-style-type: none"> • Peer Address • Peer State

Table 17: Commands Available in the Troubleshoot Device Dialog Box (*continued*)

Command	Description	Fields Displayed
show ospf neighbor	Display information about OSPF neighbors.	<ul style="list-style-type: none"> Interface Name Neighbor Address OSPF Neighbor State
show bgp neighbor	Display information about all BGP peers.	<ul style="list-style-type: none"> Peer Address Peer State Local AS
show ldp interface	Display standard status information about all LDP-enabled interfaces for all routing instances.	<ul style="list-style-type: none"> Interface Name LDP Neighbor Count
show ldp neighbor	Display standard information about LDP neighbors for all routing instances.	<ul style="list-style-type: none"> Interface Name Neighbor Address Remaining Time—remaining hold time before the neighbor expires, in seconds.
show rsvp session	Display information about Resource Reservation Protocol (RSVP) sessions.	<ul style="list-style-type: none"> Name LSP State Destination Address <p>For complete information about the fields displayed for the show rsvp session command, see the <i>Junos Software Routing Protocols and Policies Command Reference</i>.</p>
show rsvp interface	Display the status of Resource Reservation Protocol (RSVP)-enabled interfaces and packet statistics.	<ul style="list-style-type: none"> Interface Name RSVP Status Static Bandwidth Available Bandwidth Total Reserved Bandwidth
show isis adjacency	Display information about intermediate System-to-Intermediate System (*IS-IS) neighbors.	<ul style="list-style-type: none"> Interface Name Adjacency State System Name <p>For complete information about the fields displayed for the show isis adjacency command, see the <i>Junos Software Routing Protocols and Policies Command Reference</i>.</p>



NOTE: For additional information about a device configuration, you can explicitly run a **show** command with the **extensive** option, for example, **show mpls lsp extensive**.

Related Documentation

- [Deploying Device Instances on page 108](#)
- [Troubleshooting N-PE Devices Before Provisioning a Service](#)

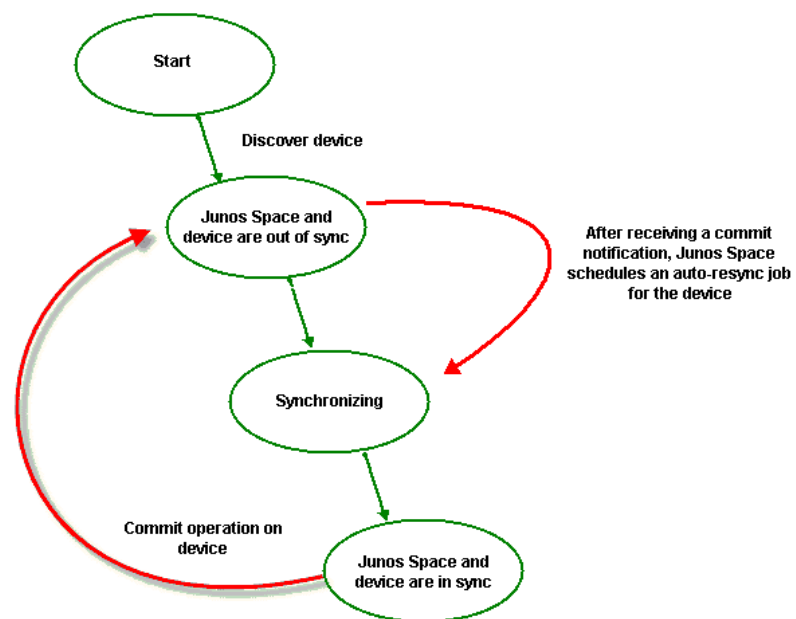
Understanding How Junos Space Automatically Resynchronizes Managed Devices

When configuration changes are made on a physical device that Junos Space manages, Junos Space automatically resynchronizes with the device. This ensures that the device inventory information in the Junos Space database matches the current configuration information on the device.

After Junos Space discovers and imports a device, Junos Space enables the auto-resync feature on the physical device by initiating a commit operation.

After auto-resynchronization is enabled, any configuration changes made on the physical device, including out-of-band CLI commits and change-request updates, automatically trigger resynchronization on the device. [Figure 67 on page 96](#) shows how a commit operation on the device triggers resynchronization.

Figure 67: Resynchronization Process



When a commit operation is performed on a managed device, Junos Space schedules a resync job to run 20 seconds after the commit notification is received. However, by default, if Junos Space receives another commit notification from the device within 25 seconds of the previous commit notification, no additional resync jobs are scheduled, but Junos Space will resynchronize both commit operations in one job. This damping feature of automatic resynchronization provides a window of time during which multiple commit operations can be executed on the device, but only one or a few resync jobs are required to resynchronize the Junos Space database after multiple configuration changes are executed on the device.

When Junos Space receives the device commit notification, the device status is "Out of Sync". When the resync job begins on the device, the Managed Status for the device

displays “Synchronizing” and then “In Sync” after the resync job has completed, unless a pending device commit operation causes the device to display “Out of Sync” while it was synchronizing.

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

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

For information about setting the damper interval to change the resync time delay and information about disabling the auto-resync feature, see [“Modifying Application Settings” on page 454](#).

**Related
Documentation**

- [Resynchronizing Managed Devices on page 80](#)
- [Device Discovery Overview on page 39](#)
- [Device Inventory Management Overview on page 62](#)
- [Viewing Managed Devices on page 63](#)

CHAPTER 7

Adding Devices and Connection Profiles

- [Add Devices Overview on page 99](#)
- [Adding Devices on page 101](#)
- [Deploying Device Instances on page 108](#)
- [Connection Profiles Overview on page 111](#)
- [Creating Connection Profiles on page 113](#)
- [Managing Connection Profiles on page 116](#)

Add Devices Overview

You can use the Add Device wizard to create deployment instances that are used to deploy SRX Series devices. You can create deployment instances either manually or by uploading a comma-separated values (CSV) file. A deployment instance contains the configlets used to deploy branch SRX Series devices that are currently using the factory default settings.

A configlet is a small subset of a configuration used by a device to obtain an IP address and connect back to the management station for further management. A configlet contains information about the device series, device platform, OS version, and the connection details used to bootstrap the device. It can be used to deploy devices from an external storage device such as a USB stick.

You need to specify the following details to create a configlet:

- Device name
- Device series
- Device platform
- OS version
- Device count
- Connectivity type
- Interface
- Connection profile
- Encryption password

You can store this configlet in an external USB storage device and plug it into the SRX Series device to start it. The device count and encryption option determine the subsequent steps in starting the SRX Series device using the configlet.

The following parameters determine the steps in booting the SRX Series device using the configlet:

- Plain text configlet

If you save the configlet as a plain text file, the device will not prompt you to enter a password during the startup process.

- Encrypted configlet using AES encryption with a custom key

If you encrypt the configlet with a custom key, the device will prompt you to enter a password. You are required to enter the 16-character password specified during the creation of the configlet. You can also save a text file named `key.txt` in the USB storage device that you are using to start the device. This file contains the password; the device will automatically use the password specified in this file.

- Device count value is 1

If you create an individual configlet for each device with a Device Count column value of 1, the configlet contains the hostname. The device does not prompt you to enter the hostname during startup.

- Device count value greater than 1

You can start devices with similar network connection parameters (for example, obtaining IP address through DHCP) using an individual configlet. This is done by specifying the number of devices that can be started with the same configlet in the Device Count column. If you create such a configlet, the device prompts for a hostname during startup. You are required to enter a unique hostname for each of the devices that are used to startup using this configlet. You can also save a text file named `hostname.txt` in the USB storage device which you are using to start the device. This file contains the hostnames for all devices that are started using the configlet.



NOTE: By default, the configlet that you download is named `Configlets.zip`. This zip file is unzipped to obtain the configlet files. You should not rename the configlet files. Renaming the configlet files may not complete the device startup process.



NOTE: If you are using Internet Explorer to download the configlets, you need to customize the browser settings to download them. Perform the following steps:

1. Open Internet Explorer and navigate to **Tools > Internet Options**.
2. Click the **Security** tab and select the **Custom Level** tab.
3. In the **Automatic prompting for file downloads** section, click the **Enable** option button.

**Related
Documentation**

- [Adding Devices on page 101](#)
- [Deploying Device Instances on page 108](#)
- [Managing DMI Schemas Overview on page 506](#)

Adding Devices

This topic includes the following procedures:

- [Creating a Deployment Instance on page 102](#)
- [Adding a Deployment Instance by Importing a CSV File on page 103](#)
- [Adding a Deployment Instance Manually on page 104](#)
- [Working with Rows and Columns on page 105](#)
- [Working with Configlets on page 107](#)

Creating a Deployment Instance

To create a new deployment instance:

1. From the navigation ribbon, select **Devices** > **Deploy Devices**.

The Deploy Devices inventory page displays icons for all the deployment instances, as shown in [Figure 68 on page 102](#).

Figure 68: Deploy Devices Inventory



2. From the navigation ribbon, select the Add Devices icon.

The Rapid Deployment dialog box appears, as shown in [Figure 69 on page 102](#).

Figure 69: Device Details dialog box



3. In the Name box, enter a name for the new deployment instance.
4. In the Description box, enter a description for the new deployment instance.

5. Add a new deployment instance either by importing a CSV file or manually. See [“Adding a Deployment Instance by Importing a CSV File” on page 103](#) or [“Adding a Deployment Instance Manually” on page 104](#).

6. Click **Next**.

The Rapid Deployment dialog box appears, displaying a table of settings for the deployment instance that you have added manually or uploaded using a CSV file. Each record in the table can be used to create a configlet.

7. Implement the configlet. See [“Working with Rows and Columns” on page 105](#) and [“Working with Configlets” on page 107](#).

8. Click **Finish**.

The new deployment instance you have added appears in the Device Details inventory page. A new job is created and the job ID appears in the Job Information dialog box.

9. Click the job ID to view more information about the job created.

This action directs you to the Job Management workspace.



NOTE: When you have a large number of devices, we recommend you wait for the Job to complete before downloading the configlets.

Adding a Deployment Instance by Importing a CSV File

To add a new deployment instance by importing a CSV file:

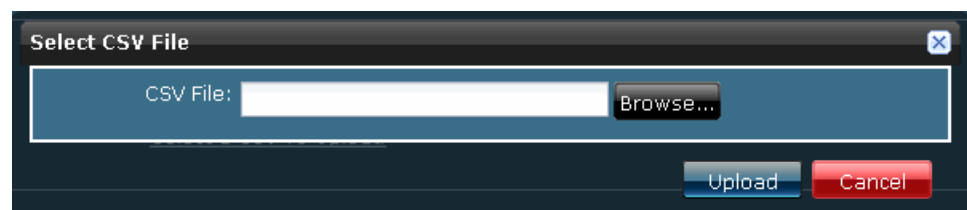
1. Select the **Import to CSV** option button.
2. Select the **View Sample CSV** link in the Import section to view a sample of a CSV file.
3. Save the sample CSV file to your storage location.
4. Make necessary changes in this CSV file and rename it with an appropriate name.



NOTE: Do not add or delete any columns in the CSV file. You cannot upload the CSV file successfully if you add or delete any columns.

5. Select the **Select a CSV To Upload** link in the Import section.
6. The Select CSV File dialog box appears, as shown in [Figure 70 on page 103](#).

Figure 70: Selecting a CSV File to Upload



7. Click **Browse** and upload the CSV file from your storage location.

If the CSV file is successfully uploaded, a Green mark appears next to the Select a CSV To Upload link.

The Upload dialog box appears.

8. Click **OK**.

Adding a Deployment Instance Manually

To add a new deployment instance manually:

1. Select the **Add Manually** option button.
2. Enter the following details in the Device Details section:
 - From the Platform list, select an appropriate platform, as shown in [Figure 71 on page 104](#).

Figure 71: Specifying Device Details

Device Details

OS Version: 6.3

Platform: ns5GT-Trust-Untrust

Number of devices: 1

SNMP Community String: public

Authentication Details

User Name:

Password:

Re-enter Password:

Back Next Finish Cancel

- From the OS Version list, select an appropriate OS version.
- In the Number of devices box, enter the number of devices with the same connection details.

These devices will use a common connection profile.

3. Enter the following details in the Connectivity Details section:
 - Specify an Interface Type: Ethernet or ADSL. [Figure 72 on page 104](#) shows the Connectivity Details section with Ethernet selected.

Figure 72: Specifying Connectivity Details

Connectivity Details

Interface Type: ☒ Ethernet ☐ ADSL

Interface: ge-0/0/0

IP Assignment via: DHCP

Connection Profile: Please select

Create

- The Interface box displays the default interface in the untrust zone, depending on the connection type chosen. Make changes to this field if necessary.

- Select an appropriate IP assignment type.
- Select an appropriate connection profile.

Working with Rows and Columns

The Rapid Deployment dialog box displays a table of settings for the deployment instance that you have added manually or uploaded using a CSV file. Each record in the table can be used to create a configlet.

You can clone, delete, sort the rows, and hide the columns in the Rapid Deployment dialog box.

[Table 18 on page 106](#) describes the icons used to perform these tasks.

Table 18: Icons in the Rapid Deployment dialog box






Icon	Description
	<p>View the details of a configlet.</p> <p>To view a configlet:</p> <ol style="list-style-type: none"> 1. Select the check box to the left of the row corresponding to the configlet you want to view. 2. Click the View Configlet icon.
	<p>Clone a row from the deployment instance table.</p> <p>To clone rows:</p> <ol style="list-style-type: none"> 1. Select the check boxes to the left of the rows you want to clone. 2. Specify the number of clones in the Clone Times field. 3. Click the Clone icon. <p>The new rows appear at the end of the table.</p>
	<p>Delete a row from the deployment instance table.</p> <p>To delete rows:</p> <ol style="list-style-type: none"> 1. Select check boxes to the left of the rows you want to delete. 2. Click the Delete icon
	<p>Create a connection profile. See "Creating Connection Profiles" on page 113.</p>
	<p>Download configlets.</p> <p>To download the configlets:</p> <ol style="list-style-type: none"> 1. Select the check boxes to the left of the rows corresponding to the configlets you want to download. 2. Click the Download Configlet icon. <p>NOTE: If you are using Internet Explorer to download the configlets, you need to customize the browser settings to be able to download them. Perform the following steps to customize the Internet Explorer settings:</p> <ol style="list-style-type: none"> 1. Open Internet Explorer and navigate to Tools > Internet Options. 2. Click the Security tab and select the Custom Level tab. 3. In the Automatic prompting for file downloads section, click the Enable option button.

Table 19 on page 107 lists the fields that you need to add manually.

Table 19: Fields Manually Entered in the Rapid Deployment Dialog Box

Field	Description
Device Count	Specify the number of devices that can be deployed using this configlet.
Interface IP	Specify the IP address of the interface.
Gateway	Specify the IP address of the gateway.

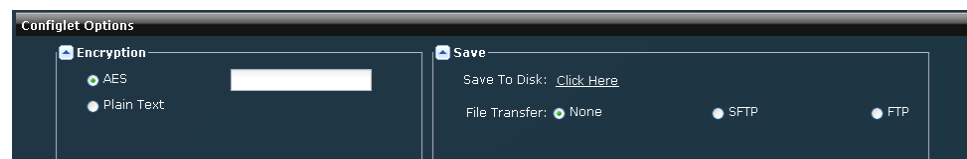
Working with Configlets

You can use the procedures in this section to package the configlet.

To encrypt the configlet:

1. Select the type of encryption you want to use in the Encryption section: AES or Plain Text. For example, [Figure 73 on page 107](#) shows AES encryption selected.

Figure 73: Specifying Configlet Options



2. Enter a password with 16 characters in the corresponding field.



NOTE: You will need to provide this password when you deploy devices using this configlet.

To save the configlet to a disk drive:

- Click the **Click Here** link next to the field in the Save section.

To save the configlet to an FTP location:

1. Select the option button corresponding to the file transfer method you want to use.
2. Enter the user ID, password, server address and folder details in the appropriate fields.

Related Documentation

- [Add Devices Overview on page 99](#)
- [Deploying Device Instances on page 108](#)
- [Managing DMI Schemas Overview on page 506](#)

Deploying Device Instances

You can view, delete and search for specific deployment instances listed in the Deploy Devices inventory page. You can also download configlets from a specific deployment instance.

You can perform the following tasks on the deployment instances and configlets:

1. [Viewing the Details of a Deployment Instance on page 108](#)
2. [Viewing the Device Status on page 108](#)
3. [Deleting a Deployment Instance on page 109](#)
4. [Downloading Configlets on page 109](#)
5. [Searching for a Deployment Instance on page 110](#)

Viewing the Details of a Deployment Instance

To view the details of a deployment instance:

1. From the navigation ribbon, select **Devices > Deploy Devices**.

The Deploy Devices inventory page appears.

2. Double-click the icon for the deployment instance whose details you intend to view.

The Deployment Instance Details report appears, as shown in [Figure 74 on page 108](#).

Figure 74: Deployment Instance Details Report

Device Name	Device Type	OS Version	Serial Number	Connection Type	Interface	Interface IP	Gateway	Connection Profile	Device Count
SRX_Sunnyvale	SRX650	10.3	JN10B8797AGD	DHCP				Sunnyvale_DHC	5
SRX_Westford	SRX210B	10.3	JN10B8797AGN	PPPoE				Westford_PPPoE	4
SRX_Australia	SRX210H	10.3	JN10B8797AGN	PPPoA				Australia_PPPoA	4
SRX_UK	SRX100B	10.3	JN10B8797AGC	Static		10.204.76.70/2	10.204.76.254	UK_Static	3

3. Click **Close**.

Viewing the Device Status

To view the device status:

1. From the navigation ribbon, select **Devices > Deploy Devices**.

The Deploy Devices inventory page appears.

2. Select the deployment instance you intend to view the device status for and click the **View Device Status** link from the Actions drawer in the left corner of the inventory page.

A dialog box displays the connection status of the devices.

3. Click **Back** on the left corner of this dialog box to return to the inventory page.

Deleting a Deployment Instance

To delete a deployment instance you have created:

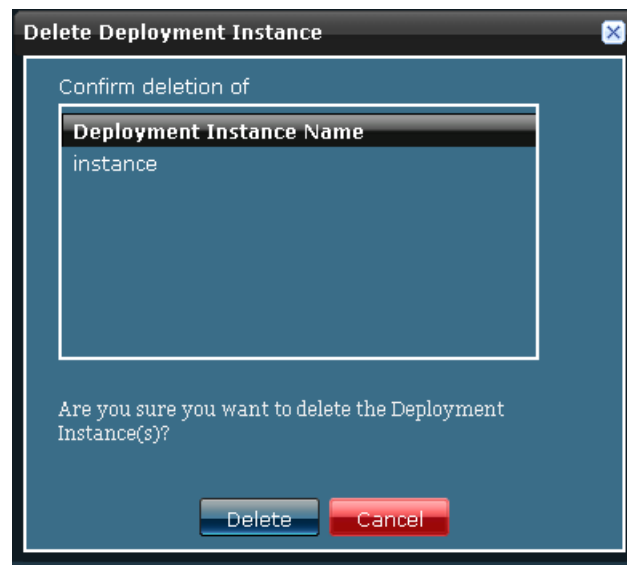
1. From the navigation ribbon, select the **Devices > Deploy Devices**.

The Deploy Devices inventory page appears.

2. Select the deployment instance you intend to delete and click the **Delete** link from the Actions Drawer in the left corner of the inventory page.

The Delete Deployment Instance dialog box appears, as shown in [Figure 75 on page 109](#).

Figure 75: Delete Deployment Instance Dialog Box



3. Select the deployment instance you want to delete and click **Delete**.

Downloading Configlets

To download the configlet you have created:

1. From the navigation ribbon, select **Devices > Deploy Devices**.

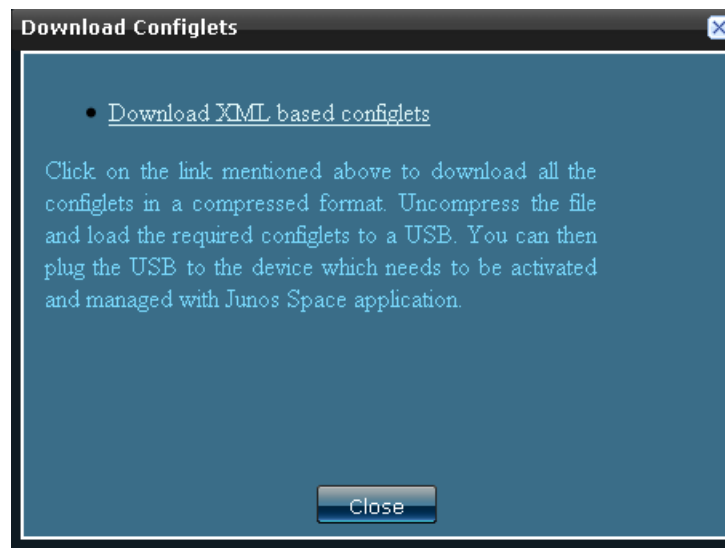
The Deploy Devices inventory page appears.

2. Select the deployment instance containing the configlet you intend to download and click the **Download Configlets** link from the Actions drawer in the left corner of the inventory page.

The Download Configlets dialog box appears.

3. Select the **Download XML based Configlets** link in the Download Configlets dialog box, as shown in [Figure 76 on page 110](#).

Figure 76: Download Configlets Dialog Box



4. Save the .zip file in your storage location.



NOTE: You can also download the configlets when you are creating a deployment instance. However, for a large number of devices we recommended downloading the configlets from the inventory page. See [“Adding Devices” on page 101](#).



NOTE: You cannot download the configlets associated with a deployment instance if a job related to that deployment instance is in progress. The Download Configlets action is disabled until the job is completed.

Searching for a Deployment Instance

To search for a deployment instance you have created:

1. From the navigation ribbon, select **Devices > Deploy Devices**.

The Deploy Devices inventory page appears.

2. In the Search box, enter the name of the deployment instance you want to search, as shown in [Figure 77 on page 110](#).

Figure 77: Searching for a Configlet



3. Click the magnifying glass icon next to the Search box.

The Deploy Devices inventory page is populated with the deployment instances matching your search criterion.

- Related Documentation**
- [Add Devices Overview on page 99](#)
 - [Adding Devices on page 101](#)

Connection Profiles Overview

You can use the Connection Profile wizard to create connection profiles that are used as part of rapid deployment to generate startup configlets. A connection profile is a network connection template that can be shared across multiple configlets.

You can configure the following parameters for a connection profile:

- SSH credentials—SSH username, SSH password
- NAT parameters—NAT IP address, port number, or both, if your Junos Space server is behind a NAT
- DHCP parameters
- PPPoA parameters
- PPPoE parameters

If you configure a DHCP-based connection profile, you need to provide the following details:

- Retransmission parameters
- Lease time
- DHCP server address

If you configure a PPPoA-based connection profile, you need to provide the following details:

- Authentication protocol used—either CHAP or PAP
- PPPoA username and password
- Access profile username and password (optional)
- Virtual Path Identifier (VPI) and Virtual Connection Identifier (VCI) values
- Encapsulation type—either LLC or VP-MUX based

If you choose to configure a PPPoE-based connection profile, you need to provide the following details:

- Authentication protocol used – either CHAP or PAP
- PPPoE username and password

- Access profile username and password (optional)
- Concentrator name (optional)
- Service name (optional)
- Time interval for auto-connect (optional)
- Time interval before an idle connection disconnects (optional)

When a connection profile is created, Junos Space creates an object in the Junos Space database to represent the connection profile. You can use this object to create configlets during rapid deployment of devices.



NOTE: VCI and VPI values used for the connection profile may differ based on the service provider. Ensure that you enter appropriate VCI and VPI values provided by your service provider.

**Related
Documentation**

- [Creating Connection Profiles on page 113](#)
- [Managing Connection Profiles on page 116](#)

Creating Connection Profiles

To create a new connection profile:

1. From the Network Application Platform navigation ribbon, select **Devices > Deploy Devices > Connection Profiles**.

The Connection Profiles inventory page appears with icons for all the connection profiles, as shown in [Figure 78 on page 113](#).

Figure 78: Connection Profiles Inventory



2. From the navigation ribbon, select the Create icon.

The Create Connection Profile dialog box appears as shown in [Figure 79 on page 113](#).

Figure 79: Creating a Connection Profile

3. Enter a name for the new connection profile.

4. Enter a description for the new connection profile.
5. Enter the following details in the SSH Credentials section:
 - Enter a username.
 - Enter a password.
 - Reenter the password to confirm.
6. Enter the following details in the NAT section:
 - Enter an IP address used by the NAT configuration.
 - Enter a port number used by the NAT configuration.
7. Select an IP Assignment Type and complete the configuration as described in [Table 20 on page 114](#).
8. Click **Create** to create a new connection profile.

Table 20: IP Assignment Types

IP Assignment Type	Configuration Guidelines
DHCP	<ul style="list-style-type: none">• Attempts—Enter the number of attempts that a DHCP client will make to get a DHCP address.• Interval (in sec)— Enter the duration between successive retransmission attempts.• Server Address—Enter the IP address of the DHCP server.• Update Server—Select this option to ensure that the DHCP server is updated.• Lease Time—Specify how the DHCP server assigns and manages the leases. Leases can be assigned and managed in the following ways:<ul style="list-style-type: none">• Default—Select to specify the default lease time.• Lease Never Expires—Select to assign a permanent lease to DHCP clients.• Lease Time—Select to specify a custom lease time. In the Lease Time (in sec) box, enter the lease time before which the DHCP server must renew the lease for the client or the client must obtain a new lease.

Table 20: IP Assignment Types (*continued*)

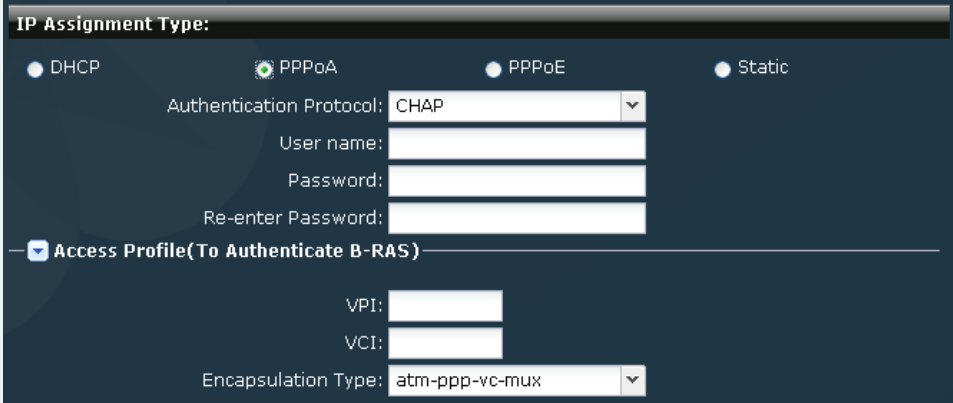
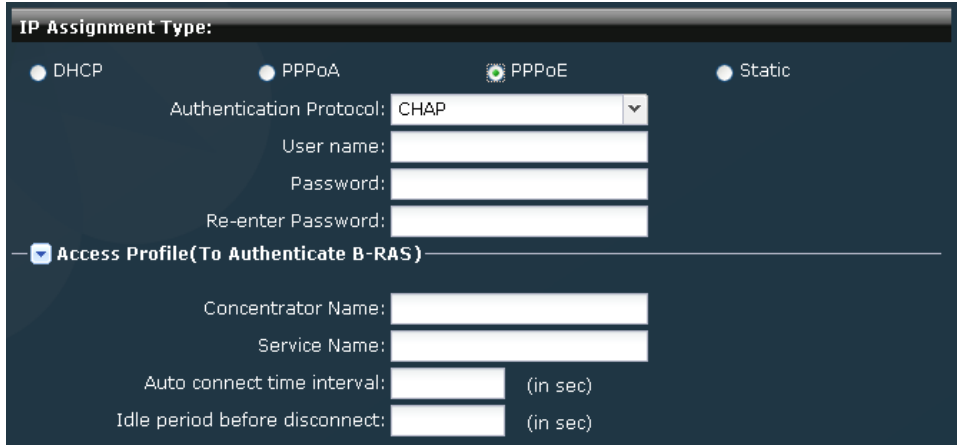
IP Assignment Type	Configuration Guidelines
PPPoA	<p data-bbox="472 386 987 420">Figure 80: PPPoA Connection Settings</p>  <ul data-bbox="472 861 1380 1092" style="list-style-type: none"> • Authentication Protocol—Select an authentication protocol. • User name—Enter a user name. • Password—Enter a password. • Re-enter Password—Reenter the password to confirm. • VPI—Enter a value for the virtual path used for this connection. • VCI—Enter a value for the virtual circuit used for this connection • Encapsulation Type—Select the type of encapsulation you intend to use for this connection.

Table 20: IP Assignment Types (*continued*)

IP Assignment Type	Configuration Guidelines
PPPoE	<p>Figure 81: PPPoE Connection Settings</p>  <ul style="list-style-type: none"> • Authentication Protocol—Select an authentication protocol. • User name—Enter a user name. • Password—Enter a password. • Re-enter Password—Reenter the password to confirm. • Concentrator Name—Enter the name of the concentrator for this connection. • Service Name—Enter a name for the service this connection uses • Auto connect time interval (in sec)—Enter a value in seconds. • Idle period before disconnect (in sec)—Enter a value in seconds.
Static	Select this option to share SSH credentials and NAT settings.

- Related Documentation**
- [Connection Profiles Overview on page 111](#)
 - [Managing Connection Profiles on page 116](#)

Managing Connection Profiles

You can view, modify, delete, copy, and search the connection profiles listed in the Connection Profiles inventory page.

You can perform the following tasks in the Connection Profiles inventory page:

1. [Viewing the Details of a Connection Profile on page 117](#)
2. [Modifying a Connection Profile on page 118](#)
3. [Deleting a Connection Profile on page 118](#)
4. [Copying a Connection Profile on page 119](#)
5. [Searching for a Connection Profile on page 119](#)

Viewing the Details of a Connection Profile

To view the details of a connection profile:


1. From the navigation ribbon, select **Devices > Deploy Devices > Connection Profiles**.

The Connection Profiles inventory page appears.

2. Double-click the icon for the connection profile you want to view.

The details of the connection profile are displayed in the Connection Profile Detail Summary report, as shown in the [Figure 82 on page 117](#).

Figure 82: Viewing the Details of a Connection Profile



The screenshot shows a window titled "Connection Profile Detail Summary" with a close button in the top right corner. The window contains three main sections: a top section with Name and Description, an "SSH Credentials" section, and a "Connection Settings" section. The "SSH Credentials" section has fields for Username and Password. The "Connection Settings" section has fields for Connection Type, Authentication Protocol, User Name, Password, Access Profile User Name, Access Profile Password, VPI, VCI, and Encapsulation Type.

Name:	Australia_PPPOA
Description:	Includes parameters for activating devices in Australia via PPPoA
SSH Credentials	
SSH Username:	root
SSH Password:	••••••••
Connection Settings	
Connection Type:	PPPoA
Authentication Protocol:	CHAP
User Name:	hkp@verizon.au.com
Password:	••••••••••••••••
Access Profile User Name:	root
Access Profile Password:	••••••••
VPI:	8
VCI:	35
Encapsulation Type:	atm-ppp-vc-mux

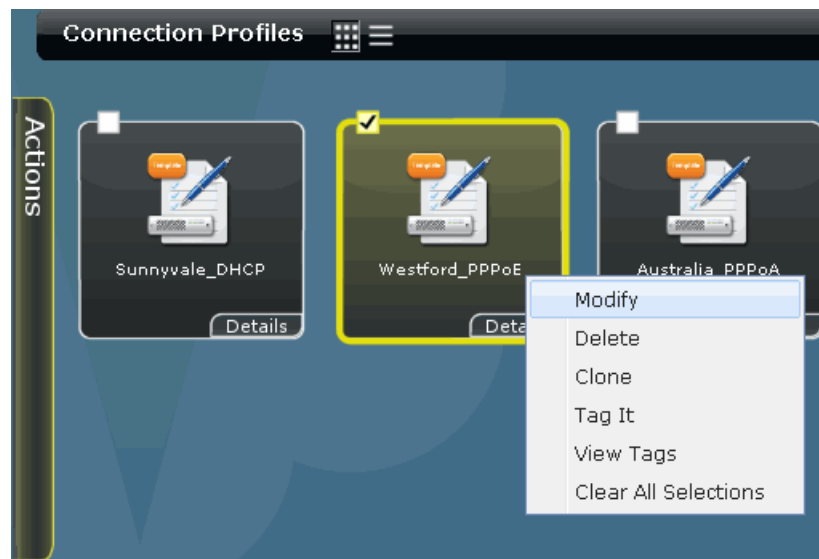
3. Click **Close**.

Modifying a Connection Profile

To modify a connection profile you have created:

1. From the navigation ribbon, select **Devices > Deploy Devices > Connection Profiles**.
The Connection Profiles inventory page appears.
2. Right-click the connection profile you want to modify and click **Modify**, as shown in [Figure 83 on page 118](#).

Figure 83: Modifying a Connection Profile



3. In the Name box, enter a new name.
4. In the Description box, enter a new description.
5. Make necessary changes in the SSH Credentials group.
6. Make necessary changes in the IP Assignment Type group.
7. Click **Modify**.

Deleting a Connection Profile

To delete a connection profile you have created:

1. From the navigation ribbon, select **Devices > Deploy Devices > Connection Profiles**.
The Connection Profiles inventory page appears.
2. Right-click the connection profile you want to delete and select **Delete**.
The Delete Connection Profile confirmation dialog box appears.
3. Click **Delete**.

Copying a Connection Profile

To copy a connection profile you have created:

1. From the navigation ribbon, select **Devices > Deploy Devices > Connection Profiles**.

The Connection Profiles inventory page appears.

2. Right-click a connection profile you want to copy and select **Clone**.

This dialog box displays the parameters of the connection profile you have copied, with the Name box left blank.

3. In the Name box, enter a name for the new connection profile.
4. Edit the other fields of the connection profile as needed.
5. Click **Create**.

The connection profile you have created appears in the Connection Profiles inventory page.

Searching for a Connection Profile

To search for a connection profile you have created:

1. From the navigation ribbon, select **Devices > Deploy Devices > Connection Profiles**.

The Connection Profiles inventory page appears.

2. In the Search box, enter the name of connection profile you want to search, as shown in [Figure 84 on page 119](#).

Figure 84: Searching for a Connection Profile



3. Click the magnifying glass icon next to the Search box.

The Connection Profiles inventory page is populated with the connection profiles matching your search criterion.

- Related Documentation**
- [Connection Profiles Overview on page 111](#)
 - [Creating Connection Profiles on page 113](#)

CHAPTER 8

Secure Console

- [Connecting to a Device on page 121](#)

Connecting to a Device

- [Secure Console Overview on page 121](#)
- [Connecting to a Device From Secure Console on page 121](#)
- [Configuring SRX Device Clusters in Junos Space on page 126](#)

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 managed device or unmanaged device. The Secure Console is a terminal window embedded in Junos Space 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 by using the credentials previously stored for the device. To connect to devices that are not managed by Junos Space, 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.

Related Documentation

- [Connecting to a Device From Secure Console on page 121](#)

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.

This topic includes the following tasks:

- [Connecting to a Managed Device on page 122](#)
- [Connecting to an Unmanaged Device on page 123](#)

Connecting to a Managed Device

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.
- The status of the managed device must be “UP”

You can use Secure Console to establish a connection to a Junos Space 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:

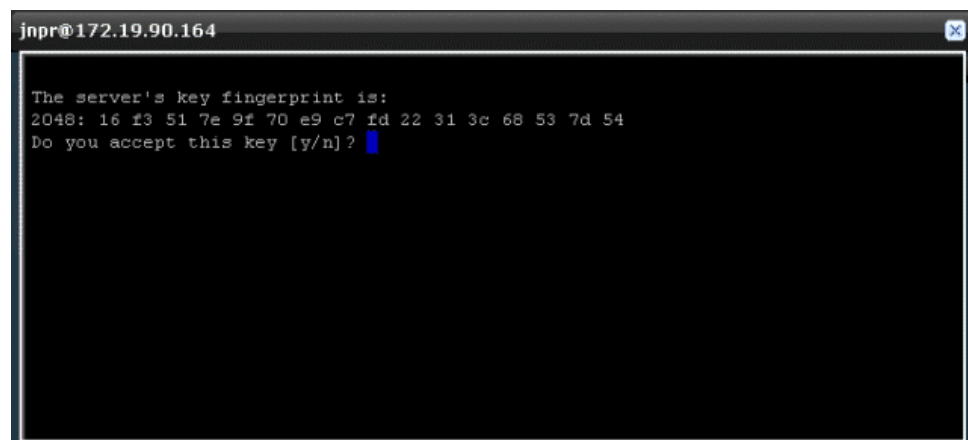
1. From the navigation ribbon, select **Devices > Manage Devices**.

The Manage Devices inventory page displays managed devices by name and IP address.

2. Select a device by clicking on the thumbnail image for the device or selecting the table row for the device.
3. In the Actions drawer, click **Secure Console**.

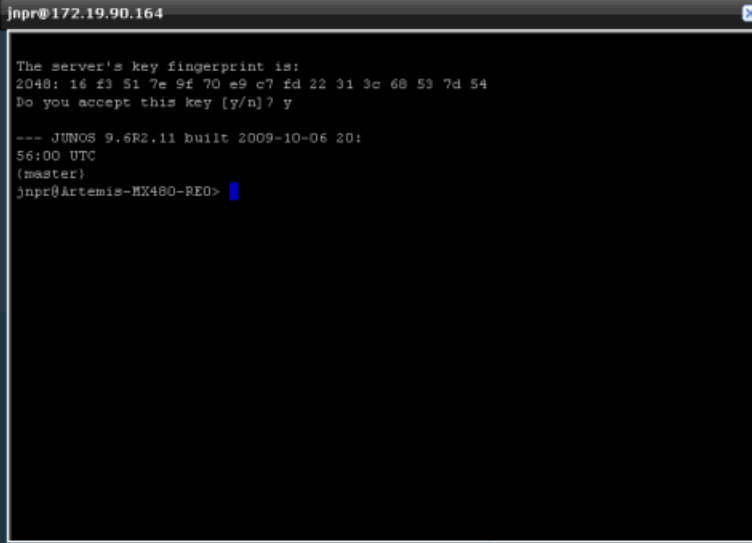
A window appears that prompts you to validate the device key fingerprint, as shown in the following illustration.

Figure 85: Secure Console Window



4. 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 the SSH connection opened on the selected device, as shown in the following example.



```

jnpr@172.19.90.164
The server's key fingerprint is:
2048: 16 f3 51 7e 9f 70 e9 c7 fd 22 31 3c 68 53 7d 54
Do you accept this key [y/n]? y

--- JUNOS 9.6R2.11 built 2009-10-06 20:
56:00 UTC
(master)
jnpr@Artemis-MX480-PE0>

```



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

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

Connecting to an Unmanaged Device

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.
- The device is configured with a static management IP address that is reachable from the Junos Space appliance.
- SSH v2 is enabled on the device. To enable SSH v2 on a device, issue the following CLI command:

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

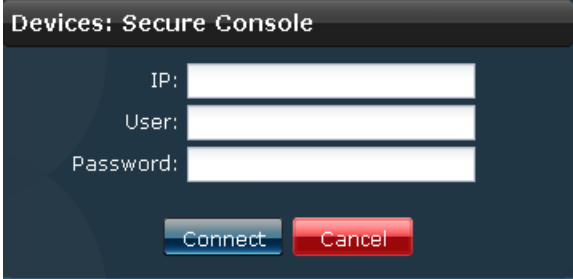
- The status of the device must be “UP”
- A valid user name and password is created on the device.

To connect to an unmanaged device:

1. From the navigation ribbon, select **Devices > Secure Console**.

The Secure Console dialog box appears, as shown in the following illustration.

Figure 86: Secure Console Dialog Box

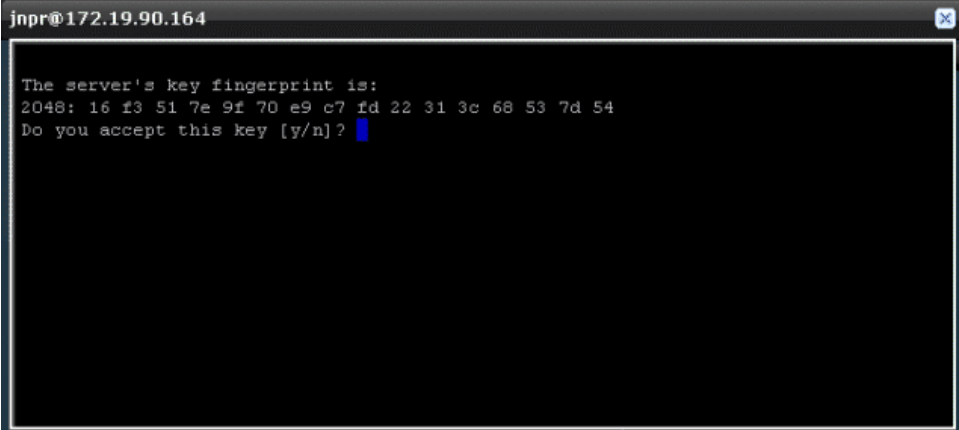
The image shows a dialog box titled "Devices: Secure Console". It has a dark blue background. Inside, there are three white input fields stacked vertically. The first field is labeled "IP:", the second "User:", and the third "Password:". Below these fields are two buttons: a blue "Connect" button and a red "Cancel" button.

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

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

4. Click **Connect**.

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



```

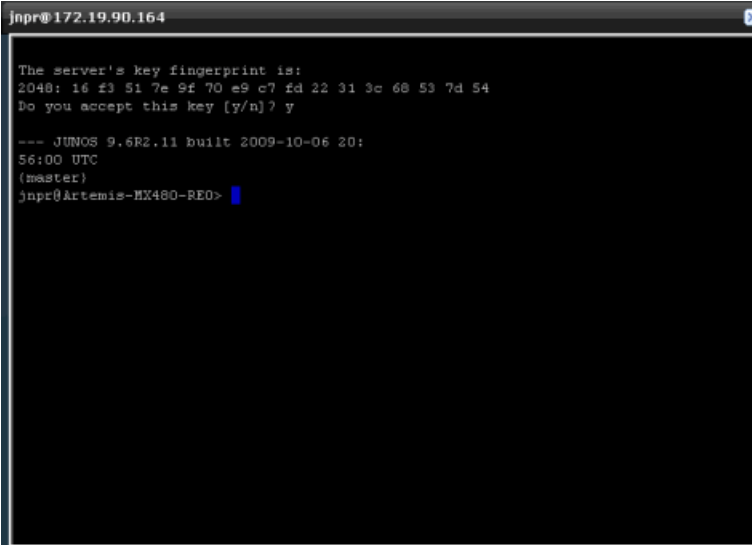
jnpr@172.19.90.164

The server's key fingerprint is:
2048: 16 f3 51 7e 9f 70 e9 c7 fd 22 31 3c 68 53 7d 54
Do you accept this key [y/n]? 

```

5. Verify that the fingerprint is for the device you want to connect to, and type **y** and press Enter to validate the Server's key fingerprint.

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



```

jnpr@172.19.90.164

The server's key fingerprint is:
2048: 16 f3 51 7e 9f 70 e9 c7 fd 22 31 3c 68 53 7d 54
Do you accept this key [y/n]? y

--- JUNOS 9.6R2.11 built 2009-10-06 20:
56:00 UTC
(master)
jnpr@Artemis-MX480-PE0> 

```



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

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

Secure Console supports the following terminal control characters:

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

Related Documentation

- [Secure Console Overview on page 121](#)

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.

This topic includes the following tasks:

- [Configuring a Standalone Device from a Single-node Cluster on page 126](#)
- [Configuring a Standalone Device from a Two-Node Cluster on page 128](#)
- [Configuring a Primary Peer in a Cluster from a Standalone Device on page 129](#)
- [Configuring a Secondary Peer in a Cluster from a Standalone Device on page 130](#)

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. From the navigation ribbon, select **Devices > Secure Console**.

The Secure Console dialog box appears.

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

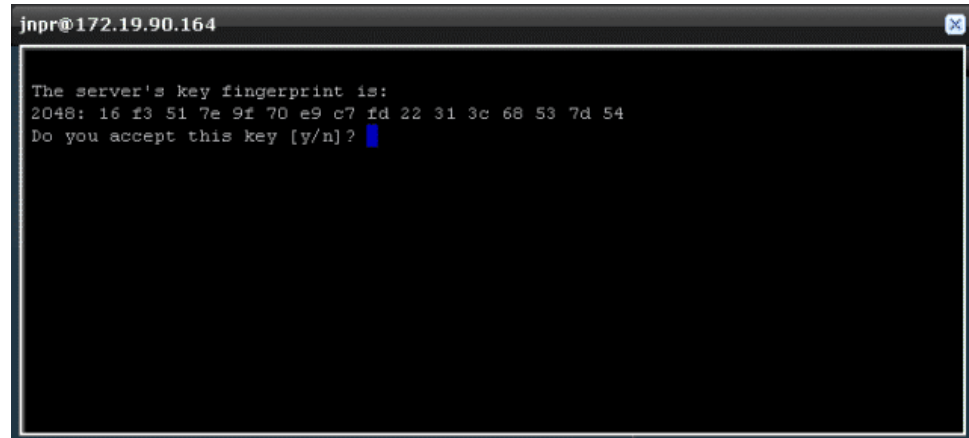


NOTE: A device in a single-node cluster is always the primary member.

3. To establish an SSH connection for the device, specify the administrator user name and password. The name and password must match the name and password configured on the device.

4. Click **Connect**.

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



5. Verify that the fingerprint is for the device you want to connect to, then type **y** and press Enter to validate the Server's key fingerprint.

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

6. Enter the set chassis command to remove the cluster configuration:

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

7. Reboot the device, by entering the command:

```
request system reboot
```

8. Copy the outbound-ssh configuration from group node to system level, for example:

```
set system services outbound-ssh client 00089BBC494A device-id 6CFF68
set system services outbound-ssh client 00089BBC494A secret
"$9$-zbgoDikf5zDjuOISyW8Xxbs"
set system services outbound-ssh client 00089BBC494A services netconf
set system services outbound-ssh client 00089BBC494A 10.155.70.252 port 7804
```

9. Copy the syslog configuration from group node to system level:

```
set system syslog file default-log-messages any any
set system syslog file default-log-messages structured-data
```

10. Copy the fxp0 interface setting from group node to system level, for example:

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

11. Delete the outbound-ssh configuration from the group node, for example:

```
delete groups node0 system services outbound-ssh
```

12. Delete the syslog configuration from the group node, for example:

```
delete groups node0 system syslog file default-log-messages any any
delete groups node0 system syslog file default-log-messages structured-data
```

13. Delete the interfaces configuration from the group node, for example:

```
delete groups node0 interfaces fxp0 unit 0 family inet address 10.155.70.223/19
```

14. Commit the configuration changes on the device:

```
commit
```

In the Junos Space user interface, the device connection status will go down and then up again. After the device connection is back up, you can verify that the device you configured displays as a standalone device.

15. To terminate the SSH session, type **exit** from the terminal window prompt, and press Enter.
16. Click in the top right corner of the terminal window to close the window.

Configuring a Standalone Device from a Two-Node Cluster

You can configure a standalone device from the secondary peer device in a cluster.



NOTE: You cannot use the primary peer in a two-node cluster to configure a standalone device.

To configure a secondary peer device in a cluster as a standalone device:

1. From the navigation ribbon, select **Devices > Secure Console**.

The Secure Console dialog box appears.

2. Specify the IP address of the secondary peer device.
3. To establish an SSH connection for the device, specify the administrator user name and password. The name and password must match the name and password configured on the device.
4. Click **Connect**.

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

5. Verify that the fingerprint is for the device you want to connect to, then type **y** and press Enter to validate the Server's key fingerprint.

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

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

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

8. Reboot the device, by entering the command:

```
request system reboot
```

9. Copy the outbound-ssh configuration from group level to system level, for example:

```
set system services outbound-ssh client 00089BBC494A device-id 6CFF68
set system services outbound-ssh client 00089BBC494A secret
"$9$-zbgoDikf5zDjuO1ISyW8Xxbs"
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 syslog configuration from group level to system level:

```
set system syslog file default-log-messages any any
```

```
set system syslog file default-log-messages structured-data
```

11. Copy the fxp0 interface setting from group level to system level, for example:

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

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

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

13. Delete the syslog configuration from the group level, for example:

```
delete groups node1 system syslog file default-log-messages any any
delete groups node1 system syslog file default-log-messages structured-data
```

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

```
delete groups node1 interfaces fxp0 unit 0 family inet address 10.155.70.223/19
```

15. Commit the configuration changes on the device:

```
commit
```

In the Junos Space user interface, the device connection status will go down and then up again. After the device connection is back up, you can verify that the device you configured displays as a standalone device.

After the device connections are up, verify the following changes in the Manage Devices inventory landing page:

- The device you configured now displays as a standalone device.
 - The cluster that formerly included a primary and secondary peer device now displays the primary peer device only.
16. To terminate the SSH session, type **exit** from the terminal window prompt, and press Enter.
 17. Click in the top right corner of the terminal window to close the window.

Configuring a Primary Peer in a Cluster from a Standalone Device

You can create a device cluster from two standalone devices. Use the following procedure to configure a standalone device as the primary peer in a cluster.

To configure a primary peer in a cluster from a standalone device:

1. From the navigation ribbon, select **Devices > Secure Console**.

The Secure Console dialog box appears.

2. Specify the IP address of the standalone device that you want to configure as the primary peer in the cluster.
3. To establish an SSH connection for the device, specify the administrator user name and password. The name and password must match the name and password configured on the device.
4. Click **Connect**.
The device key fingerprint window appears.
5. Verify that the fingerprint is for the device you want to connect to, and type **y** and press Enter to validate the Server's key fingerprint.

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

6. For the standalone device, enter the command:

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

7. Reboot the device, by entering the command:

```
request system reboot
```

8. Copy the outbound-ssh configuration from the system level to the group level, for example:

```
set groups node0 system services outbound-ssh client 00089BBC494A device-id 6CFF68  
set groups node0 system services outbound-ssh client 00089BBC494A secret  
"$9$-zbgoDikf5zDjuO1ISyW8Xxbs"  
set groups node0 system services outbound-ssh client 00089BBC494A services netconf  
set groups node0 system services outbound-ssh client 00089BBC494A 10.155.70.252 port  
7804
```

9. Copy the fxp0 interface configuration from the system level to the group level, for example:

```
set groups node0 interfaces fxp0 unit 0 family inet address 10.155.70.223/19
```

10. Copy the syslog configuration from system level to group level:

```
set groups node0 system syslog file default-log-messages any any  
set groups node0 system syslog file default-log-messages structured-data
```

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

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

12. Delete the syslog configuration from the system level, for example:

```
delete system syslog file default-log-messages any any  
delete system syslog file default-log-messages structured-data
```

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

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

14. Commit the configuration changes on the device again:

```
commit
```

After the device connection is up, verify the following changes:

- In the Manage Devices inventory landing page:
 - The cluster icon appears for the device.
 - The new cluster device appears as the primary device.
 - In the physical inventory landing page, Junos Space displays chassis information for the primary device cluster.
15. To terminate the SSH session, type **exit** from the terminal window prompt, and press Enter.
 16. Click in the top right corner of the terminal window to close the window.

Configuring a Secondary Peer in a Cluster from a Standalone Device

If a device cluster contains only a primary peer, you can configure a standalone device to function as a secondary peer in the cluster. Use the following procedure to ensure that Junos Space is able to manage both devices.

To add a standalone device to a cluster:

1. From the navigation ribbon, select **Devices > Secure Console**.

The Secure Console dialog box appears.

2. Specify the IP address of the standalone device that you want to configure as a secondary peer in a cluster.
3. To establish an SSH connection for the device, specify the administrator user name and password. The name and password must match the name and password configured on the device.

4. Click **Connect**.

The device key fingerprint window appears.

5. Verify that the fingerprint is for the device you want to connect to, and type **y** and press Enter to validate the Server's key fingerprint.

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

From the terminal window prompt, you can enter CLI commands to create a standalone device from the device cluster.

6. For the standalone device, enter the command:

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

7. Enter the command:

```
request system reboot
```

8. Copy the outbound-ssh configuration from the system level to the group level, for example:

```
set groups node1 system services outbound-ssh client 00089BBC494A device-id 6CFF68
set groups node1 system services outbound-ssh client 00089BBC494A secret
"$9$-zbgoDikf5zDjuO1ISyW8Xxbs"
set groups node1 system services outbound-ssh client 00089BBC494A services netconf
set groups node1 system services outbound-ssh client 00089BBC494A 10.155.70.252 port
7804
```

9. Copy the fxp0 interface configuration from the system level to the group level, for example:

```
set groups node1 interfaces fxp0 unit 0 family inet address 10.155.70.223/19
```

10. Copy the syslog configuration from system level to group level:

```
set groups node1 system syslog file default-log-messages any any
set groups node1 system syslog file default-log-messages structured-data
```

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

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

12. Delete the syslog configuration from the system level, for example:

```
delete system syslog file default-log-messages any any
delete system syslog file default-log-messages structured-data
```

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

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

14. Commit the configuration changes on the device again:

commit

15. Connect the HA cable to each device in the cluster.
16. Establish an SSH connection to the primary device in the cluster.
17. On the primary device, make some trivial change to the device, for example, add a description, and commit the change:

commit

After the device connections are up for both devices in the cluster, verify the following changes:

- In the Manage Devices inventory landing page:
 - Each peer device displays the other cluster member.
 - The cluster icon appears for each member device.
 - One device appears as the primary device and the other as the secondary device in the cluster.
 - In the physical inventory landing page, chassis information appears for each peer device in the cluster.
18. To terminate the SSH sessions, type **exit** from the terminal window prompt, and press Enter.
 19. Click in the top right corner of the terminal window to close the window.

CHAPTER 9

Device Adapters

- Installation/Management on page 133

Installation/Management

- Screen OS Software Adapter Overview on page 133
- Installing the ScreenOS Software Adapter for Managing Non-DMI Security Devices on page 134
- Deleting a ScreenOS Adapter on page 140
- Worldwide Junos OS Adapter Overview on page 140
- Installing the Worldwide Junos OS Adapter on page 141

Screen OS Software Adapter Overview

The Junos Space ScreenOS (SOS) software adapter makes it possible for you to manage Juniper Networks non-DMI security devices through Junos Space. Use the SOS Adapter to manage all security devices supported by ScreenOS, Version 6.0 or later. For a list of supported devices refer to the Juniper Web site:

<http://www.juniper.net/us/en/products-services/>

Before you can install the ScreenOS Adapter, complete the following prerequisites:

- The ScreenOS Adapter image has been downloaded to the local client workstation.
- The ScreenOS Firewall device has been deployed on the network.
- Junos Space servers must have been deployed and are reachable from the device you plan to add to Junos Space.

Related Documentation

- [Installing the ScreenOS Software Adapter for Managing Non-DMI Security Devices on page 134](#)
- [Deleting a ScreenOS Adapter on page 140](#)

Installing the ScreenOS Software Adapter for Managing Non-DMI Security Devices

This document describes the process for installing the ScreenOS Software Adapter. The ScreenOS software Adapter allows you to manage Juniper Networks non-DMI security devices through Junos Space.

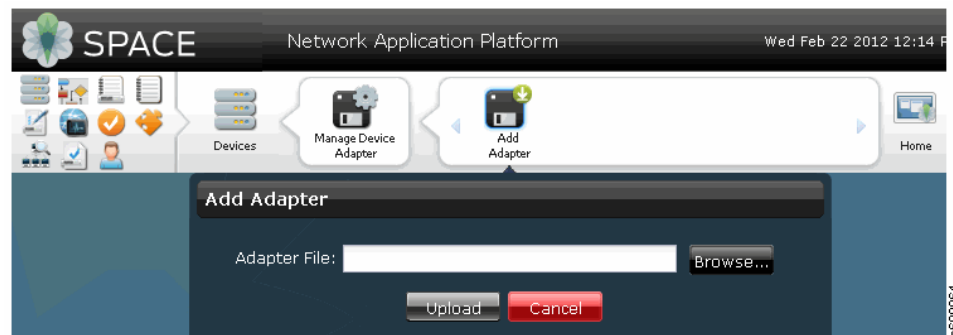
This multi-task process includes instructions for

1. [Uploading the SOS Adapter Image on page 134](#)
2. [Installing the ScreenOS Adapter on page 134](#)
3. [Verifying the SOS Adapter Installation on page 135](#)
4. [Adding Screen OS Devices to Junos Space on page 136](#)
5. [Uploading the Device Management Commands on page 139](#)

Uploading the SOS Adapter Image

Before you can install the SOS Adapter, you need to upload the image. Navigate to the Upload screen on the Devices task page.

1. Navigate to **Network Application Platform > Devices > Manage Device Adapter > Upload Adapter**
2. Browse to the adapter image file and select the filename so that the full path appears in the Software File field.
3. Click Upload to bring the image into Junos Space. A pop-up window shows the progress of the image upload.



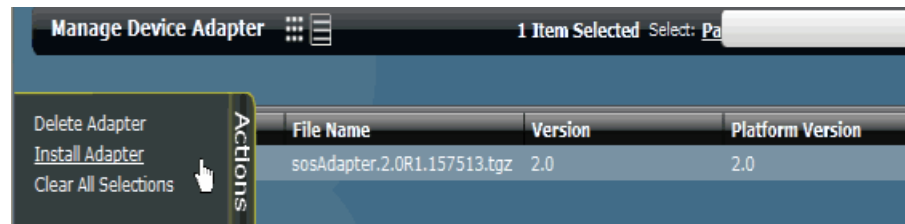
Installing the ScreenOS Adapter

Once you install the SOS Adapter, you will be able to add devices supported by ScreenOS so that they can be monitored and managed through the Devices workspace.

To install the SOS Adapter from the image you just uploaded, follow these steps:

1. Navigate to **Network Application Platform > Devices > Manage Device Adapter**. The Manage Software window appears with the SOS Adapter showing in the list of manageable devices.

2. Select the SOS Adapter and open the Action drawer to see the list of tasks that you can perform.



3. Click Install Software from the action list. The adapter starts automatically when it is installed.

Verifying the SOS Adapter Installation

Before you add any devices, verify that the installation was successful. This procedure shows how to verify the installation, as well as stop and start the adapter as needed.

To verify that the installation was successful, look at the device console on the Space server.

1. On the server, change directories to verify that the SOS Adapter directory has been created.

```
cd /home/jmp/
sosadapter
```

2. To verify that the SOS Adapter is running, enter the following command on the Space server:

```
Router > service sosadapter status
service adapter start to start the adapter
```

If the SOS Adapter is not active, you will see the status as

```
service adapter stop to stop the adapter
```

Use the following commands to either start or stop the SOS Adapter:

```
service adapter start to start the adapter
```

```
service adapter stop to stop the adapter
```

3. To see the SOS Adapter logs, change directories to the adapter directory.

```
cd /home/jmp/sosadapter/var/errorlog
sosadapterserver.0
```

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

Adding Screen OS Devices to Junos Space

You can register supported devices with Junos Space so that they can be managed through the Manage Devices task. You can add one or more devices by uploading a comma-separated values (.CSV) file that contains the device definitions, or you can manually add one device at a time by entering the device information.

To add ScreenOS devices, navigate to **Network Application Platform > Devices > Add Deployed Devices > Add Device**

Add Devices

Name:

Description:

Note: Only ScreenOS devices are supported with this workflow. You need to paste the generated CLIs on the device console.

☒ Import From CSV ☐ Add Manually

Import

[View Sample CSV](#)

[Select a CSV To Upload](#)

Adding Devices Manually

This procedure describes how to add devices manually, one at a time.

1. From the list of devices displayed in the device wizard, select the newly uploaded adapter.

Add Devices

Name:

Description:

Note: Only ScreenOS devices are supported with this workflow. You need to paste the generated CLIs on the device console.

☐ Import From CSV ☒ Add Manually

Device Details

Platform:

OS Version:

Number of devices:

Authentication Details

User Name:

Password:

Re-enter Password:

Adding Devices Using a .CSV File

This procedure describes how to add a group of devices by uploading a .CSV file.



NOTE: You must create the .CSV file before you begin this procedure.

In the .CSV file you define each device by providing the following information for each device:

- Device name
- Platform
- Screen OS Version

To see a sample .CSV file, click [View Sample .CSV](#). The following figure illustrates the format to use for the .CSV file.

	A	B	C	D	E
1	#Rows which start with '#' are treated as a commented row				
2	#Explanation for the Column Names				
3	#Device Name - The name of the device to be created in SPACE.				
4	#				
5	#Platform - The SSG20-WLAN)				
6	#				
7	#OS Version - The ScreenOS version of the box				
8	#				
9	#Device Name	Platform	OS Version		
10	Seattle_ISG	nsISG1000	6		
11	Toronto_SSG	SSG550	6.1		
12	Auckland_SSG	SSG350	6.1		
13	UK_SSG	SSG20-WLAN	6.1		
14					

To upload the .CSV file, follow these steps:

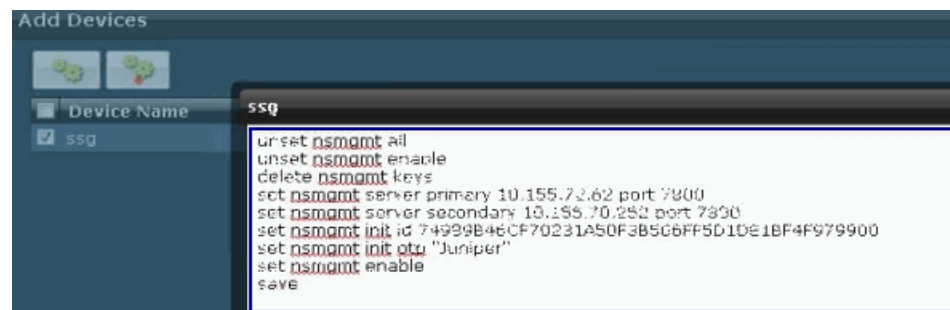
1. Click the .CSV radio button to open the File Upload window.
2. Browse to the .CSV file that you have created and select it so that the full path appears in the .CSV File field.



3. Click Upload.

Uploading the Device Management Commands

A set of management commands is created automatically for each device you add. The following figure shows the set of commands you will see for the SOS Adapter.



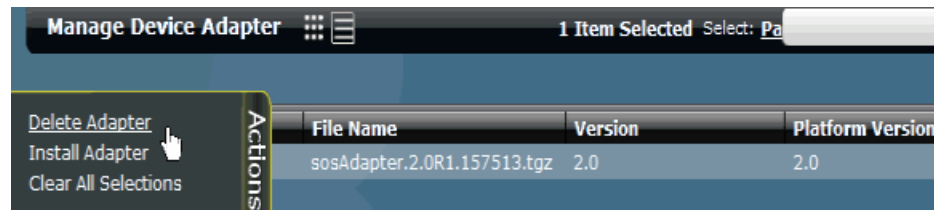
You must copy the entire set of commands for each device into the device console. You must repeat this procedure for each device you add. To retrieve the device management commands, perform the following steps:

1. Navigate to **Network Application Platform > Devices > Manage Devices > View Management CLI**
2. Select the device you have added to display the management commands for that device.
3. Copy the entire set of commands.
4. Past the copied commands into the device console.
5. Click Finish to complete the installation.

Deleting a ScreenOS Adapter

To delete a ScreenOS adapter, navigate to **Network Application Platform > Devices > Manage Devices**.

- In the device list, select the ScreenOS adapter that you want to delete.
- Open the Action Drawer.



- Click **Delete Adapter**.

Related Documentation

- [Add Deployed Devices Wizard Overview on page 51](#)
- [Adding Deployed Devices on page 52](#)
- [Managing Deployed Devices on page 54](#)
- [Installing the ScreenOS Software Adapter for Managing Non-DMI Security Devices on page 134](#)

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.

ww Junos OS devices use Telnet instead of Secure Shell (SSH2) to communicate with other network elements. Junos Space 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 identifies the device as a ww Junos OS device. Since Junos Space does not support Telnet, it uses an adapter to communicate with ww Junos OS devices. Junos Space 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 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 needs a minimum of three Telnet connections with the device in order to be able to manage it.



NOTE: For ww Junos OS devices, the Junos Space Service Now application works only on AI-Scripts version 2.5R1 and later.

The Secure Console workspace and the option in the right-click context menu in the Manage Devices workspace are disabled for ww Junos OS devices.

For more information, see “Installing the Worldwide Junos OS Adapter” on page 141.

Related Documentation

- [Installing the Worldwide Junos OS Adapter on page 141](#)

Installing the Worldwide Junos OS Adapter

This section shows you how to install and use the wwadapter to manage devices running on the worldwide version of Junos OS (ww Junos OS devices).

This section includes the following tasks:

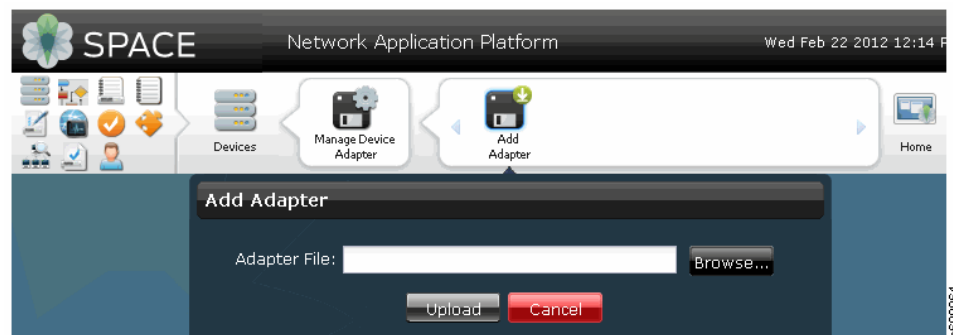
- [Installing the wwadapter Image on page 141](#)
- [Connecting to ww Junos OS Devices on page 143](#)

Installing the wwadapter Image

Before you install the wwadapter, you must upload the ww Junos OS device wwadapter image file.

To upload the wwadapter image file:

1. From the application chooser, select **Network Application Platform > Devices > Manage Device Adapter > Upload Adapter**.



2. Browse to the wwadapter image file and select the filename so that the full path appears in the Software File field.
3. Click **Upload** to bring the image into Junos Space.

A status box shows the progress of the image upload.

To install the ww Junos OS device wwadapter:

1. From the application chooser, select **Network Application Platform > Devices > Manage Device Adapter**.

The Manage Device Adapter dialog box appears with the wwadapter displayed in the list of manageable adapters.

2. Select the adapter and select **Install Software** from the Actions drawer.

The adapter starts automatically after installation.

Before you connect to any device, you must verify that the installation was successful.

To verify that the installation was successful, look at the device console on the Space server.

1. On the server, change directories to verify that the wwadapter directory has been created.

```
cd /home/jmp/wwadapter
```

2. To verify that the wwadapter is running, enter the following command on the Space server:

```
prompt > service wwadapter status  
wwadapter running
```

If the wwadapter is not active, you see the following status:

```
wwadapter stopped
```

Use the following commands to start or stop the wwadapter:

To start the wwadapter:

```
service wwadapter start
```

To stop the wwadapter:

```
prompt > ps -ef | grep wwadapter  
prompt > kill -9 {wwadapter pid}
```

To see the wwAdapter logs, change directories to the wwadapter directory.

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

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

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

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

Connecting to ww Junos OS Devices

A device running worldwide Junos OS (ww Junos OS device) cannot initiate a connection with Junos Space. Junos Space must initiate the connection to the device. To configure this setting:

1. From the application chooser, select **Network Application Platform > Administration > Manage Applications**.

The Manage Applications page appears displaying all the applications currently running in the Junos Space server.

2. Select **Network Application Platform** and click **Modify Application Settings** from the Actions drawer.

The Modify Application Settings page appears.

3. Select **Junos Space initiates connection to device**.
4. Select **Support ww Junos Devices** so that Junos Space can connect to a ww Junos OS device using the wwadapter.

After Junos Space has discovered the ww Junos OS device through the wwadapter ([“Discovering Devices” on page 40](#)), it manages the device just as it would manage a device that runs the domestic version of Junos OS.



NOTE: The Secure Console workspace and the SSH to Device option on the right-click contextual menu in the Manage Devices workspace are disabled for ww Junos OS devices.



NOTE: If you are not able to discover the WW Junos OS device, make sure that the NMAP utility returns ‘telnet’ as open for port 23 on the device.

```
$ nmap -p23 < Device IP >
```

Related Documentation • [Modifying Application Settings on page 454](#)

CHAPTER 10

Discovering Topologies

- [Topology Discovery Overview on page 145](#)
- [Discovering a Topology on page 148](#)
- [Managing Device Targets on page 149](#)
- [Managing SNMP Probes on page 151](#)

Topology Discovery Overview

Topology discovery is the process of discovering information about network devices and their interconnections. The topology discovery process creates a topology map that displays how the devices in the network are connected. You can use topology maps to monitor the network and ensure that the network is functioning effectively. You can identify weaknesses in the network infrastructure, such as bottlenecks and failures within a network, and isolate problem areas when you are troubleshooting network problems.

Using Discover Topology, you can search for network topologies based on a target device or subnet that you specify. When you discover a topology, Topology Visualization creates objects in the Junos Space database representing all the discovered devices and links.

Topology Discovery consists of two main steps:

1. Specifying the device target

To discover a topology using Topology Discovery, you must first specify a device target. This device initiates topology discovery. Junos Space searches for all the devices and subnets that are connected to the specified device. You can specify either the hostname or IP address of the device target. You can also use a range of IP addresses or an IP subnet to initiate topology discovery.

2. Specifying the SNMP probes

Junos Space uses SNMP to discover network elements that are connected to the specified target devices and subnets. The Junos Space server uses SNMP probes to contact the targeted devices and get the relevant management information base (MIB) information needed to compute the topology.

You can also specify a hop count to limit the number of routers that you want Junos Space to discover from the specified device. For example, if you specify a hop count of 1 for a target device, then all the IP addresses present in the routing table of that

device are targeted for discovery. If the hop count is 2, this process is repeated for all the routing tables of the devices that were discovered in the first hop.

For more information about how to discover a topology, see [“Discovering a Topology” on page 148](#).

To go to the Discover Topology task, select **Platform** on the application switcher, and select **Topology Visualization > Discover Topology**.

The Discover Topology landing page appears ([Figure 87 on page 146](#)) displaying details of the last topology discovery job that was carried out as described in [Table 21 on page 146](#).

Figure 87: Discover Topology

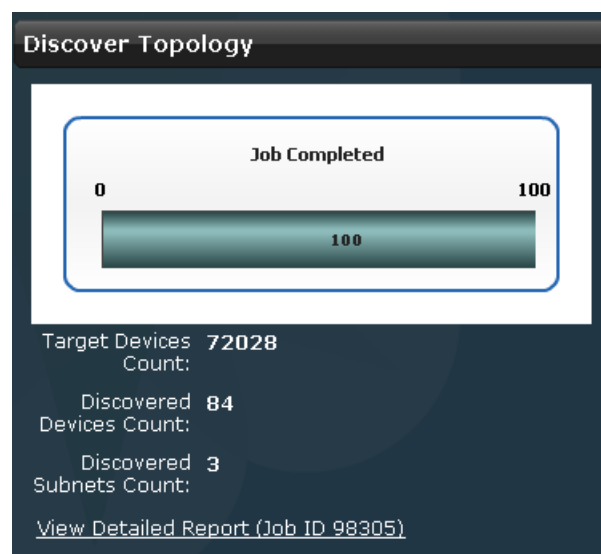


Table 21: Discover Topology Landing Page Field Name and Descriptions

Field Name	Description
Job Completion bar	How much of the job is completed as a percentage
Target Devices Count	Number of target devices that were specified for the job
Discovered Devices Count	Number of devices that were discovered
Discovered Subnets Count	Number of subnets that were discovered
View Detail Report	Link to the Discovery Job Details dialog box

The Discovery Job Details report displays information about the discovery job, as shown in [Figure 88 on page 147](#). [Table 22 on page 147](#) describes the report.

Figure 88: Discovery Job Details Report

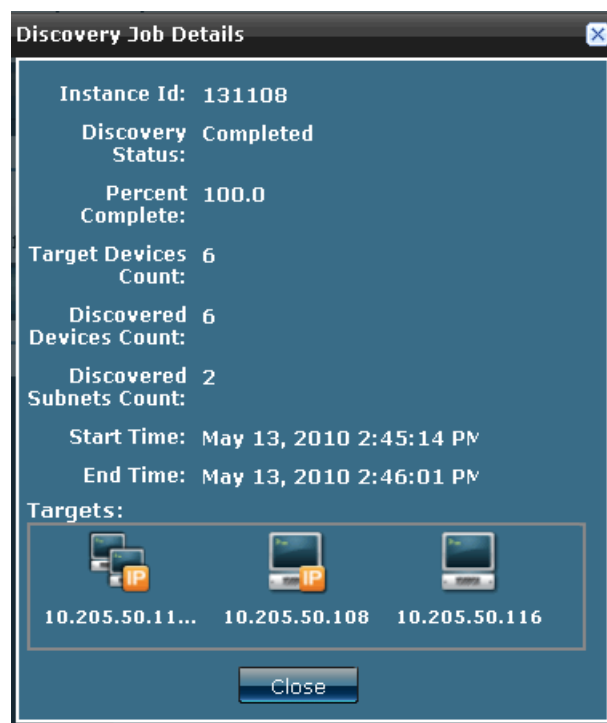


Table 22: Discovery Job Details Field Names and Descriptions

Field Name	Description
Instance ID	Unique identification number of the topology discovery job
Discovery Status	Job status The status can be Starting , In Progress , Stopped , Completed , or Fail .
Percent Complete	How much of the job was completed The value ranges from 0.0 to 100.0.
Target Devices Count	Number of target devices that were specified for the job
Discovered Devices Count	Number of devices that were discovered
Discovered Subnets Count	Number of subnets that were discovered
Start Time	Date and time when the job started
End Time	Date and time when the job was completed
Targets	Targets and corresponding IP addresses that were specified for the discovery job

Prerequisites for Discovering a Topology

For Junos Space to discover a topology, the following conditions must be met.

- SNMP credentials must be configured on all the targeted devices in the network.
- Either LLDP or xSTP protocols must be enabled on all the devices in the network.

To view logs of tasks performed from the Topology Visualization user interface, select **Audit Logs > View Audit Logs**. Audit logs list information about the task, such as task name, result, description, and job ID. For more information about audit logs, see [“Junos Space Audit Logs Overview” on page 357](#).

Related Documentation

- [Discovering a Topology on page 148](#)

Discovering a Topology

To discover a topology:

1. From the navigation ribbon, select **Topology Visualization > Discover Topology > Specify Targets**.

The Topology Visualization Workspace: Specify Targets page appears, as shown in [Figure 89 on page 148](#).

Figure 89: Specify Device Targets



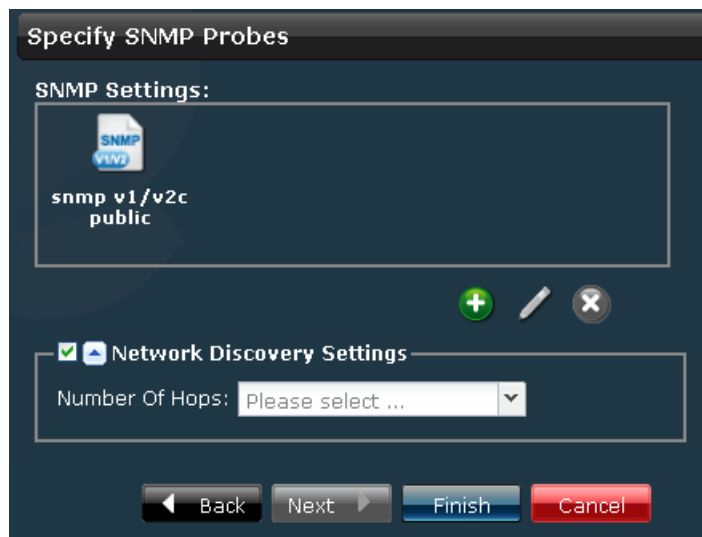
Here you can add, edit, or delete device targets. For more information, see [“Managing Device Targets” on page 149](#).

2. (Optional) You can select the **Include Managed Devices as Targets** check box if you want Junos Space to use the Juniper Networks devices as the target devices for topology discovery.
3. Click **Next** to open the Specify SNMP Probes page, as shown in [Figure 90 on page 149](#).

Alternatively, click **Finish** to discover topologies based on the seed devices that you have specified.

You can also click **Cancel** to go back to the Discover Topology page.

Figure 90: Specify SNMP Probes



On the Specify SNMP Probes page, you can add, edit, or delete SNMP probes that specify how Junos Space discovers the network. See [“Managing SNMP Probes” on page 151](#).

4. (Optional) You can specify a hop count to limit the number of routers from the target that Junos Space tries to discover. To do so, select the **Network Discovery Settings** check box and select the number of hops from the Number of Hops list.

The hop count limits the number of routers from the target device that you want Junos Space to discover.

5. Click **Finish** to discover topologies based on the seed devices and SNMP probe settings that you have specified.

Alternatively, click **Back** to go to the previous step of the Discover Topology wizard. You can also click **Cancel** to go back to the Discover Topology page

- Related Documentation**
- [Topology Discovery Overview on page 145](#)
 - [Managing Device Targets on page 149](#)
 - [Managing SNMP Probes on page 151](#)

Managing Device Targets

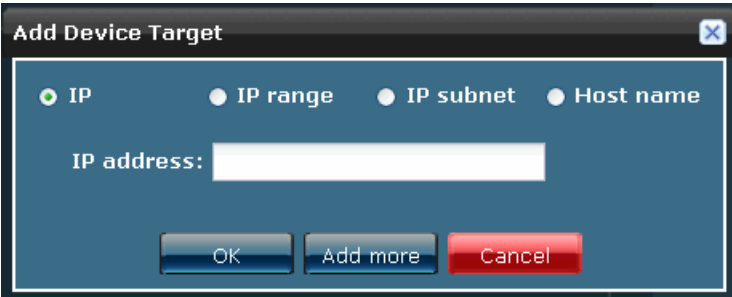
To add a target:

1. From the task ribbon, select **Topology Visualization > Discover Topology > Specify Target**.

The **Topology Visualization Workspace: Specify Target** page appears.

2. Click the Add (+) button to open the **Add Device Target** dialog box ([Figure 91 on page 150](#)).

Figure 91: Add Device Target Dialog Box

The image shows a dialog box titled "Add Device Target" with a close button (X) in the top right corner. Inside the dialog, there are four radio buttons: "IP" (which is selected), "IP range", "IP subnet", and "Host name". Below these buttons is a text input field labeled "IP address:". At the bottom of the dialog, there are three buttons: "OK", "Add more", and "Cancel".

3. Select one of the following options and enter the appropriate value in the field provided.
 - **IP**—Select this option to discover devices that are connected to the target device whose IP address you specified. Enter the IP address of the device in the **IP address** field. For example, 10.204.33.1.
 - **IP range**—Select this option to discover the network devices and connections that are connected to the target devices whose IP addresses you specified. Enter the addresses in the **IP range** field. For example, 10.204.33.1-10.204.33.20.
 - **IP subnet**—Select this option to discover the network devices and connections that are connected to the target subnets whose IP address you specified. Enter the IP address of the subnet in the **IP subnet** field. For example, 10.204.33.1 / 24.
 - **Hostname**—Select this option to discover the network devices and connections that are connected to the target device whose hostname you specified. Enter the hostname in the **Hostname** field.
4. Click **OK** to close the **Add Device Target** dialog box and add the device target to the **Device Targets** list.

Alternatively, click **Add More** to add the device target to the list without closing the **Add Device Target** dialog box so that you can add more device targets to the device targets list.

You can also click **Cancel** to close the **Add Device Target** dialog box without adding any device targets.

To edit a target:

1. From the task ribbon, select **Topology Visualization > Discover Topology > Specify Target**. The **Topology Visualization Workspace: Specify Target** dialog box appears.
2. Select the device target that you want to edit and click **Edit** to open the **Edit Device Target** dialog box.

3. Select one of the following options and enter the appropriate value in the field provided.

You can choose to edit the existing values in the selected option, or you can select a different option and enter the desired values for that option.

- **IP**—Select this option to discover devices that are connected to the target device whose IP address you specified. Enter the IP address of the device in the **IP** field. For example, 10.204.33.1.
 - **IP range**—Select this option to discover the network devices and connections that are connected to the target devices whose IP addresses you specified. Enter the addresses in the **IP range** field. For example, 10.204.33.1-10.204.33.20.
 - **IP subnet**—Select this option to discover the network devices and connections that are connected to the target subnets whose IP address you specified. Enter the IP address of the subnet in the **IP subnet** field. For example, 10.204.33.1 / 24.
 - **Hostname**—Select this option to discover the network devices and connections that are connected to the target device whose hostname you specified. Enter the hostname in the **Hostname** field.
4. Click **OK** to save your changes and close the **Edit Device Target** dialog box. Alternatively, click **Cancel** to close the **Edit Device Target** dialog box without editing the device target.

To delete a target:

1. From the task ribbon, select **Topology Visualization > Discover Topology > Specify Target**.

The **Topology Visualization Workspace: Specify Target** dialog box appears.

2. Select the device target that you want to delete and click **Delete** to open the **Delete Device Target** dialog box.
3. Click **OK** to delete the device target and remove it from the device targets list.

Click **Cancel** to close the **Delete Device Target** dialog box without deleting a target.

Related Documentation

- [Discovering a Topology on page 148](#)

Managing SNMP Probes

You can specify an SNMP probe to connect to and discover the devices in a network.

To add an SNMP probe:

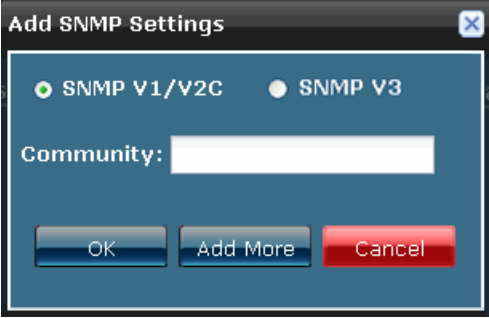
1. From the task ribbon, select **Topology Visualization > Discover Topology > Specify SNMP Probes**.

The **Topology Visualization Workspace: SNMP Probes** dialog box appears.

2. Click the **+** button to open the **Add SNMP Settings** dialog box.

3. Select one of the following options and enter the appropriate value in the field provided.
 - Select **SNMP V1/V2C** and specify the community string in the **Community** field. The SNMP v1/v2c community string “public” is available by default. The SNMP v1/v2c community string is based on the community string configured on the devices in your network.


Figure 92: Add SNMP V1/V2C Settings Dialog Box



The dialog box titled "Add SNMP Settings" has a close button (X) in the top right corner. It contains two radio buttons: "SNMP V1/V2C" (which is selected) and "SNMP V3". Below the radio buttons is a text field labeled "Community:". At the bottom are three buttons: "OK", "Add More", and "Cancel".

- Select **SNMP V3** and enter the information in the fields provided as displayed in [Figure 93 on page 152](#).

Figure 93: Add SNMP V3 Settings Dialog Box



The dialog box titled "Add SNMP Settings" has a close button (X) in the top right corner. It contains two radio buttons: "SNMP V1/V2C" and "SNMP V3" (which is selected). Below the radio buttons are several fields: "Username:" with a text field, "Privacy type:" with a dropdown menu showing "Please select ...", "Privacy password:" with a text field, "Authentication type:" with a dropdown menu showing "Please select ...", and "Authentication password:" with a text field. At the bottom are three buttons: "OK", "Add More", and "Cancel".

- a. Enter the SNMP V3 username in the **Username** field.
- b. Select the privacy protocol (the encryption standard for the SNMP user) from the **Privacy type** list.
The available options are **AES128**, **DES**, and **None**. By default, the Privacy type for SNMP version 3 is set to **None**.
- c. Enter the password used to generate the key used for encryption in the **Privacy password** field.
The password must be at least eight characters long. You can include all character classes in a password (alphabetic, numeric, and special characters) except control characters.

- d. Select the authentication type for the SNMP user from the **Privacy type** drop-down list.
The available options are **MD5**, **SHA1**, and **none**. By default, the authentication type for SNMP version 3 is set to **none**.
 - e. Enter the password used to generate the key used for authentication in the **Authentication password** field.
The password must be at least eight characters long. You can include all character classes in a password (alphabetic, numeric, and special characters) except control characters.
4. Click **OK** to close the **Add SNMP Settings** dialog box and add the SNMP probe to the **SNMP Settings** list.

The **Specify Probes** window displays the configured SNMP settings.

Alternatively, click **Add More** to add the device target to the list while keeping the **Add SNMP Settings** dialog box open to add more SNMP probes.

You can also click **Cancel** to close the **Add SNMP Settings** dialog box without adding any SNMP probes.

To edit an SNMP probe:

1. From the task ribbon, select **Topology Visualization > Discover Topology > Specify SNMP Probes**.

The **Topology Visualization Workspace: SNMP Probes** dialog box appears.

2. Select the SNMP probe that you want to edit and click the **Edit** button to open the **Edit SNMP Settings** dialog box.
3. Select one of the following options and enter the appropriate value in the field provided.

You can choose to edit the existing values in the selected SNMP version, or you can select a different SNMP version and enter the desired values.

- Select **SNMP V1/V2C** and specify the community string in the **Community** field.
You can enter “public”, “private”, or a predefined string.
- Select **SNMP V3** and enter the information in the fields provided.
 - a. Enter the SNMP version 3 username in the **Username** field.
 - b. Select the privacy protocol—that is, the encryption standard for the SNMP user—from the **Privacy type** list.
The available options are **AES128**, **DES**, and **None**. By default, the Privacy type for SNMP version 3 is set to **None**.
 - c. Enter the password used to generate the key used for encryption in the **Privacy password** field.
The password must be at least eight characters long. You can include all character classes in a password (that is, alphabetic, numeric, and special characters) except control characters.

- d. Select the authentication type for the SNMP user from the **Privacy type** drop-down list.

The available options are **MD5**, **SHA1**, and **none**. By default, the authentication type for SNMP version 3 is set to **none**.

- e. Enter the password used to generate the key used for authentication in the **Authentication password** field.

The password must be at least eight characters long. You can include all character classes in a password (that is, alphabetic, numeric, and special characters) except control characters.

4. Click **OK** to save your changes and close the **Edit SNMP Settings** dialog box.

The **Specify Probes** window displays the configured SNMP settings.

Alternatively, click **Cancel** to close the **Edit SNMP Settings** dialog box without editing any SNMP probes.

To delete an SNMP probe:

1. From the task ribbon, select **Topology Visualization > Discover Topology > Specify SNMP Probes**.

The **Topology Visualization Workspace: SNMP Probes** dialog box appears.

2. Select the SNMP probe that you want to delete and click **Delete** to open the **Delete SNMP Settings** dialog box.

3. Click **OK** to delete the probe and remove it from the **SNMP Settings** list.

The **Specify Probes** window displays the configured SNMP settings.

Click **Cancel** to close the **Delete SNMP Settings** dialog box without deleting the probe.

Related Documentation

- [Discovering a Topology on page 148](#)

PART 3

Device Templates

- [Overview on page 157](#)
- [Device Template Definitions on page 161](#)
- [Device Templates on page 203](#)
- [Troubleshooting on page 215](#)

CHAPTER 11

Overview

- [Device Templates Overview on page 158](#)
- [Device Templates Workflow Overview on page 159](#)

Device Templates Overview

Device Templates provides the tools to create custom device templates deployable through Junos Space. Unlike other systems that provide configuration of most aspects of a device and allow implementation of some form of template, Device Templates is schema-driven and therefore has all the configuration commands and values that can be sent down to all supported devices. Conversely, when you want to focus on a single device family, the configuration commands for other device families are filtered out.

For efficient device deployment, device templates implements two roles: a designer who understands the technical details of device configuration and knows how to implement this knowledge to solve specific business problems; and an operator, a junior individual to execute the orders of the designer.

A template definition designer creates template definitions and publishes them. An operator selects a template definition and creates from it a template to configure one or more devices. The operator then tests the template on the devices (without deploying it). If the template is validated, the operator deploys the template to the devices. With this division of labor, the operator does not need specialist knowledge. The designer can design the device templates to allow (or prevent) specific tasks to be performed by specified administrator roles. Alternatively, one person can be both designer and operator.

Device Templates provides two views: the designer's view and the operator's view. While creating the definition, the designer can verify what the operator sees. The operator, however, cannot see what the designer sees.

Designers can subdivide the device configuration tasks into areas, each to be handled by a separate template definition. Designers can choose not only which options to display to their operators, but also whether to display them at all. They can make configuration options editable or read-only, and even provide customized explanations for operators. Operators can immediately deploy a template to the devices they select, or schedule a later deployment.

Both kinds of user require the appropriate permissions; see ["User Privileges in Device Templates" on page 215](#).

**Related
Documentation**

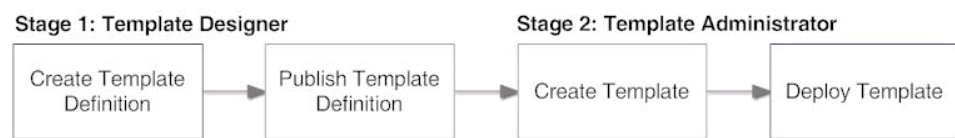
- [Device Templates Workflow Overview on page 159](#)
- [Defining the Operator's View on page 167](#)
- [Defining the Content the Operator Enters on page 179](#)

Device Templates Workflow Overview

The device templates workflow has two main parts, with two different roles:

- The designer, who creates the template definition (see [“Device Template Definition Workflow” on page 163](#)).
- The operator, who creates a template from a template definition (see [“Creating a Device Template Overview” on page 206](#)).

Figure 94: Workflow for Device Template Definition and Template Creation



Both designer and operator must ensure that they have appropriate permissions. See [“User Privileges in Device Templates” on page 215](#).



NOTE: Do not use your browser’s Back and Forward buttons to navigate in the Device Templates pages.

Related Documentation

- [Device Templates Overview on page 158](#)
- [Creating a Device Template Overview on page 206](#)

CHAPTER 12

Device Template Definitions

- [Managing Device Template Definitions Overview on page 162](#)
- [Importing Device Template Definitions Overview on page 162](#)
- [Device Template Definition Workflow on page 163](#)
- [Creating a Device Template Definition Overview on page 164](#)
- [Junos OS Configuration Hierarchy Reference on page 164](#)
- [Defining the Operator's View on page 167](#)
- [Selecting the Device Family and Naming a Device Template Definition on page 169](#)
- [Creating Configuration Pages for a Device Template Definition on page 170](#)
- [Finding Configuration Options on page 174](#)
- [Filling in the General Tab on page 176](#)
- [Filling in the Description Tab on page 178](#)
- [Defining the Content the Operator Enters on page 179](#)
- [Filling in the Validation Tab on page 181](#)
- [Composing Error Messages on page 184](#)
- [Filling in the Advanced Tab on page 185](#)
- [Using Rules Overview on page 186](#)
- [Managing CSV Files on page 187](#)
- [Working with Rules on page 188](#)
- [Specifying Device-Specific Data in Definitions on page 190](#)
- [Specifying Default Values for Configuration Options on page 194](#)
- [Publishing and Unpublishing a Device Template Definition on page 196](#)
- [Modifying a Device Template Definition on page 197](#)
- [Cloning a Device Template Definition on page 198](#)
- [Deleting a Device Template Definition on page 199](#)
- [Importing a Device Template Definition on page 200](#)
- [Exporting a Device Template Definition on page 201](#)

Managing Device Template Definitions Overview

Managing template definitions gives you access to the entire template definition workflow.

Before you begin, make sure you have the appropriate permissions; see [“User Privileges in Device Templates” on page 215](#).



NOTE: Do not use your browser’s Back and Forward buttons to navigate in Device Templates pages.

To manage Device Template definitions, navigate to the Manage Definitions inventory page by selecting **Platform > Device Templates > Manage Definitions**. The Manage Definitions inventory page displays all published or unpublished template definitions, and has two views: thumbnail and table. You can display the definitions themselves as icons or in table format: change from one view to the other by clicking on the display format icon in the platform navigation ribbon. You can select or deselect all items, and you can use the search function to find a template definition by name.

From the Manage Definitions page, you can also publish, unpublish, modify, delete, import, export, and clone a template definition. You can also tag and untag an object.

Related Documentation

- [Device Template Definition Workflow on page 163](#)
- [Publishing and Unpublishing a Device Template Definition on page 196](#)
- [Modifying a Device Template Definition on page 197](#)
- [Deleting a Device Template Definition on page 199](#)
- [Importing a Device Template Definition on page 200](#)
- [Exporting a Device Template Definition on page 201](#)
- [Cloning a Device Template Definition on page 198](#)
- [Tagging an Object on page 495](#)
- [Untagging Objects on page 497](#)
- [Managing Device Templates Overview on page 203](#)
- [Changing Device Template Definition States on page 215](#)

Importing Device Template Definitions Overview

The Import Definition facility in Device Templates enables you to import template definitions from xml files and export template definitions to xml files. You can therefore send definitions to other parties and or transfer definitions from one Junos Space fabric to another.

A definition retains its state when it is exported or imported: published definitions that are exported also appear as published when they are imported. Therefore, if you import

a definition that was published, but do not want it to be available to operators, you must unpublish it either before you export it or immediately after importing it.

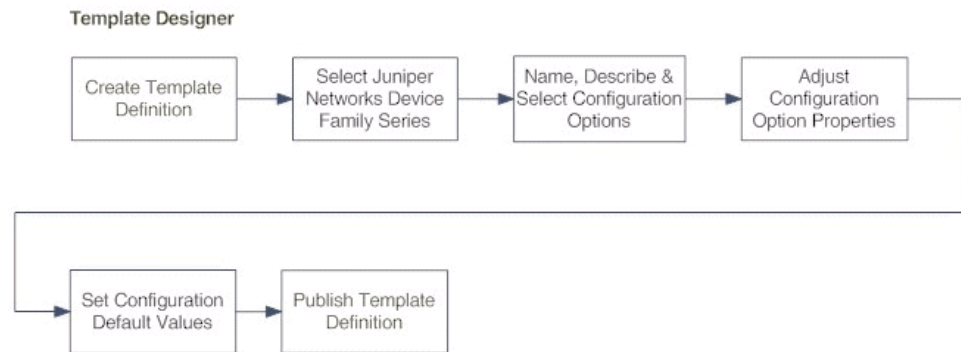
Related Documentation

- [Exporting a Device Template Definition on page 201](#)
- [Importing a Device Template Definition on page 200](#)
- [Publishing and Unpublishing a Device Template Definition on page 196](#)
- [Managing Device Template Definitions Overview on page 162](#)

Device Template Definition Workflow

The workflow for creating a template definition is illustrated by [Figure 95 on page 163](#).

Figure 95: Template Definition Workflow



Creating a template definition includes the following tasks:

1. Select a device family. See [“Selecting the Device Family and Naming a Device Template Definition” on page 169](#).
2. Select the configuration options to be included in the definition. See [“Creating Configuration Pages for a Device Template Definition” on page 170](#).
3. Define the text, labels, and template UI elements the operator sees, which includes defining the parameters the operator sees and can change. See [“Defining the Operator’s View” on page 167](#).
4. Set the default values for the parameters. See [“Specifying Default Values for Configuration Options” on page 194](#).
5. Set the values the operator sees. See [“Defining the Content the Operator Enters” on page 179](#).
6. Preview the template and if necessary modify the definition. See [“Modifying a Device Template Definition” on page 197](#).



NOTE: Template definitions are published by default. If you want to avoid making a definition available to operators, you must unpublish it. See [“Publishing and Unpublishing a Device Template Definition” on page 196](#).

- Related Documentation**
- [Device Templates Overview on page 158](#)
 - [Device Templates Workflow Overview on page 159](#)

Creating a Device Template Definition Overview

There are three main stages in creating a template definition.

First you select the device family and configuration options the definition will handle. This is covered in:

1. [Selecting the Device Family and Naming a Device Template Definition on page 169](#)
2. [Creating Configuration Pages for a Device Template Definition on page 170](#)

Then, you configure the options: “Defining the Operator’s View” on page 167 gives an overview of:

3. [Filling in the General Tab on page 176](#)
4. [Filling in the Description Tab on page 178](#)
5. [Filling in the Validation Tab on page 181](#)
6. [Composing Error Messages on page 184](#)
7. [Filling in the Advanced Tab on page 185](#)
8. [Specifying Device-Specific Data in Definitions on page 190](#)
9. [Using Rules Overview on page 186](#)

Finally, you specify the content the operator can enter. This is covered in “Defining the Content the Operator Enters” on page 179, which in turn gives an overview of:

8. [Specifying Default Values for Configuration Options on page 194](#)



NOTE: Do not use your browser’s Back and Forward buttons to navigate in the Device Templates pages.

- Related Documentation**
- [Device Template Definition Workflow on page 163](#)
 - [Publishing and Unpublishing a Device Template Definition on page 196](#)

Junos OS Configuration Hierarchy Reference

This topic provides references for configuring device configuration template definitions for the following Junos Space-supported devices;

- J Series, M Series, MX Series, T Series, and TX Matrix routing platforms
- SRX Series Services Gateway

- EX Series Ethernet Switches
- Firewalls NS/SSG Series
- Data Center / Media Flow Controller

Junos Space Device Templates supports the Juniper Networks device family DMI schemas. Each device family you select supports a unique set of Junos OS configuration hierarchy options available in the Create Definition user interface. [Table 23 on page 165](#) lists the main Junos OS configuration hierarchy options and the Junos configuration guides where you can find information about them.

[Table 23 on page 165](#) also maps the Device Template configuration options hierarchy to the Juniper Networks guides that describe how to configure the individual options. For a comprehensive list of Junos OS configuration guides, see http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/junos/product/.

Table 23: Junos OS Configuration Hierarchy Guide Reference

Configuration Hierarchy	Junos OS for J Series, M Series, MX Series, and T Series Routing Platform Configuration Guide
access	<i>Junos OS System Basics Configuration Guide</i> and Junos subscriber management documentation
accounting-options	Network management documentation
applications	Services interfaces documentation
bridge-domains	Layer 2 configuration documentation
chassis	<i>Junos OS System Basics Configuration Guide</i>
class-of-service	Class of service documentation
diameter	Junos subscriber management documentation
dynamic-profiles	Junos subscriber management documentation
event-options	<i>Junos OS Hierarchy and Standards Reference</i>
firewall	<i>Junos OS Policy Framework Configuration Guide</i>
forwarding-options	Policy framework documentation
groups	CLI user guide documentation
interfaces	<i>Junos OS Junos Network Interfaces Configuration Guide</i>
jsrc	Junos subscriber management documentation
logical-systems	Routing protocols documentation

Table 23: Junos OS Configuration Hierarchy Guide Reference (*continued*)

Configuration Hierarchy	Junos OS for J Series, M Series, MX Series, and T Series Routing Platform Configuration Guide
multicast-snooping-options	Multicast protocols documentation
policy-options	<i>Junos OS Policy Framework Configuration Guide</i>
protocols	<i>Junos OS Routing Protocols Configuration Guide</i>
routing-instances	<i>Junos OS Routing Protocols Configuration Guide</i>
routing-options	<i>Junos OS Routing Protocols Configuration Guide</i>
security	<i>Junos OS System Basics Configuration Guide</i> and the SRX Series release 10.0 documentation
services	Services interfaces documentation
snmp	<i>Junos OS Network Management Configuration Guide</i>
switch-options	Junos MX Series routers Layer 2 services — bridging, address learning, and forwarding
system	<i>Junos OS System Basics Configuration Guide</i>
virtual-chassis	<i>Junos OS Hierarchy and Standards Reference</i> and documentation for the EX Series Ethernet Switches
vlan	<i>Junos OS Hierarchy and Standards Reference</i> and documentation for the EX Series Ethernet Switches
wlan	Documentation for the SRX Series Services Gateway

EX-Series Devices

For more information about configuring EX Series devices, see

http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/ex-series/product/

SRX Series Devices

For more information about configuring SRX Series devices, see

<http://www.juniper.net/techpubs/hardware/junos-srx/index.html>.

Defining the Operator's View

This section gives an overview of the Create Definition pages. The designer specifies the fields that will be in templates based on the definition, and determines what data can be entered in those fields. Designers determine whether fields are visible and editable by the operator.



NOTE: Do not use your browser's Back and Forward buttons to navigate in Device Templates pages.

Table 24 on page 167 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 itself determines the method of validation and the way the parameters are displayed.

Table 24: Data Types and Tabs

Data Types	Tabs			
	General	Description	Validation	Advanced
Container	*	*		
Table	*	*	*	*
String - Key column in a table	*	*	*	*
String	*	*	*	*
Integer [Number]	*	*	*	*
Boolean	*	*		*
Enumeration	*	*		*
Choice	*	*		*

Table 25 on page 167 lists the validation parameters for the data types supporting validation.

Table 25: 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	

Table 25: Data Types and Validation Parameters (*continued*)

Data Type	Validation Parameters		
String - Key column in a table	Min Length	Max Length	Regular Expression

- All table configuration options have a key column by default.
- You can use any sequence to move options onto your pages.
- Because the tabs and their contents depend on the data type of the option selected, each tab has its own help topic:
 - [Filling in the General Tab on page 176](#)
 - [Filling in the Description Tab on page 178](#)
 - [Filling in the Validation Tab on page 181](#)
 - [Composing Error Messages on page 184](#)
 - [Filling in the Advanced Tab on page 185](#)
- Selecting another tab or option or configuration page saves the settings you enter. The **Next** or **Finish** buttons also save your settings. To save the template definition, click **Finish**.

After creating configuration groups and filling in all the tabs for each option, continue with [“Defining the Content the Operator Enters” on page 179](#) and [“Specifying Default Values for Configuration Options” on page 194](#).

Related Documentation

- [Specifying Device-Specific Data in Definitions on page 190](#)
- [Creating Configuration Pages for a Device Template Definition on page 170](#)
- [Creating a Device Template Definition Overview on page 164](#)

Selecting the Device Family and Naming a Device Template Definition

The first task in creating a template definition is selecting the device family and naming your template definition.

Each template definition is associated with a Juniper Networks Device Family DMI schema determining the Junos OS versions and device platforms supported. Before creating any template definitions, you must therefore set a default DMI schema for each device family. See [“Setting a Default DMI Schema” on page 513](#).

Each template definition must have a unique name. Although the description is optional, operators have no other way of identifying the contents of the definition without going through all the options visible to them in the template they create on the basis of that definition.



NOTE: Do not use your browser’s Back and Forward buttons to navigate in the Device Templates pages.

To select the device family and name the template definition:

1. From the Network Application Platform, click **Device Templates**. The Device Templates statistics page appears, displaying all available statistics for both template definitions and templates.
2. Click **Manage Definitions**. The Device Templates inventory page appears, displaying all template definitions.
3. Click **Create Definition**.

The **Create Definition** page appears.

4. From the Device Family Series pane, select the device family to which your definition will apply. The Junos OS versions and hardware platforms supported by the selected device family appear in the Description pane on the right. The OS version, which is related to the default DMI schema, appears on the lower left. By default, the OS version displayed is the one that is set as default for that device family (see [“Setting a Default DMI Schema” on page 513](#)).



NOTE: This information is not displayed to the operator. Unless you include it in the definition name or description, the operator will not know to which device family this definition applies.

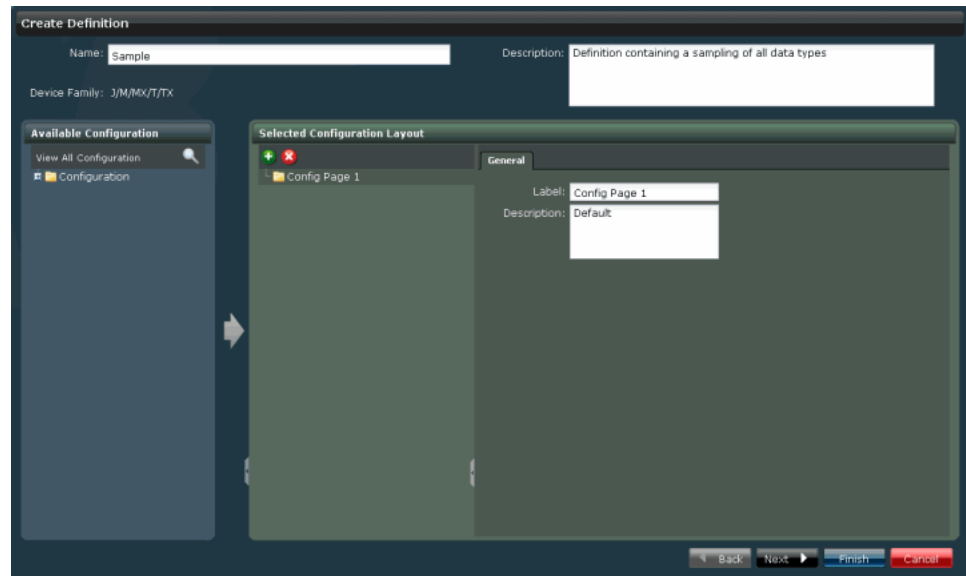
5. Select the appropriate OS version from the dropdown list in the lower part of the left pane.



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

6. Click **Next**.

The following page displays the selected device family, Available Configuration pane and the Selected Configuration Layout pane.



7. In the Name box, enter a name for the template definition (limit of 63 characters). It is helpful to give the definition a name that makes sense to the operator. Entering text in the Description field is optional, but again, helpful for the operator, who has no other way of knowing to which device family this definition applies (limit of 255 characters).

In the next task in the process of creating a template definition, “[Creating Configuration Pages for a Device Template Definition](#)” on page 170, you select configuration options and insert them into configuration pages.

Related Documentation

- [Creating a Device Template Definition Overview on page 164](#)
- [Device Template Definition Workflow on page 163](#)
- [Setting a Default DMI Schema on page 513](#)
- [Managing DMI Schemas Overview on page 506](#)

Creating Configuration Pages for a Device Template Definition

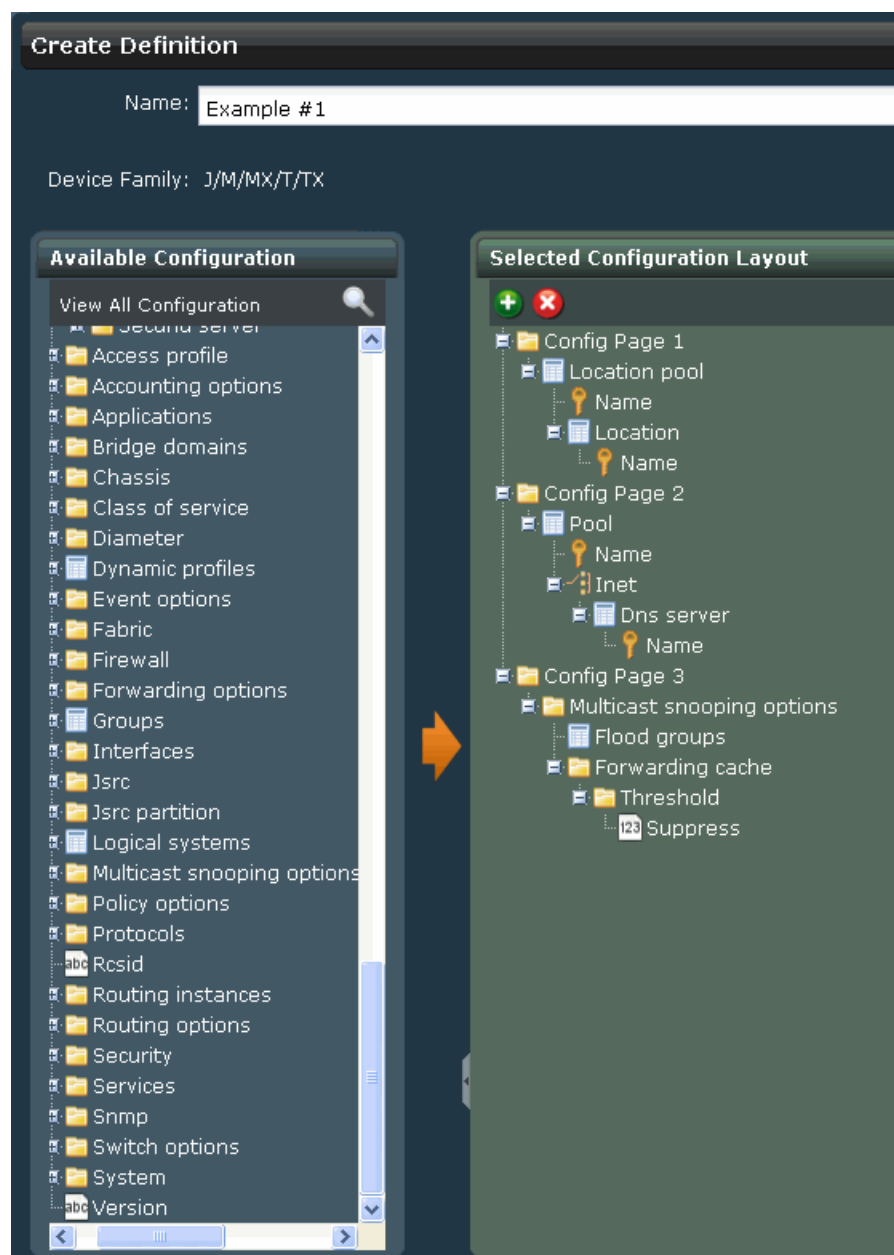
You create configuration pages as part of the process of selecting configuration options, to organize and group those options.

Before you begin, complete the steps in “[Selecting the Device Family and Naming a Device Template Definition](#)” on page 169.

The list in the Available Configuration pane displays the Junos OS configuration hierarchy level options available for the device family you selected. In the Selected Configuration Layout pane, you construct your groupings by putting the options into pages. Because operators never see the hierarchy in the Available Configuration pane, they need guidance

in understanding precisely which options they are configuring. Bear this in mind when composing a page of configuration options. Consider reducing the number of options per page.

Figure 96: Create Definition Dialog Box



To find particular configuration options, see [“Finding Configuration Options” on page 174](#).

To create a configuration page:

1. In the Create Definition page, expand the list of options available for the selected device family by opening the list, filtering, or searching, as described in [“Finding Configuration Options” on page 174](#).
2. Move an option from the Available Configurations pane to a page in the Selected Configuration Layout pane. The first page, “Config Page 1,” is available by default.

There are two ways to move an option from the Available Configurations pane to a page in the Selected Configuration Layout pane:

- Dragging and dropping from one pane to the other.
- Selecting the option and then clicking the arrow between the panes.

Any sequence is permissible, and there is no limit on the number of options a page can hold.



NOTE: You cannot put children of the same parent into different pages.



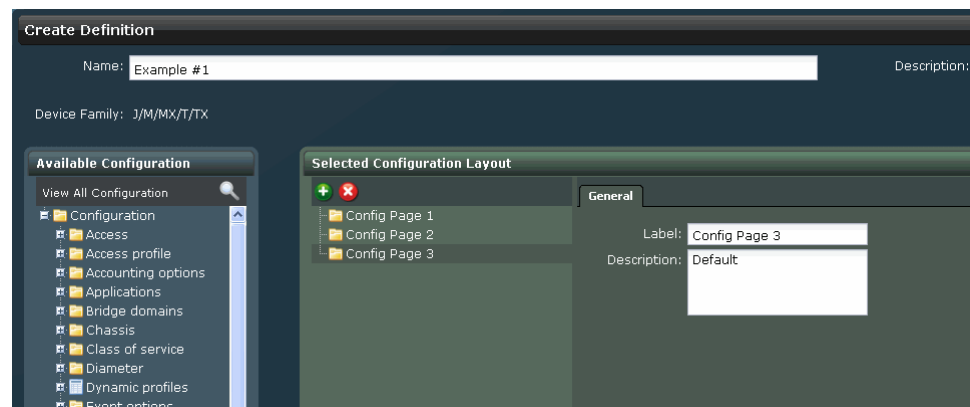
NOTE: Options that are either subsidiary or integral to others bring their respective parents and children with them when you move them onto a page. If you drill down and select a parameter deep in the hierarchy, such as L3 interface, dragging that parameter causes all the other parameters that require configuration to come with it. In this example, you get not only L3 interface, but also Name, both of which are under VLAN. This ensures that all the parameters required for a particular configuration option are present in your configuration group.

Conversely, you cannot add an option of the 'choice' data type directly to a page. Instead, add a child of the choice to add the choice itself.

3. Name your configuration grouping by double-clicking the placeholder name; in the example below, “Config Page 3” under Selected Configuration Layout.

On the right, the General tab appears.

Figure 97: General Tab



4. (Optional) In the Label field on the General tab, replace the placeholder name (Config Page x) with a more informative name.
5. (Optional) Enter a description in the Description field.

Add or remove pages as desired.

In both cases, in the status bar at the bottom of the page a message indicates whether your definition had any validation errors. If it did, revise your entries.

To add a page:

5. Click the plus icon [+] at the top left of the Selected Configuration Layout pane.
A new page appears: "Config Page x."

To remove a page or a configuration option from a page:

6. Select the page or configuration option and click the X at the top left of the Selected Configuration Layout pane.
The page disappears.

7. When you have finished creating configuration pages, click **Next**.

Continue with "[Defining the Operator's View](#)" on page 167.

Related Documentation

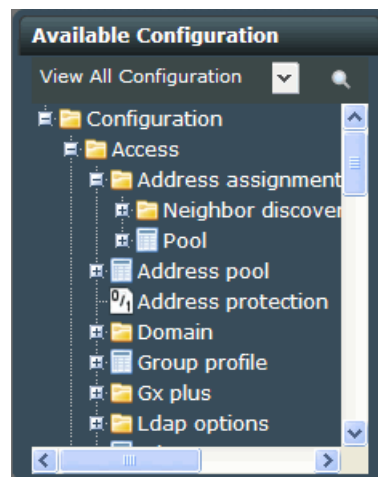
- [Filling in the General Tab on page 176](#)
- [Filling in the Description Tab on page 178](#)
- [Filling in the Validation Tab on page 181](#)
- [Composing Error Messages on page 184](#)
- [Filling in the Advanced Tab on page 185](#)
- [Device Template Definition Workflow on page 163](#)

Finding Configuration Options

There are two ways to locate particular configuration options: you can browse the list or use the search function.

To display the top level configuration options, click the plus sign [+] or expansion icon at the top of the tree in the Available Configuration pane. Many of the options contain further parameters. To display these, click on the plus sign [+] or expansion icon left of the option.

Figure 98: Browsing the



To search for a specific configuration option:

1. Click the magnifying glass icon.

The search term bar appears.

2. Enter your search term.

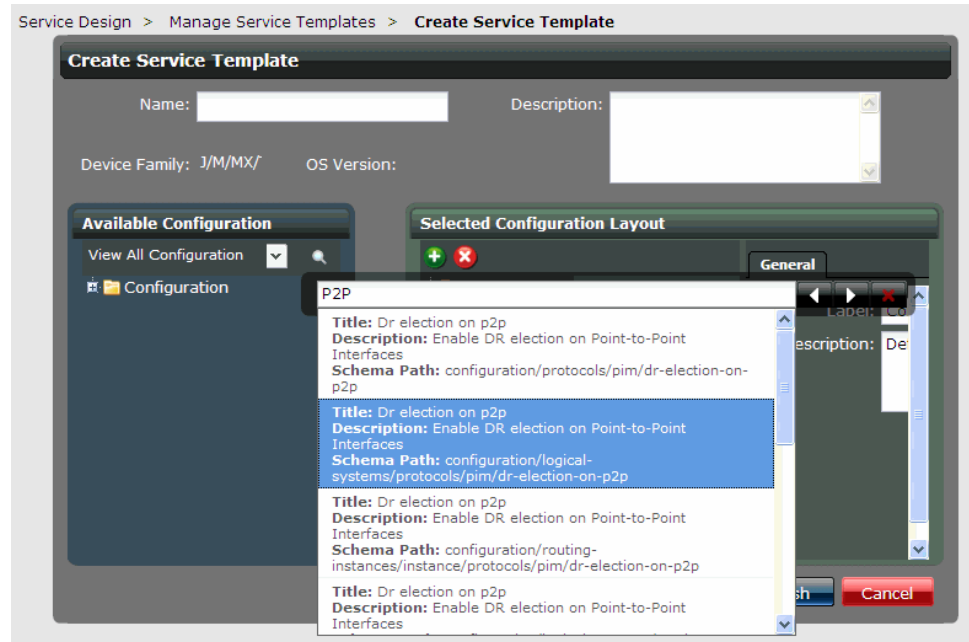
As soon as you enter the first three letters, the bar opens downwards, displaying the search results.

Search displays only the first ten matches for your term.



TIP: Search results appear while you are typing. You can continue typing or even delete text. Note that the cursor might not be visible in the search field if the focus is somewhere within the list of search results.

The order of the search results is not dependent on the order of those items in the Available Configuration pane. It is based on the similarity of your search term to indexed fields.



3. While the result list is still visible, select a result by:

- Using the mouse to click on it.
- Pressing the Enter key to select the first result in the list.
- Using the up and down arrow keys on the keyboard to move through the list, pressing the Enter key to select a result.

The tree in the Available Configuration pane jumps to the location of the match for the result you selected and highlights the option. The list of results disappears.

4. (Optional) To review the results that you did *not* select, either:

- Click the white arrows next to the Search box.
Click the arrow to the left to move to the result listed previous to the selected result.
Click the arrow to the right to move to the result after the selected result.
- Use the left and right arrow keys on the keyboard.
Press the arrow to the left to move to the result listed previous to the selected result.
Press the arrow to the right to move to the result after the selected result.

5. To close the search bar, click the X in the top right corner of the bar.

Related Documentation

- [Creating Configuration Pages for a Device Template Definition on page 170](#)

Filling in the General Tab

This topic describes how to fill in the General tab in the Selected Configuration Layout pane when you are creating a template definition.

Before you begin, review [“Defining the Operator’s View” on page 167](#) and [“Creating Configuration Pages for a Device Template Definition” on page 170](#).

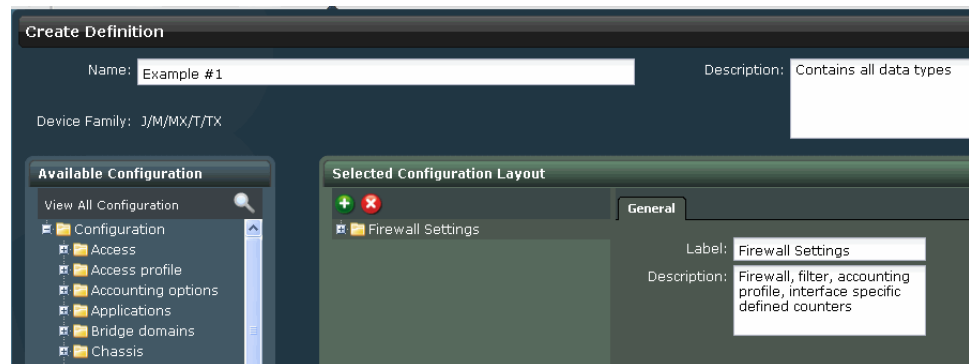
The General tab enables you to create field labels that help the operator enter correct field data. The General tab applies to both the configuration *pages* and the configuration *options* you select.

To fill in the General tab:

1. For the *page* you are building, in the Selected Configuration Layout pane, select a page (the default is “Config Page x”).

The General tab appears.

2. In the **Label** field, enter an informative name for the configuration page you are creating.



3. (Optional) In the **Description** field, enter a description of the configuration grouping.

Your entries are saved when you click any other configuration layout page, option, or button on the page.

4. In the Selected Configuration Layout pane, select the first *configuration option* in the newly named page.

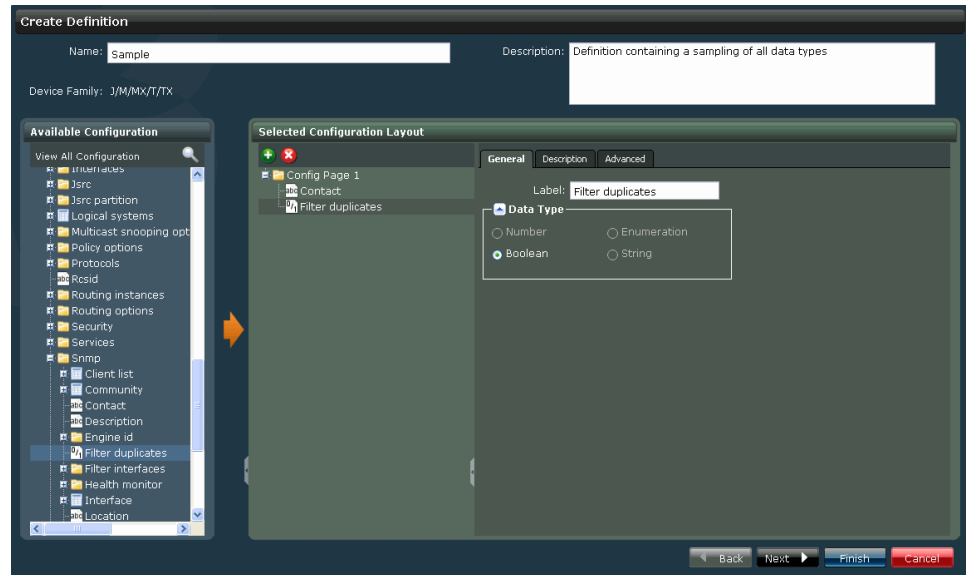
The General tab appears.

5. (Optional) To rename the selected option, in the **Label** field, enter a name for that configuration option. You can leave the default name, if desired.



TIP: Because the context of the configuration options you move to the Available Configuration pane will not match that of the Selected Configuration Layout pane, consider changing the labels to give some indication to the operator where they are located in the configuration tree, which operators do not see in templates. 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 component's data type, which determines not only the tabs displayed, but also the method of validation. For tables showing the various data types and their tabs, see [“Defining the Operator's View” on page 167](#).

6. (Optional) If the data type of the selected option is String, you can change it to Enumeration by clicking the String option button while the option is selected.

Either a box containing ready-made choices appears, or a box to contain the choices you create appears, and next to it, plus [+] and minus [-] icons.

7. To enter the enumeration choices, for each one, click the plus [+] icon and enter text in the field that appears (limit 255 alphanumeric characters).



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.

Click **OK** to save each entry, or to delete it, click **Close**.

To close the window, click **Close**.

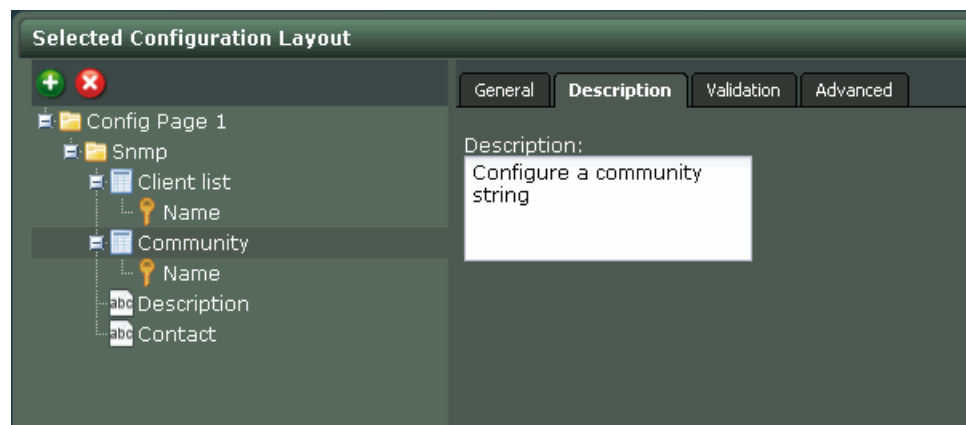
8. To save your entries on the General tab, select another tab or another option, or click **Next** or **Finish**.
9. Either fill in the General tab as described above for each option in your configuration group, or go on to fill in the Description tab for the current option (see [“Filling in the Description Tab” on page 178](#)).

Related Documentation

- [Defining the Content the Operator Enters on page 179](#)
- [Specifying Default Values for Configuration Options on page 194](#)
- [Device Template Definition Workflow on page 163](#)
- [Creating a Device Template Definition Overview on page 164](#)
- [Defining the Operator's View on page 167](#)
- [Filling in the Description Tab on page 178](#)

Filling in the Description Tab

This topic describes how to fill in the Description tab in the Selected Configuration Layout pane when you create a template definition.



Before you begin, review [“Defining the Operator’s View” on page 167](#), [“Creating Configuration Pages for a Device Template Definition” on page 170](#), and [“Filling in the General Tab” on page 176](#).

The Description tab enables you to add descriptive text to help the operator enter the correct data. When the operator creates a template, he or she can view your description or explanation by clicking the little Information icon to the right of the parameter. A pop-up appears, displaying the content you entered in the Description field.



To fill in the Description tab:

1. In the Selected Configuration Layout pane, select a configuration option. It can be the same option for which you have just filled out the General tab, or any other option.
2. Click the Description tab to display it.
3. In the Description field, enter [additional] descriptive text for the selected configuration option, or leave the default text, if desired.
4. To save your the description, move to another tab or another option, or click **Next**.

Related Documentation

- [Defining the Operator's View on page 167](#)
- [Creating Configuration Pages for a Device Template Definition on page 170](#)
- [Filling in the General Tab on page 176](#)
- [Filling in the Validation Tab on page 181](#)
- [Creating a Device Template on page 206](#)

Defining the Content the Operator Enters

This topic describes how you define the content the operator can enter into the template.

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 (see [“Filling in the Validation Tab” on page 181](#)). Another situation might be when a particular attribute allows values A/B/C/D/E, but you want templates that allow only values A/C.



TIP: Remember that the definition is just the “template of the template.” Therefore in the definition you only need to set up one Primary Resolver, for example, because it is during template creation that the number of actual instances will be determined.

After you have filled out the tabs (General, Description, **Validation**, **Advanced**) for your configuration options, specify the default values for the configuration parameters.

Specify default values for configuration parameters Operator View

Add_LdapSvr >> Ldap_server >>

Lightweight Directory Access Protocol server options

Id	Name	Port	Retry	Source address	Timeout
1	245.1.1.100	389	3	245.1.1.254	5

No Validation Error

Back Next Finish Cancel

The Specify default values for configuration parameters page of the template definition shows the parameter fields the operator sees. The parameters shown are for the table data type, so table rows can be added, edited, and deleted (see [“Specifying Default Values for Configuration Options” on page 194](#)). If you have specified that the option (for example, LDAP server) and its parameters are editable (see [“Filling in the Advanced Tab” on page 185](#)), the operator sees the same page as you do, and the operator can also add, edit, and delete table rows. If you specify that the option is hidden, the **Operator View** shows nothing.

When you add a row, the fields shown as column headings on the **Create Definition** page display as a list of fields.

Specify default values for configuration parameters Operator View

Add_LdapSvr >> Ldap_server >> Ldap_server [new] >>

Lightweight Directory Access Protocol server options Save Undo

Name:

Port: 389

Retry: 3

Source address:

Timeout: 5

No Validation Error

Back Next Finish Cancel

Again, the fields that the operator sees are determined by your settings on the Advanced tab on the previous page. The operator's ability to edit the fields is also dependent on

the Advanced tab settings. What the operator can enter in the fields is determined by your **Validation** tab settings. Clicking the little blue Information icon to the far right of each option on this page displays a pop-up with the information from the Description tab.

Click **Save** at any time to save your draft. Also, if you click **Back** or move to another page, you are prompted to save your draft.



NOTE: Do not use your browser's Back and Forward buttons to navigate in Device Templates pages.

Related Documentation

- [Specifying Default Values for Configuration Options on page 194](#)
- [Junos OS Configuration Hierarchy Reference on page 164](#)

Filling in the Validation Tab

This topic describes how to fill in the **Validation** tab in the Selected Configuration Layout pane when you are creating a template definition. Both the template definition and the template must be valid before they can be respectively used and deployed.

Before you begin, review “[Defining the Operator's View](#)” on page 167 and “[Creating Configuration Pages for a Device Template Definition](#)” on page 170.

The **Validation** tab displays the validation criteria for the selected configuration option, if relevant. These criteria are determined by the option's data type: string, integer/number, table, container, choice, or enumeration.

The following screen capture shows the validation tab for a string.

The screenshot shows the 'Selected Configuration Layout' window with the 'Validation' tab selected. The left pane displays a configuration hierarchy with 'Config Page 1' expanded, showing options like 'Contact', 'Filter duplicates', 'Use mac address', 'Local', 'Use default ip address', 'Use mac address', 'Commit delay', 'Agent address', 'Trap group', 'Name', 'Destination port', 'Logical system', 'Categories', 'Authentication', 'Chassis', and 'Configuration'. The right pane shows the validation settings for a selected option:

- Min Length: 0
- Max Length: 214748364
- Regular Expression: ^.{1,27}\$
- Regular Expression: Must be a string of 27 char.
- Error Message:

At the bottom of the window are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.

The next screen capture shows the Validation tab for the integer/number data type.

The screenshot shows the 'Selected Configuration Layout' window with the 'Validation' tab selected. The left pane displays a tree structure of configuration elements, including 'Config Page 1', 'Contact', 'Filter duplicates', 'Use mac address', 'Local', 'Use default ip address', 'Use mac address', 'Commit delay', 'Agent address', 'Trap group', 'Name', 'Destination port', 'Logical system', 'Categories', 'Authentication', 'Chassis', and 'Configuration'. The right pane shows the validation settings for the selected element, with 'Min Value' set to 0 and 'Max Value' set to 429496729. At the bottom, there are 'Back', 'Next', 'Finish', and 'Cancel' buttons.

The following shows the Validation tab for the table data type.

The screenshot shows the 'Selected Configuration Layout' window with the 'Validation' tab selected. The left pane displays the same tree structure of configuration elements as the previous screenshot. The right pane shows the validation settings for the selected element, with 'Min Occurrence' set to 0 and 'Max Occurrence' set to 214748364. At the bottom, there are 'Back', 'Next', 'Finish', and 'Cancel' buttons.

For a table showing data type correlated to validation criteria, see [“Defining the Operator’s View” on page 167](#).



NOTE: If values are already displayed on the validation tab, note that they provide the limits within which you or the operator must remain when you set the default values for the current device template definition (see [“Specifying Default Values for Configuration Options” on page 194](#)). The operator only sees the validation criteria and their values if you supply them when you create an error message (see [“Composing Error Messages” on page 184](#)).

You do not always need to enter anything on the **Validation** tab. However, in certain cases, input is mandatory, for example when a hostname is to be validated.

To fill in the **Validation** tab:

1. In the Selected Configuration Layout pane, select a configuration option of the appropriate type. It can be the same option for which you have just filled out the General and the Description tabs, or any other option for which validation is relevant.
2. Click the **Validation** tab in the **Create Definition** page.
3. Enter the parameters for the option in the appropriate fields.

If the fields already display default values and you change them, ensure that your values do not exceed the default values.

4. (Optional) For a string, in the **Regular Expression** field, enter a regular expression to further constrain what the operator can enter.
5. (Optional) For a string, compose an error message.

This is not a validation parameter but instead a clue to enable the operator to enter correct field data. See [“Composing Error Messages” on page 184](#).

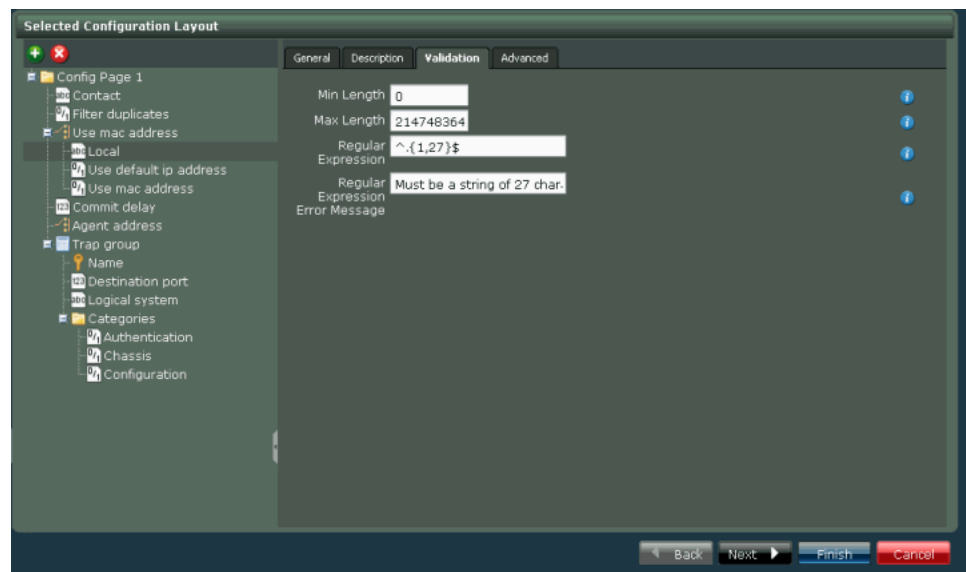
6. To save your entries, select another tab or another option, or click **Next** or **Finish**.

Related Documentation

- [Defining the Operator’s View on page 167](#)
- [Creating Configuration Pages for a Device Template Definition on page 170](#)
- [Filling in the General Tab on page 176](#)
- [Creating a Device Template on page 206](#)
- [Filling in the Description Tab on page 178](#)
- [Composing Error Messages on page 184](#)

Composing Error Messages

This topic describes how to create an error message that appears when an operator enters invalid content in a template field. Composing an error message is optional, but 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.



Before you begin, review [“Filling in the Validation Tab” on page 181](#), [“Defining the Operator’s View” on page 167](#), and [“Creating Configuration Pages for a Device Template Definition” on page 170](#).

The Regular Expression Error Message box on the Validation tab appears only if you configure an option of the string data type.

To complete the configuration:

1. In the Create Definition page, in the Selected Configuration Layout pane, select a configuration option of the string data type. It can be the same option for which you have just filled out the Validation tab, or any other option of the string data type.
If you select another option, the General tab appears.
2. If it is not already on top, select the Validation tab.
3. In the Regular Expression Error Message box, enter an error message that explains the meaning of the regular expression you entered on this tab, so that the operator understands how to correct his or her input. For example, for `^[a-zA-Z0-9_]*$` you might provide the following error message: **Enter only upper and lowercase letters, numbers, and underscores.**
4. To save your entries, move to another tab or another option, or click **Next** or **Finish**.

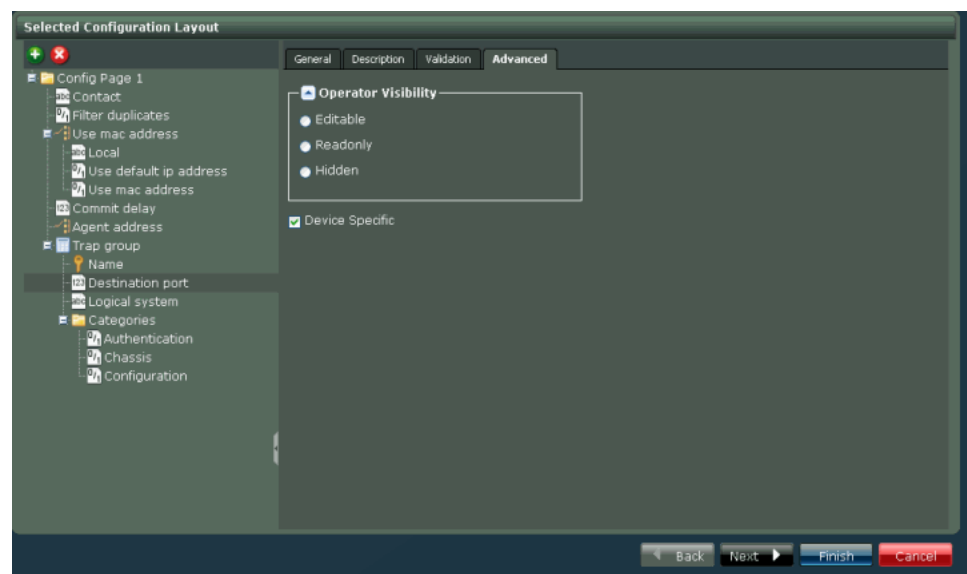
Related Documentation

- [Filling in the Validation Tab on page 181](#)
- [Defining the Operator's View on page 167](#)
- [Creating Configuration Pages for a Device Template Definition on page 170](#)
- [Filling in the General Tab on page 176](#)
- [Creating a Device Template on page 206](#)

Filling in the Advanced Tab

This topic describes how to fill in the Advanced tab in the Selected Configuration Layout pane when you are creating a template definition. The settings on this tab determine whether the operator can see the selected option or edit its values.

Before you begin, review [“Defining the Operator’s View” on page 167](#) and [“Creating Configuration Pages for a Device Template Definition” on page 170](#). The Advanced tab does not display for all data types.



To fill in the Advanced tab:

1. Navigate to the Advanced tab in the **Create Definition** page.
2. In the Selected Configuration Layout pane, select a configuration option. It can be the same option for which you have just filled out other tabs, or any other.
If it is not already visible, the General tab appears.
3. Select the Advanced tab.
4. Select **Editable**, **Readonly**, or **Hidden**, depending on how you want the operator to interact with the option.

5. (Optional) To mark this configuration option as device-specific, click the **Device Specific** check box. For more information on this, go to step 4 ff of [“Specifying Device-Specific Data in Definitions” on page 190](#).
6. To save your entries, select another tab or another option, or click **Next** or **Finish**.

The next task in this sequence is [“Specifying Default Values for Configuration Options” on page 194](#).

**Related
Documentation**

- [Defining the Operator’s View on page 167](#)
- [Creating Configuration Pages for a Device Template Definition on page 170](#)
- [Defining the Content the Operator Enters on page 179](#)
- [Creating a Device Template on page 206](#)
- [Using Rules Overview on page 186](#)

Using Rules Overview

Device Templates uses rules to supplement the device-specific value capability supplied by CSV files.

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.

**Related
Documentation**

- [Working with Rules on page 188](#)
- [Managing CSV Files on page 187](#)
- [Filling in the Advanced Tab on page 185](#)
- [Specifying Device-Specific Data in Definitions on page 190](#)
- [Creating a Device Template Definition Overview on page 164](#)
- [Creating a Device Template Overview on page 206](#)

Managing CSV Files

Device Templates uses CSV files to specify device-specific values, in addition to rules (see [“Using Rules Overview” on page 186](#)). The Managing CSV Files task describes how to import this type of CSV file into Space. For instructions on the procedure for linking the file to a definition and identifying the key column for Device Templates, see [“Specifying Device-Specific Data in Definitions” on page 190](#).

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, from its native application (for example, Microsoft Excel or Notepad), you must upload it again. You can do this within the device templates workflow.

To add the CSV files you use for template definitions to Junos Space:

1. From the Device Templates workspace, navigate from **Manage Definitions** to **Manage CSV Files**.

The Manage Template Definitions page appears.

2. Click **Upload**.

The CSV File upload dialog appears.

3. Click **Browse**.

The File Upload dialog opens.

4. Navigate to the desired CSV file, select it and click **Open**.

The CSV File upload dialog reappears, this time displaying the name of the selected file.

5. Click **Upload**.

The Manage CSV Files page reappears. The name of the file just imported appears in the left pane.

To display the content of a file, select its name in the left pane. Its content displays in the right pane.

To use the file you just uploaded, either follow the sequence of tasks in [“Creating a Device Template Definition Overview” on page 164](#) or go directly to [“Specifying Device-Specific Data in Definitions” on page 190](#).

To

- Related Documentation**
- [Managing Device Template Definitions Overview on page 162](#)
 - [Defining the Content the Operator Enters on page 179](#)
 - [Creating a Device Template Overview on page 206](#)

Working with Rules

Specify rules to resolve device specific values at the time of deployment. Rules are applied in the order shown. You can change the order as necessary.

You can create rules for devices whose names start with a specific word, or rules for devices with a specific tag.

For the selected configuration option, on the Advanced tab, select the **Device Specific Value** check box to trigger the **Device Specific Value** dialog.

After “[Filling in the Advanced Tab](#)” on page 185 continue with “[Specifying Device-Specific Data in Definitions](#)” on page 190.

You can add, edit, move, and delete rules. Instructions for all of these actions follow.

You can only select one rule at a time. If no rule is selected, only the **Add** button is enabled.

To add a rule:

1. In the **Device Specific Value** dialog, select the check box to the left of **Specify rules to resolve the value at deploy time**.

The rules section of the dialog is activated, displaying the name of the configuration option for which you are setting a device specific value.

2. Click the [+] icon.

Two options appear:

- Rule matching tagged device
- Rule matching device name.

3. Select the appropriate option.

A rule appears, depending on your selection in the previous step, either of the following:

- Set to a specific value for devices tagged with a specific tag
- Set to a specific value for devices with name starting with a specific word.

In both cases, the phrase “a specific value” is a link, as are “a specific tag” and “a specific word.”

4. Click either **a specific tag** or **a specific value**.

The **Set \$dsv** field appears.

5. Enter the appropriate value.

If the value you enter is not valid, an error message appears in the form of a tool tip explaining why the entry is invalid.

6. To save your input, click the **OK** button. To clear your input, click the **[X]** button.

The rule reappears, this time with your input replacing the link.

7. (Optional) To change the sequence of in which the rules will be applied, select a rule and click either the up arrow icon or the down arrow icon.

The selected rule moves to the new position.

8. (Optional) To delete a rule, select the rule and click the **[X]** button.

The selected rule disappears.

9. (Optional) To clone a rule, select the rule and click the last icon on the right, next to the down arrow.

A clone of the selected rule appears.

10. (Optional) Refresh the rules display by clicking the Refresh icon in the lower bar of the Rules section of the Device Specific Value dialog.

11. When you have finished working with rules, close the Device Specific Value dialog box by clicking **Close**.

**Related
Documentation**

- [Using Rules Overview on page 186](#)
- [Managing Device Template Definitions Overview on page 162](#)
- [Creating a Device Template Definition Overview on page 164](#)
- [Defining the Content the Operator Enters on page 179](#)
- [Creating a Device Template Overview on page 206](#)

Specifying Device-Specific Data in Definitions

Template designers can use a comma-separated value (CSV) file to provide device-specific values in a template definition. For example, the designer can use a CSV file to specify the SNMP contact as shown.

	A	B	C	D	E	F	G	H
1	device	contact	ip					
2	SanDiego	sd-contac	123.123.123.123					
3	Sacremen	sac-conta	123.123.123.124					
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								

Use one row per device. For each value to be specified, use one column. In the example illustrated above, if you wanted to specify interfaces in addition to the contact and the IP address, you would simply add a column for each interface, as in this second example (following), which describes two interfaces on a single device:

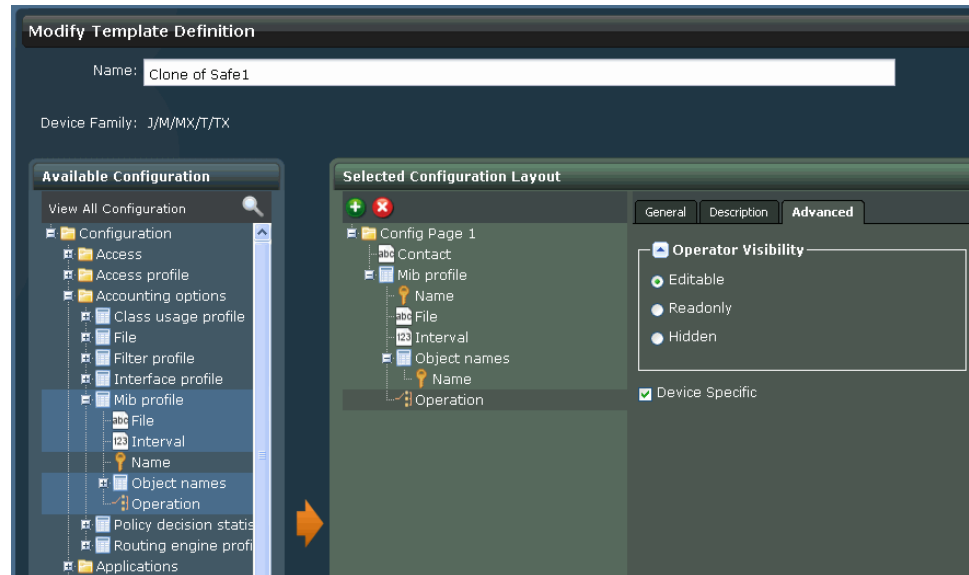
device,interface-1,mtu-1,traps-1,interface-2,mtu-2,traps-2

gemini-re0,ge-0/1/1,1514,1,ge-0/1/2,1518,0

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.

To use a CSV file to set device-specific values in a template definition:

1. Select the desired configuration option in the Selected Configuration layout panel.



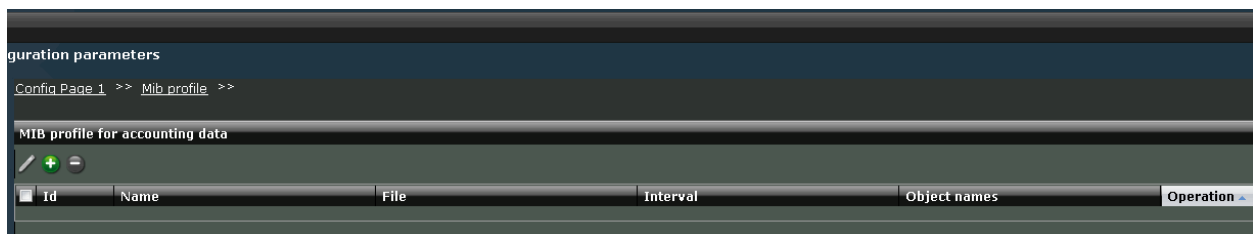
2. Select the Advanced tab, and select the **Device Specific** check box.
3. Click **Next**.

The second Create Definition page appears, displaying the title **Specify default values for configuration parameters**.

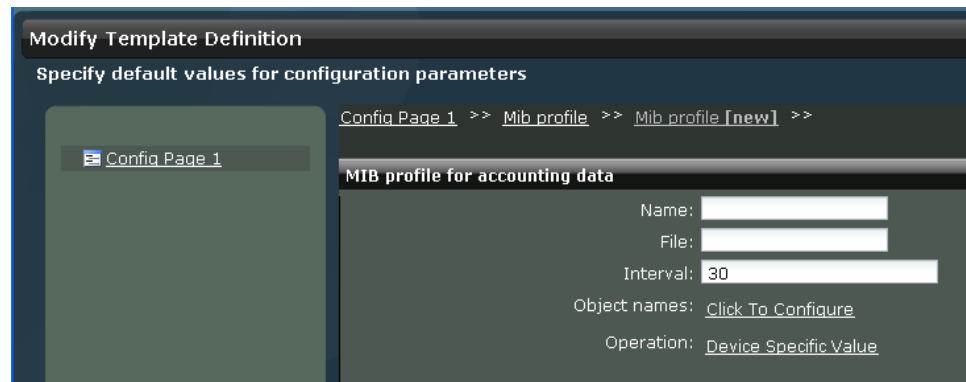
4. Drill down into the configuration pages in the panel on the left and select the option for which you want to use device-specific values.

The parameters for the selected option appear on the right.

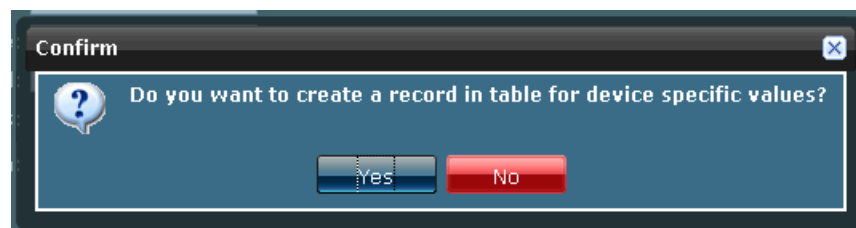
5. If necessary, drill down into the parameters in the panel on the right to find the **Device Specific Value** link.



In the example illustrated, you must click the **Add** button above the table to display the Device Specific Value link next to the Operation label.



Where the device-specific value is in a table, as in the example illustrated, a message appears, asking you to confirm that you want to add a record to the table. Click **Yes**.



6. Click the **Device Specific Value** link.

The Device Specific Value [name of selected configuration option] dialog box appears.

7. Select the **Resolve the value from a CSV file at deploy time** check box.
8. Click **Please select a CSV file**.

The Manage CSV files dialog box appears.

Use the Manage CSV files dialog box to either select a file already in the system, or to navigate and upload CSV files from the local file system. You can view the content of a CSV file already in the system by selecting it in the left pane. Its content displays in the right pane.

9. To upload a file not already in the system, follow the procedure described in ["Managing CSV Files" on page 187](#).

or

To use a CSV file already in the system, select it and click **OK**.

The Device Specific Value [name of selected configuration option] dialog box reappears, this time displaying the name of the CSV file you selected in the previous steps, and the name of the configuration option whose value is to be specified by the CSV file

10. Specify the column and the key column in the CSV file.

To illustrate, we will use an example:

device,interface-1,mtu-1,traps-1,interface-2,mtu-2,traps-2

gemini-re0,ge-0/1/1,1514,1,ge-0/1/2,1518,0

- a. For **Column** select the column with the value to be used. You could begin by specifying any of the values, but we will specify the *name of the first interface*: you would select **interface-1**, and for **Key Column** you would select **device**. These specify the value **ge-0/1/1**.
- b. Still in the **Device Specific Value [name of selected configuration option]** dialog box, click **Save**. The **Create Definition / Specify default values for configuration parameters** page reappears.
- c. You would now specify the *first MTU*, i.e. the one associated with the first interface. Click **Device Specific Value** next to the **Mtu** label, and specify the column and the key column in the CSV file.

For **Column** select **mtu-1** and for **Key Column**, select **device**. These will give you the value **1514**.
- d. Still in the **Device Specific Value [name of selected configuration option]** dialog box, click **Save**. The **Create Definition / Specify default values for configuration parameters** page reappears.
- e. You would continue in the same way by specifying the *traps* for this first interface and MTU, and you would finish by repeating all three operations for the second interface, MTU, and traps. All six values are taken from the same CSV file, although you could use different CSV files if you wished.

11. Click **Finish**.

The template definition is automatically published.

An operator can now create a template from the template definition.

**Related
Documentation**

- [Deploying a Device Template on page 209](#)

Specifying Default Values for Configuration Options

This procedure assumes you have performed the tasks described in [“Creating a Device Template Definition Overview” on page 164](#).

This topic describes how to specify default values for configuration options that the operator sees when using the definition to create a template.

If you choose not to enter default values, the operator must decide what values to enter when creating a template.

To specify default values for configuration parameters:

1. In the Specify default values for configuration parameters page, on the left, select one of your configuration pages.

To the right a breadcrumb of that name appears, and in the pane under that, the options you added to the page on the Create Definition page.

2. 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 [“Defining the Operator's View” on page 167](#).

The screen shows the default configuration parameters for an option of the table data type.

Figure 99: Specify Default Values Page

Specify default values for configuration parameters

Operator View

Add_LdapSvr >> Ldap server >>

Lightweight Directory Access Protocol server options

Id	Name	Port	Retry	Source address	Timeout
1	245.1.1.100	389	3	245.1.1.254	5

No Validation Error

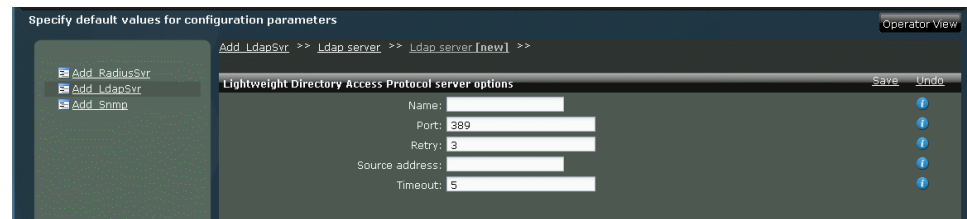
Back Next Finish Cancel

3. 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).

Figure 100: Specify Default Values Page



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.

4. Enter the data as appropriate.



TIP: You may click **Back** to review your settings. 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 was entered on the Description tab.

5. To verify what the operator sees, click **Operator View**. Settings you add from the Operator View are saved to your template definition if you click **Yes** in answer to the question “Do you want to save this draft before you leave this page?” that appears when you click **Designer View**.

To return to the designer view, click **Designer View**.

Repeat these steps as necessary with all your configuration options.

6. To complete the template definition, click **Finish**.



Related Documentation

- [Creating a Device Template Definition Overview on page 164](#)
- [Junos OS Configuration Hierarchy Reference on page 164](#)
- [Specifying Device-Specific Data in Definitions on page 190](#)

Publishing and Unpublishing a Device Template Definition

In the lifecycle of a definition there are two states. [Table 26 on page 196](#) shows the icons that indicate the states of a template definition.

Table 26: Template Definition States

Icon	Description
	Unpublished template definition. When you finish creating a definition, it is automatically published and available to operators.
	Published template definition To make a template definition unavailable to operators, you must unpublish it. You must also unpublish a definition before you can modify or delete it.



NOTE: If you unpublish a definition that is already being used as the basis for templates, all templates based on that definition are disabled. Republishing the definition alone is not enough to re-enable the templates. The templates must be reviewed before they can be re-enabled (see [“Managing Device Templates Overview” on page 203](#)).

1. To view all template definition states, select **Platform > Device Templates > Manage Definitions**.



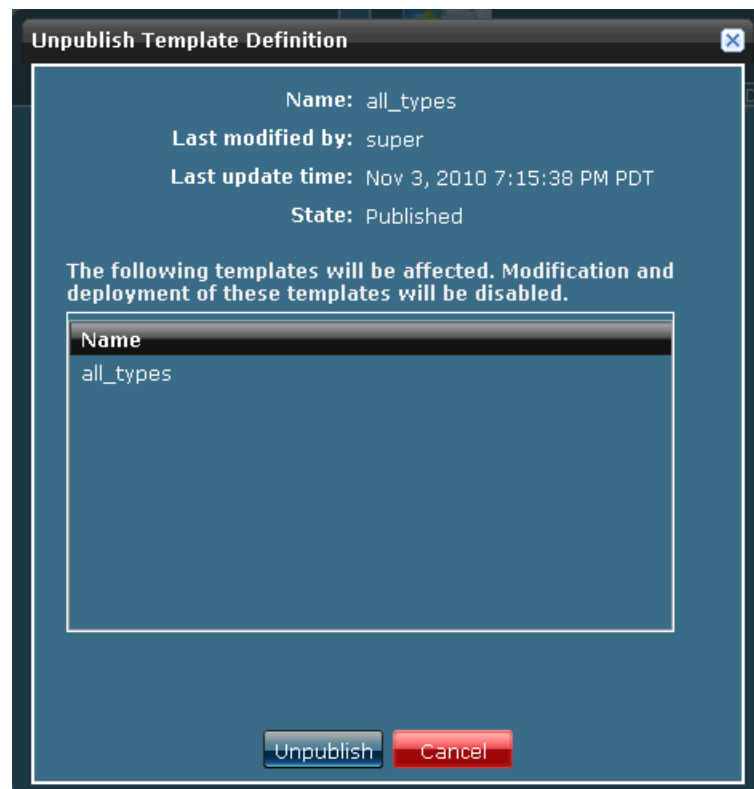
TIP: To use an existing published definition as the basis for a new definition, clone the existing definition and make your modifications to the clone (see [“Cloning a Device Template Definition” on page 198](#)).

To publish a template definition:

1. Navigate to **Manage Definitions**, and select the definition.
2. Either mouse over the Actions drawer to select **Publish** or **Unpublish**, or select the appropriate command from the object right-click pop-up menu.

If you try to unpublish a definition already being used for templates, the **Unpublish Template Definition** dialog box notifies you that in unpublishing, you will disable those templates, and prompts you to confirm you want to do this.

Figure 101: Unpublish Template Definition



Related Documentation

- [Cloning a Device Template Definition on page 198](#)
- [Modifying a Device Template Definition on page 197](#)
- [Changing Device Template Definition States on page 215](#)

Modifying a Device Template Definition

You can modify a template definition only when it is unpublished.

To modify a published definition, you must first unpublish it (see [“Publishing and Unpublishing a Device Template Definition” on page 196](#)).

When you modify a template definition, you cannot change the device family. Also, by default, the same OS and schema versions are used as in the original template definition.

When you modify a template definition, you cannot change any existing pages. You can only add additional pages.

To modify a template definition:

1. Navigate to **Manage Definitions**, and select the definition by clicking on its check box.
2. Either mouse over the Actions drawer to select **Modify**, or select **Modify** from the right-click menu.

3. To make the modified definition available to operators, publish it.



NOTE: Because you must unpublish a definition before modifying it, any templates based on that definition are disabled. After you modify a definition and republish, templates based on that definition are not automatically re-enabled. The status of the affected templates is **Needs Review**.

Related Documentation

- [Publishing and Unpublishing a Device Template Definition on page 196](#)
- [Cloning a Device Template Definition on page 198](#)
- [Deleting a Device Template Definition on page 199](#)
- [Importing a Device Template Definition on page 200](#)
- [Exporting a Device Template Definition on page 201](#)

Cloning a Device Template Definition

Cloning a template definition is the same as copying it. If you want to copy a definition from one Junos Space fabric to another, however, you must import or export it.

To modify a template definition without disabling templates based upon that definition, first clone the definition, then modify the clone.

Unlike the **Modify** function, the **Clone** function does not require that a definition be unpublished.

When you clone a template definition, you cannot change the device family or any existing pages.

To add additional pages, modify the clone (see [“Modifying a Device Template Definition” on page 197](#)).

To clone a template definition:

1. Navigate to **Manage Definitions**, and select the definition by clicking on its check box.
2. Either mouse over the Actions drawer to select **Clone**, or select **Clone** from the right-click menu.

The new definition appears, named **Clone of ...**

3. To make the cloned definition available to operators, publish it (see [“Publishing and Unpublishing a Device Template Definition” on page 196](#)).

Related Documentation

- [Deleting a Device Template Definition on page 199](#)
- [Modifying a Device Template Definition on page 197](#)
- [Publishing and Unpublishing a Device Template Definition on page 196](#)
- [Importing Device Template Definitions Overview on page 162](#)

Deleting a Device Template Definition

You can delete a template definition only when it is unpublished. This status is indicated by an appropriate icon. A different icon indicates a published definition.

To delete a published definition, you must first unpublish it (see [“Publishing and Unpublishing a Device Template Definition” on page 196](#)). When you unpublish a definition, any templates based on that definition are disabled. When you delete a definition, all templates based on that definition are permanently disabled. They can therefore be neither modified nor deployed.

To delete a template definition:

1. Navigate to **Manage Definitions**, and select the definition.
2. Either mouse over the Actions drawer to select **Delete**, or select **Delete** from the right-click menu.



TIP: Ensure that you have a plan in place before you delete a definition that is being used for templates. All templates based on a deleted definition are disabled.

Related Documentation

- [Publishing and Unpublishing a Device Template Definition on page 196](#)
- [Cloning a Device Template Definition on page 198](#)
- [Modifying a Device Template Definition on page 197](#)
- [Changing Device Template Definition States on page 215](#)

Importing a Device Template Definition

Importing a template definition enables you to transfer a definition from another Junos Space fabric.

A template definition is based on a specific OS version, or DMI schema. If the definition you import is based on a schema that is not found, the definition is set to the default DMI schema assigned to the device family to which the definition applies. If you have not set default schemas for your device families, Junos Space 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 Device Template Definition” on page 201](#)).

To import a template definition:

1. From the navigation ribbon, select the Device Templates workspace, and then click the Manage Definitions icon.
2. From the navigation ribbon, click the Import Definition icon.

The Import Definition dialog appears.

3. Click **Browse**.

The File Upload dialog box opens.

4. Navigate to the appropriate file, select it, and click **Open**.

The Import Definition dialog box reappears, displaying the name of the selected file in the Definition File box.



NOTE: Under some circumstances, when the **Import Definition** dialog box reappears, it displays a message beginning the phrase “Confirm name mapping of”. This message serves as a warning that the system has changed:

- The name mapping on the CSV file associated with the imported definition.
- The name of the definition itself.

5. Click **Import**.

The **Manage Template Definitions** page reappears, displaying the newly imported template definition.

The newly imported definition has the same name as the original definition, so you may wish to use the **Modify** command to rename it.

Related Documentation

- [Importing Device Template Definitions Overview on page 162](#)
- [Exporting a Device Template Definition on page 201](#)

- [Modifying a Device Template Definition on page 197](#)
- [Managing Device Template Definitions Overview on page 162](#)

Exporting a Device Template Definition

Exporting a template definition enables you to transfer it to another Junos Space fabric.

Before you begin, you must have a template definition already created.

To export a definition:

1. From the **Manage Template Definitions** page, select the definition to export.
2. Hover over the Actions drawer and select **Export** or right-click the definition and select **Export**.

The **Export Template Definition** dialog box appears.

3. Click **Download file for selected template definitions (tgz format)**.

The **Opening xxx.tgz** dialog box appears. (XXX is a placeholder for the name of the definition.)

4. Select **Save File** and click **OK**.

You may have to toggle between the option buttons to activate the **OK** button.

The **Enter name of file to save to ...** dialog appears.

5. Rename the file if desired and save it to the appropriate location.

The **Export Template Definition** dialog reappears.

6. Click **Close**.

Although the exported definition file is an .xml file, it is saved as a .tgz file, which is the format the system uses to import xml files.

You can now import the definition into another Junos Space fabric.

Related Documentation

- [Importing Device Template Definitions Overview on page 162](#)
- [Importing a Device Template Definition on page 200](#)
- [Cloning a Device Template Definition on page 198](#)
- [Managing Device Template Definitions Overview on page 162](#)

CHAPTER 13

Device Templates

- [Managing Device Templates Overview on page 203](#)
- [Creating a Device Template Overview on page 206](#)
- [Creating a Device Template on page 206](#)
- [Deploying a Device Template on page 209](#)
- [Modifying a Device Template on page 210](#)
- [Deleting a Device Template on page 211](#)
- [Viewing Device Template Inventory on page 212](#)
- [Viewing Device Template Statistics on page 212](#)

Managing Device Templates Overview

The Manage Templates page gives you access to the entire template workflow.

The Manage Templates inventory page enables you to view the Junos OS device templates created to deploy configuration changes to multiple Juniper Networks discovered devices simultaneously. Device templates are derived from device template definitions created by a designer, who assigns the template operator certain configuration settings to configure, review, or validate as necessary, and then deploy.

Device templates appear as icons in the Manage Templates thumbnail view and as rows in a table in tabular view.

From Platform > Device Templates > Manage Templates, you can create , deploy, modify, or delete device templates.






NOTE: Do not use your browser's Back and Forward buttons to navigate in the Device Templates pages.

Template States

Device templates have several states that are identified by icon indicators in the Manage Templates inventory page in thumbnail view. In tabular view these states are indicated in the State column of the table: review, disabled, and enabled—ready to deploy. The title and description tell you how to manage the device template. See [Table 27 on page 204](#).

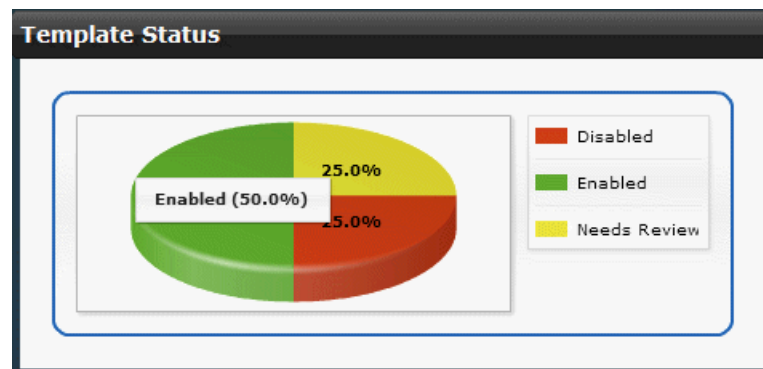
Table 27: Device Template State Icon Indicators

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

Filtering and Searching Templates

You can filter the view of the device templates by state using the Platform > Device Templates statistics page. A quick way to view which templates you need to review, modify, or deploy is to click the status type in the Template Status pie chart—Disabled, Enabled, Needs Review. The Manage Templates inventory page appears filtered by the state you selected.

Figure 102: Template Status Report



You can also search for templates by name using the Search box at the top-right in the Manage Templates inventory page. If you start typing a template name in the Search box, you see the name in the Search Name list.

Device Template Detailed Information

To view detailed template information in the Manage Templates inventory page in thumbnail view, click the **Details** link or double-click the template. In tabular view, template detailed information displays in the table columns. [Table 28 on page 204](#) describes the device template detailed information.

Table 28: Descriptive Information

Information	Description
-------------	-------------

Table 28: Descriptive Information (*continued*)

Name	Unique name for the template.
Description	Description of the device template.
Device Family	Refers to the Juniper Networks DMI Schema, for example J/M/MX/T/TX.
Last Modified By	Login name of the operator who last modified the template.
Last Update Time	Time when the template was last updated.
State	Template deployment readiness: needs review, disabled, or enabled.

Template Actions

From the Manage Templates inventory page, you can perform the following actions:

- Create Template—See [“Creating a Device Template” on page 206](#).
- Deploy Template—See [“Deploying a Device Template” on page 209](#).
- Modify Template—See [“Modifying a Device Template” on page 210](#).
- Delete Template—See [“Deleting a Device Template” on page 211](#).
- Tag It—See [“Tagging an Object” on page 495](#).
- View Tags—See [“Viewing Tags” on page 496](#).
- UnTag It—See [“Untagging Objects” on page 497](#).
- Clear All Selections—All selected device templates on the Manage Templates inventory page are deselected. This action works the same as the **Select: None** link to the left of the Search box.

Related Documentation

- [Creating a Device Template Overview on page 206](#)
- [User Privileges in Device Templates on page 215](#)
- [Deploying a Device Template on page 209](#)
- [Modifying a Device Template on page 210](#)
- [Deleting a Device Template on page 211](#)
- [Creating a Tag on page 498](#)
- [Tagging an Object on page 495](#)
- [Viewing Tags on page 496](#)
- [Untagging Objects on page 497](#)

Creating a Device Template Overview

Device templates enable you to update the configuration committed on multiple Juniper Networks devices in one mechanism. Deploying device templates from Junos Space saves time and reduces the risk of errors, especially when you are responsible for updating the configuration on a large number of devices in the same network when many of the configuration parameters are the same.

The Junos Space device templates user interface is based upon Juniper Network device family schemas. The Device Management Interface (DMI) enables Junos Space to connect with and configure Juniper Networks devices.

This topic covers template creation. Template definitions must be available before you can create any templates.

Ensure that you have the appropriate user permissions before undertaking any of these tasks (see [“User Privileges in Device Templates” on page 215](#)).



NOTE: Do not use your browser’s Back and Forward buttons to navigate in Device Templates pages.

Related Documentation

- [Creating a Device Template on page 206](#)
- [Deploying a Device Template on page 209](#)

Creating a Device Template

Device templates enable operators to update the Junos OS configuration running on multiple Juniper Networks devices at once. Operators can create and deploy device templates (based on definitions created by designers) from Platform > Device Templates > Manage Templates.

Before you begin, ensure that you have the appropriate permissions (see [“User Privileges in Device Templates” on page 215](#)).



NOTE: Do not use your browser’s Back and Forward buttons to navigate in Device Templates pages.

To create a template, complete these main tasks, in order:

1. [Selecting a Device Template Definition on page 207](#)
2. [Naming and Describing a Device Template on page 207](#)
3. [Entering Data and Finishing the Device Template on page 208](#)
4. [Deploying the Device Template on page 209](#)



NOTE: Do not use your browser's Back and Forward buttons to navigate in Device Templates pages.

1. [Selecting a Device Template Definition on page 207](#)
2. [Naming and Describing a Device Template on page 207](#)
3. [Entering Data and Finishing the Device Template on page 208](#)
4. [Deploying the Device Template on page 209](#)

Selecting a Device Template Definition

The Select Template Definitions inventory page enables you to select a template definition from which to create a device template.

You can view the details of the template definition by clicking on the **Details** button on each definition icon in the image view, or by looking at the grid view.

Operators cannot create or change template definitions, only templates themselves. You can regard the device template as an instance of a template definition. You can only make changes to the configuration parameters in your template if the designer has made them editable.

To select a template definition:

1. Navigate to Platform > Device Templates > Manage Templates > Create Templates.
The **Select Template Definition** inventory page appears.
2. Select a template definition.



TIP: Operators can only see published definitions. If you do not see a definition that you expect to see, the designer might have unpublished it.

3. Click **Next**.

The **Create Template** page appears.

Naming and Describing a Device Template

The Create Templates page enables you to view the definition content so that you can name and describe the template you will create from it.

To name and describe a device template:

1. On the Create Templates page, in the Template Name box, enter a name for the device template.

The template name is required. The template name must be unique and limited to 63 characters.

2. Enter a template description in the Description box.

The template description is optional and limited to 255 characters.

If you leave a required field empty, an error message prompts you to fix the error.

Entering Data and Finishing the Device Template

In your template, you can see only the parameters that the definition designer has made visible. You can edit only the parameters that the definition designer has made editable. If you are looking at a template that is in the Needs Review state, it is necessary to look at all the visible parameters, whether you can change them or not.

1. In the **Create Template** page, on the left, select a configuration page.

To the right a breadcrumb of that name appears, and in the pane under that, the configuration options.



TIP: To navigate through the configuration options on any page, click the breadcrumbs.

As you drill down, successive breadcrumbs appear, with the names of the options you clicked to configure, enabling you to navigate through multiple configuration option levels.

The layout of the configuration settings on the page varies depending on the data type of the configuration option selected.

2. To display the settings that are not immediately evident, click **Click To Configure**.
3. (Optional) For information on the individual parameters, click the little blue information icons to the right of the configuration settings to display the explanations the designer wrote.
4. (Optional) 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.

5. To save your entries, you can:

- Click **Save**.
- Click another link or a breadcrumb.

A message appears, prompting you to confirm that you want to save.

- Click **Finish**.

6. (Optional) To delete your entries, click **Undo**.

7. (Optional) To add a row to a table, click the plus sign (+).

To remove a row from a table, select the row and click the minus sign (-). To edit a table row, select the row and click the pencil icon (looks like a diagonal line).

8. Enter the data, as appropriate.

If you enter an invalid value, a red exclamation mark icon appears. Click the icon to find out what the value should be.

9. Click **Finish**.

The template appears on the Manage Templates inventory page. The template details include the name, description, device family, last modified by login name, last update time, and state. The template is automatically enabled.

Deploying the Device Template

To deploy a device template to selected devices, see [“Deploying a Device Template” on page 209](#).

Related Documentation

- [Deploying a Device Template on page 209](#)
- [Modifying a Device Template on page 210](#)
- [Selecting the Device Family and Naming a Device Template Definition on page 169](#)
- [Publishing and Unpublishing a Device Template Definition on page 196](#)

Deploying a Device Template

Deploying a device template allows the Template Administrator or operator to update the device configuration on multiple devices. Deploying a template is the second stage of creating a template. For more information about creating a template, see [“Creating a Device Template” on page 206](#). You can deploy a template when you create it or schedule it to deploy later.



NOTE: When you select devices in a service order selection, you can select devices that are down. This is permitted because the device status could change between the time the deploy is submitted and the time the actual push is performed.

Junos Space allows you to validate the template against the device family and against the device.

To deploy a device template:

1. Navigate to Platform > Device Templates > Manage Templates.

The Manage Templates inventory page appears.

2. Right-click the template you want to deploy and select **Deploy Template** from the pop-up menu.

You can also select **Deploy Template** from the Actions drawer.

The **Platform > Devices > Manage Devices > Select Devices** inventory page appears, displaying Junos Space devices.

3. Select the devices to which you want to deploy the template.

4. Click **Next**.

The **Review Changes** page appears for you to review the validation result.

This is the static template validation related to the CSV file. Does the CSV file have all the device specific values? If there is an error, request that the designer fix the CSV file or ensure that the right devices have been selected to deploy the template.

The validation ensures that the template is syntactically correct against the device family.

5. Click **Validate** to test the template against the selected device.

The device validation ensures that the template is semantically correct. Junos Space performs a check on the device and displays any errors in the Device Validation Result dialog box, which lists all the devices that are affected.

6. If the device validation result is successful, click **OK**.

7. Click **Next**.

The **Deployment Confirmation** dialog box appears.

You can select the deployment options, including scheduling deployment at a later time.

If you schedule deployment at a later time, set the time and date.

If you do not schedule template deployment, the template deploys immediately.

8. Click **Finish**.

Junos Space creates a job. The **Deploy Template Job Information** dialog box appears.

9. Click the **job ID** to ensure the template deployment is successful.

10. Click **OK**.

11. If you need to troubleshoot template deployment, navigate to **Platform > Audit Logs > View Audit Logs** to review what configuration was deployed on each device.

The **Audit Log** page captures all template deployment operations.

Related Documentation

- [Creating a Device Template Overview on page 206](#)
- [Creating a Device Template on page 206](#)
- [Modifying a Device Template on page 210](#)
- [Deleting a Device Template on page 211](#)

Modifying a Device Template

Modifying a device template allows you to make changes to it before deploying.

If you need to modify the template after deployment, the Template Designer must check the template and the template definition to fix any errors. Thereafter, you must redeploy the template. For more information about deploying a template, see [“Deploying a Device Template” on page 209](#).

You must have the appropriate user privileges before undertaking this task (see [“User Privileges in Device Templates” on page 215](#)).

A device template must be enabled for you to modify or deploy it.

To modify a device template:

1. Navigate to Platform > Device Templates > Manage Templates.

The Manage Templates inventory page appears.

2. Right-click the device template you want to modify and select Modify Template.

You can also select the device template and hover over the Actions drawer to select Modify.

3. Modify the template name, description, or configuration settings.

4. Click **Finish**.

Now, you can deploy the template.

If you need to modify the template after deployment, the Template Designer must check the template and the template definition to fix any errors. Thereafter, you must redeploy the template. For more information about deploying a template, see [“Deploying a Device Template” on page 209](#)

Related Documentation

- [Creating a Device Template Overview on page 206](#)
- [Creating a Device Template on page 206](#)
- [Deploying a Device Template on page 209](#)
- [Deleting a Device Template on page 211](#)

Deleting a Device Template

Deleting a device template removes it from the Junos Space database.

You need to have the appropriate user privileges before undertaking this task (see [“User Privileges in Device Templates” on page 215](#)).

1. Navigate to Platform > Device Templates > Manage Templates.

The Manage Templates inventory page appears.

2. Right-click the device template you want to delete and select **Delete Template** from the pop-up menu.

The device template disappears from the Manage Templates inventory page.

- Related Documentation**
- [Creating a Device Template Overview on page 206](#)
 - [Modifying a Device Template on page 210](#)

Viewing Device Template Inventory

To view Device Template inventory, in the Device Template workspace, click **Manage Templates**. The Manage Templates inventory page appears.

You can display templates in thumbnail or tabular views. To change the view, click the appropriate icon in the Manage Templates banner. You can also do the following:

- Use the Search function to find a particular template.
- Select all templates on a page, or you can deselect them.
- You can refresh the page by clicking on the Refresh icon in the status bar.
- When you have selected a template, you can perform actions on it by right-clicking it or hovering over the Actions drawer.

- Related Documentation**
- [Deleting a Device Template on page 211](#)
 - [Deploying a Device Template on page 209](#)
 - [Modifying a Device Template on page 210](#)
 - [Tagging an Object on page 495](#)
 - [Untagging Objects on page 497](#)
 - [Viewing Device Template Statistics on page 212](#)

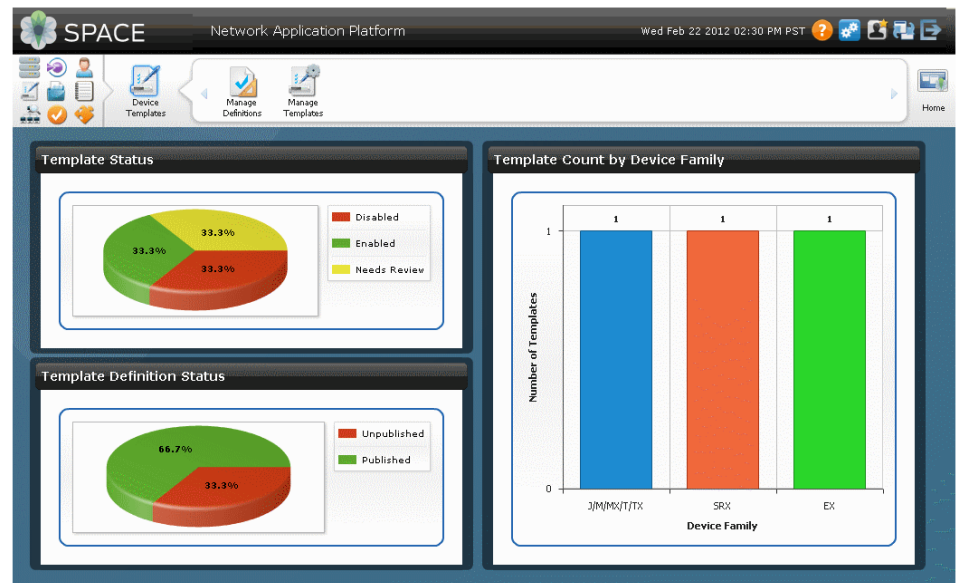
Viewing Device Template Statistics

The device template statistics page shows the states of both definitions and templates, and the number of templates per device family.

All the charts are interactive. Clicking on the enabled templates part of the Template Status chart, for example, takes you directly to the page displaying that category of template.



NOTE: Do not use your browser's Back and Forward buttons to navigate in Device Templates pages.



The Device Templates statistics page displays the following information:

- **Template Status**—this pie chart shows the templates that are enabled, disabled, and needing review. The templates based on a definition that is currently in a published state are enabled. Templates based on a definition that is currently unpublished are disabled. Templates based on a republished definition are marked as needing review.
- **Template Definition Status**—this pie chart shows published and unpublished definitions (available for template creation and unavailable, respectively).
- **Template Count by Device Family**—this bar chart shows the number of templates per device family (each template can apply to only one device family).

Related Documentation

- [Changing Device Template Definition States on page 215](#)
- [Viewing Device Template Inventory on page 212](#)
- [Managing Device Template Definitions Overview on page 162](#)
- [Publishing and Unpublishing a Device Template Definition on page 196](#)

Troubleshooting

- [Changing Device Template Definition States on page 215](#)
- [User Privileges in Device Templates on page 215](#)

Changing Device 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 215](#)

- 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 Device Template Definition on page 196](#)
- [Device Template Definition Workflow on page 163](#)
- [Creating a Device Template on page 206](#)
- [Creating a Device Template Definition Overview on page 164](#)

User Privileges in Device Templates

In Junos Space 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 371](#)

PART 4

Device Images and Scripts

- [Overview on page 219](#)
- [Device Images on page 223](#)
- [Scripts on page 225](#)
- [Operations on page 229](#)
- [Script Bundles on page 231](#)
- [Configuration: Device Images on page 233](#)
- [Configuration: Scripts on page 247](#)
- [Configuration: Operations on page 259](#)
- [Configuration: Script Bundles on page 267](#)
- [Administration: Scripts on page 275](#)
- [Administration: Operations on page 279](#)

CHAPTER 15

Overview

- [Device Images and Scripts Overview on page 219](#)

Device Images and Scripts Overview

In Junos Space, a device image is a software installation package that enables you to upgrade or downgrade from one Junos operating system (Junos OS) release to another. Scripts are configuration and diagnostic automation tools provided by Junos OS.

Device Images and Scripts is a workspace in the Junos Space Network Application Platform that enables you to manage these device images and scripts.

You can access the Device Images and Scripts workspace by clicking **Device Images and Scripts** on the navigation ribbon.

The Device Images and Scripts workspace enables you to perform the following tasks:

- Manage device images

You can upload device images from your local file system and deploy these device images to a device or onto multiple devices of the same device family simultaneously. After uploading device images, you can stage a device image on a device, verify the checksum, and deploy the staged image whenever required. You can also schedule the staging, deployment, and validation of device images.

- Manage scripts

You can import multiple scripts into the Junos Space server and perform various tasks such as modifying the scripts, viewing their details, exporting their content, comparing them, and deploying them on multiple devices simultaneously. After you deploy scripts onto devices, you can use Junos Space to enable, disable, and execute them on those devices.

- Manage operations

You create, manage, and execute operations that combine multiple script and image tasks, such as upgrading images and deploying or executing scripts, into a single bundle for efficient use and reuse.

- Manage script bundles

You can group multiple op scripts into a script bundle. Script bundles can be deployed and executed on devices. You can also modify and delete script bundles.

User Roles

The Junos Space user administrator creates users and assigns roles (permissions) so that users can access and perform different tasks. You must be given access to a page in order to view it. While Junos Space allows the admin to create users and control their access to different tasks, it also has a set of predefined user roles. [Table 29 on page 220](#) describes the Device Images and Scripts tasks to which different users have access, based on the roles the admin assigns to them.

You can create users and manage them on the Manage Users page, if you have user administrator permissions. To create and manage these users, navigate to **Application Switcher > Network Application Platform > Users > Manage Users**. The Manage Users page lists the existing users. Use this page to create and assign roles to Device Images and Scripts users.

You can enable and disable scripts on devices that use Junos Space 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.

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

Table 29: Device Images and Scripts User Roles

User Role	Permitted Tasks
For Device Images	
Device Image Manager	Viewing, uploading, modifying, deleting, staging, verifying the checksum of, and deploying device images.
Device Script Manager	Viewing, importing, modifying, comparing, deleting, deploying, enabling, disabling, verifying, removing, and executing scripts.
For Scripts	
Device Script Read Only User	Viewing Manage Scripts and Manage Script Bundles pages. Exporting scripts.
Device Image Read Only User	Viewing Manage Images pages.

- Related Documentation**
- [Device Images Overview on page 223](#)
 - [Operations Overview on page 229](#)
 - [Scripts Overview on page 225](#)
 - [Script Bundles Overview on page 231](#)

CHAPTER 16

Device Images

- [Device Images Overview on page 223](#)

Device Images Overview

In Junos Space, a device image is a software installation package that enables you to upgrade or downgrade from one Junos operating system (Junos OS) release to another. You can download these device images from <https://www.juniper.net/customers/support/>. For more information about downloading the device image, see the *Junos OS Installation and Upgrade Guide*.

Junos Space facilitates management of device images for devices running Junos OS by enabling you to upload device images from your local file system and deploy these device images onto a device or onto multiple devices of the same device family simultaneously. You can modify the platforms supported by the device image and the description of the device image. After uploading device images, you can stage a device image on a device, verify the checksum, and deploy the staged image whenever required. You can also schedule the staging, deployment, and validation of device images.

[Table 30 on page 223](#) describes the Manage Images page.

Table 30: Manage Images Page

Field	Description
File Name	Name of the device image.
Version	Version of the device image.
Series	Series supported by the device image.

You can perform the following tasks from the Manage Images page:

- Stage an image on devices
- Verify the checksum
- Deploy device images

- [Delete device images](#)
- [Modify device images](#)

**Related
Documentation**

- [Deploying Device Images on page 238](#)
- [Staging Device Images on page 234](#)
- [Modifying Device Image Details on page 244](#)
- [Uploading Device Images to Junos Space on page 233](#)
- [Scripts Overview on page 225](#)
- [Script Bundles Overview on page 231](#)
- [Operations Overview on page 229](#)

Scripts

- [Scripts Overview on page 225](#)

Scripts Overview

Scripts are configuration and diagnostic automation tools provided by Junos OS. They help reduce network downtime and configuration complexity, automate common tasks, and decrease the time to problem resolution. Junos OS scripts are of three types: commit, op, and event scripts.

- **Commit scripts:** Commit scripts enforce custom configuration rules and can be used to automate configuration tasks, enforce consistency, prevent common mistakes, and more. Every time a new candidate configuration is committed, the active commit scripts are called and inspect the new candidate configuration. If a configuration violates your custom rules, the script can instruct the Junos OS to perform various actions, including making changes to the configuration, and generating custom, warning, and system log messages.
- **Op scripts:** Op scripts enable you to add your own commands to the operational mode CLI. They can automate the troubleshooting of known network problems, and correcting them.
- **Event scripts:** Event scripts use event policies to enable you to automate network troubleshooting by diagnosing and fixing issues, monitoring the overall status of the router, and examining errors periodically. Event scripts are similar to op scripts but are triggered by events that occur on the device.

Using Junos Space you can import multiple scripts into the Junos Space server. After importing scripts, you can perform various tasks such as modifying the scripts, viewing their details, exporting their content, comparing them, and deploying them on multiple devices simultaneously. After you deploy scripts onto devices, you can use Junos Space to enable, disable, and execute them on those devices. You can remove the scripts from the devices as well. To help ensure that the deployed scripts are not corrupt, you can verify the checksum of the scripts.

Junos Space 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.

[Table 31 on page 226](#) describes the information that appears on the Manage Scripts page (see [Figure 103 on page 226](#)).

Figure 103: Manage Scripts page

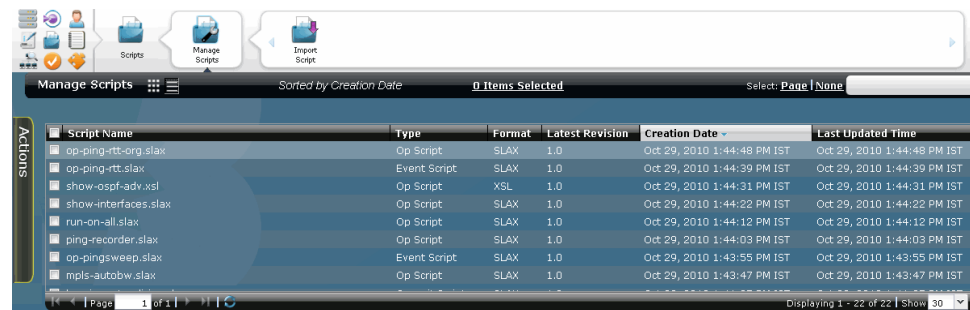


Table 31: Manage Scripts Page Fields Description

Field	Description
Script Name	Name of the script file.
Type	Type of script: <ul style="list-style-type: none"> • Commit script • Op script • Event script
Format	Format of the script file: <ul style="list-style-type: none"> • XSL • SLAX
Version	Version number of the script.
Creation Time	Date and time when the script was created.
Last Updated Time	Latest time when the script was last updated.

You can perform the following tasks from the Manage Scripts page:

- Import scripts
- View script details
- Modify scripts
- Modify script types
- Compare script versions
- Delete scripts
- Export scripts in .tar format
- Deploy scripts to devices
- Verify the checksum of scripts on devices
- View verification results

- Enable scripts on devices
- Disable scripts on devices
- Remove scripts from devices
- Execute scripts on devices

**Related
Documentation**

- *Scripts User Roles*
- [Importing a Script on page 247](#)
- [Viewing Script Details on page 275](#)
- [Modifying a Script on page 248](#)
- [Modifying Script Types on page 249](#)
- [Comparing Script Versions on page 250](#)
- [Deleting Scripts on page 251](#)
- [Exporting Scripts in Tar Format on page 278](#)
- [Deploying Scripts on Devices on page 252](#)
- [Verifying the Checksum of Scripts on Devices on page 253](#)
- [Viewing Verification Results on page 277](#)
- [Enabling Scripts on Devices on page 255](#)
- *Disabling Scripts on Devices*
- [Removing Scripts from Devices on page 256](#)
- [Executing Scripts on Devices on page 257](#)
- [Device Images Overview on page 223](#)
- [Script Bundles Overview on page 231](#)
- [Operations Overview on page 229](#)

CHAPTER 18

Operations

- [Operations Overview on page 229](#)

Operations Overview

In Junos Space, a device image is a software installation package that enables you to upgrade or downgrade from one Junos operating system (Junos OS) release to another. Scripts are configuration and diagnostic automation tools provided by Junos OS.

Junos Space enables you to simultaneously execute scripts and device images by allowing you to group tasks, such as staging device images and deploying or executing scripts, into a single operation. This facilitates efficient use and reuse.

Using the Manage Operations task, you can:

- Create an operation
- Modify an operation
- Create a copy of an existing operation
- Execute (or run) an operation
- Delete an operation
- View information about operations in four stages of execution (successful, failed, in progress, and scheduled).

Related Documentation

- [Creating an Operation on page 259](#)
- [Modifying an Operation on page 262](#)
- [Running an Operation on page 263](#)
- [Copying an Operation on page 264](#)
- [Viewing Operations Results on page 279](#)
- [Deleting an Operation on page 265](#)
- [Scripts Overview on page 225](#)
- [Device Images Overview on page 223](#)
- [Script Bundles Overview on page 231](#)

CHAPTER 19

Script Bundles

- [Script Bundles Overview on page 231](#)

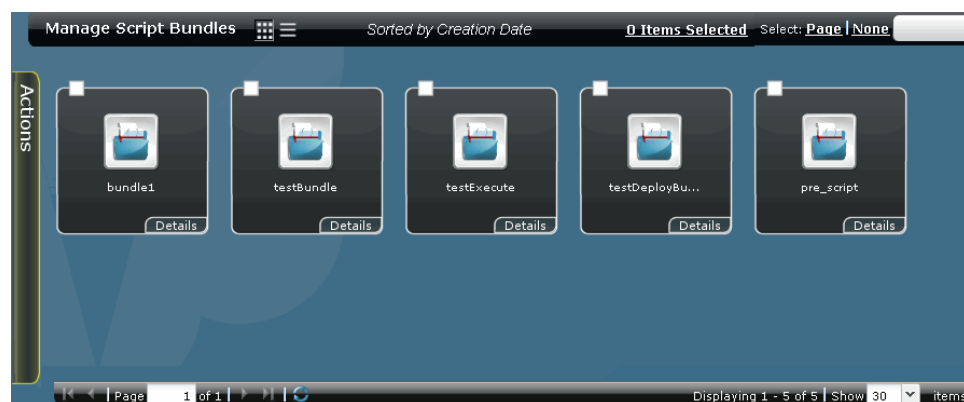
Script Bundles Overview

Scripts are configuration and diagnostic automation tools provided by Junos OS. They help reduce network downtime and configuration complexity, automate common tasks, and decrease the time to problem resolution. Junos OS scripts are of three types: commit, op, and event scripts.

Junos Space 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 a Script” on page 247](#)). The script bundles that you create are displayed on the Manage Script Bundles page (see [Figure 104 on page 231](#)). 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 225](#).

Based on the user role assigned to your username, Junos Space enables and disables different tasks. For more information about Network Application Platform–Scripts user roles see, *Scripts User Roles*.

Figure 104: Manage Script Bundles Page



You can execute the following tasks from the Manage Script Bundles page:

- Create script bundles
- Deploy script bundles to devices
- Execute script bundles on devices
- Modify a script bundle
- Delete script bundles

**Related
Documentation**

- [Creating a Script Bundle on page 267](#)
- [Deploying Script Bundles on Devices on page 270](#)
- [Executing Script Bundles on Devices on page 271](#)
- [Modifying a Script Bundle on page 268](#)
- [Deleting Script Bundles on page 270](#)
- [Device Images Overview on page 223](#)
- [Scripts Overview on page 225](#)
- [Operations Overview on page 229](#)

CHAPTER 20

Configuration: Device Images

- Uploading Device Images to Junos Space on page 233
- Staging Device Images on page 234
- Verifying the Checksum on page 235
- Viewing and Deleting MD5 Validation Results on page 236
- Deploying Device Images on page 238
- Viewing Device Image Deployment Results on page 243
- Deleting Device Images on page 243
- Modifying Device Image Details on page 244

Uploading Device Images to Junos Space

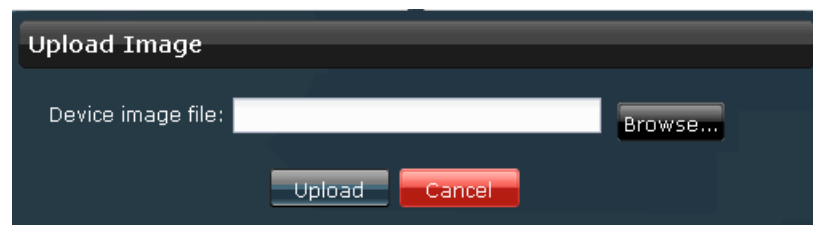
To deploy a device image that uses Junos Space, you must first download the device image from the Juniper Networks Support webpage <http://www.juniper.net/customers/support/>. Download the device image to the local file system of your workstation or client, and then upload it into the Junos Space server. Once the image is uploaded, you can stage a device image, verify the checksum, deploy the device image on one or more devices, modify the description and supported platforms, and also delete the device image from Junos Space.

To upload device images:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Images > Upload Image**.

The Upload Image dialog box appears.

Figure 105: Upload Image Dialog Box



2. Click **Browse**.

The File Upload dialog box displays the directories and folders on your local file system.

3. Navigate to the device image file and click **Open**.
4. Click **Upload**.

The time taken to upload the file depends on the size of the device image and the connection speed between the local machine and the Junos Space server. Once the file is uploaded onto the platform, it is listed on the Manage Images page.

Related Documentation

- [Device Images Overview on page 223](#)
- [Deploying Device Images on page 238](#)
- [Staging Device Images on page 234](#)

Staging Device Images

Junos Space enables you to stage an image on one device or on multiple devices of the same device family simultaneously. Staging an image enables you to hold a device image on a device, ready to be deployed when needed. At any given time, you can stage only a single device image. Staging images repeatedly on a device merely replaces the staged device image. While staging device images, you can also delete existing device images from the device. After you stage a device image, you can verify the checksum to ensure that the device image was transferred completely.

To stage an image on devices:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Images**.

The Manage Images page appears.

2. Select the image that you want to stage on one or more devices.

The selected image is highlighted.

3. Right-click the selected device image and select **Stage Image on Device**.

The Stage Image On Devices dialog box displays a list of the Junos Space devices.

Stage Image On Devices

Image name: jinstall-ex-4500-10.3R1.9-domestic-signed.tgz

Host Name	IP Address	Platform	Serial Number	Software Version
tsunami5-nmft	10.204.97.231	EX4500-40F	DE0210215083	11.1-20101030.0

Page 1 of 1 | Displaying 1 - 1 of 1

Staging Options

☐ Delete any existing image before download

☐ Schedule at a later time

Stage Image **Cancel**

4. Select the device or devices on which you want to stage the device image. By default, 25 devices are displayed. Use the navigation arrows to select devices across multiple pages.
5. To delete existing device images from the device, expand the Staging Options section and select the **Delete any existing image before download** check box. This deletes all .tgz files and files whose filenames begin with **jinstall**.
6. 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.
7. Click **Stage Image**.

The image is staged on the selected device or devices and a Jobs dialog box displays the job ID.
8. To verify the status of this job, click the job ID link or navigate to the Manage Jobs page and view the status of the job. When there is a failure in the staging of the device image, you can view the reason for failure within the job description.

To verify the checksum of the staged device image, see [“Verifying the Checksum” on page 235](#).

Table 32: Stage Image On Devices Dialog Box Fields Descriptions

Field	Description
Image Name	Name of the device image.
Host Name	Identifier used for network communication between Junos Space and the Junos OS device.
IP Address	IP address of the device.
Platform	Model number of the device.
Serial Number	Serial number of the device chassis.
Software Version	Operating system firmware version running on the device.

- Related Documentation**
- [Device Images Overview on page 223](#)
 - [Deploying Device Images on page 238](#)
 - [Verifying the Checksum on page 235](#)

Verifying the Checksum

When you stage an image on a device that use Junos Space, sometimes the device image might not get completely transferred to the device. Verifying the checksum helps validate the completeness of the staged device image.

To verify the checksum:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Images**.

The Manage Images page appears.

2. Select the image whose checksum you want to verify.
3. Right-click the selected device image and select **Verify Checksum**.

The Manage Images dialog box appears.

4. Select the devices that have the device image staged on them.
5. To schedule a time for verifying the checksum, select the **Schedule a later time** check box and use the lists to specify the date and time.
6. Click **Verify**.

The selected image is verified and a Jobs dialog box displays the job ID.

7. To check the status of verification you can click on the job ID link or navigate to the Manage Jobs page and view the job status.

- Related Documentation**
- [Device Images Overview on page 223](#)
 - [Deploying Device Images on page 238](#)

Viewing and Deleting MD5 Validation Results

Using Junos Space, you can validate completeness of a device image that is staged on devices. See “[Verifying the Checksum](#)” on page 235. 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 236](#)
- [Deleting the MD5 Validation Results on page 237](#)

Viewing the MD5 Validation Results

The MD5 validation results indicate whether the device image that is staged on a device is completely transferred to the device or not. The result also indicates whether the device image is not present on the selected devices.

To view the MD5 validation results:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Images**.
The Manage Images page displays the list of device images.
2. Select a device image.
3. Right-click your selection and select **MD5 Validation Result**.

The Validation Results page displays the results of verification tasks, as shown in [Figure 106 on page 237](#).

Device image name	Device name	Action	Checksum Result	Remarks	Verification Time
jinstall-ex-3200-10.0R2.10-domestic-signed.tgz	e48t2-nmsft	Verify	Success		May 7, 2010 1:44:22 PM IST
jinstall-ex-3200-10.0R2.10-domestic-signed.tgz	e48p2-nmsft	Verify	Failed	Error from device md5: /var/tmp/jinstall-ex-3200-10.0R2.10-domestic-signed.tgz: No such file or directory	May 7, 2010 1:44:02 PM IST
jinstall-ex-3200-10.0R2.10-domestic-signed.tgz	e123	Verify	Failed	Error from device md5: /var/tmp/jinstall-ex-3200-10.0R2.10-domestic-signed.tgz: No	May 7, 2010 1:44:00 PM IST

Table 33 on page 237 describes the Validation Results page.

Table 33: Validation Results Page Field Descriptions

Field Name	Description
Device Image Name	Name of the device image selected for verifying the checksum.
Device Name	Name of the selected devices on which the device images are verified.
Action	Name of the action performed.
Checksum Result	Result of the verification
Remarks	Observations made during the verification.
Verification Time	Time at which the verification was initiated.

Deleting the MD5 Validation Results

To delete the MD5 validation results:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Images**.

The Manage Images page appears.

2. Select a device image.

3. Right-click your selection and select **MD5 Validation Result**.

The Validation Results page displays the results of all verification tasks.

4. Select the result that you want to delete.

5. Right-click your selection and select **Delete Validation Results**.

The **Delete Validation Results** dialog box displays the selected results.

6. Click **Delete** to confirm.

The selected results are removed from Junos Space.

Related Documentation

- [Device Images Overview on page 223](#)
- [Staging Device Images on page 234](#)
- [Verifying the Checksum on page 235](#)

Deploying Device Images

Junos Space enables you to deploy device images onto a device or on multiple devices of the same device family simultaneously. During deployment, a device image is installed on the device. After you deploy an image onto a device, you can reboot the device, delete the device image from the device, check the device image's compatibility with the current configuration of the device, and load the image when even a single statement is valid. Using an image that is already staged on a device eliminates the time taken to load the device image on a device and directly jumps to the installation process. Junos Space also enables you to schedule a time when you want the image to be deployed.

On dual Routing Engine platforms, you can also do an in-service software upgrade (ISSU) between two different Junos software releases with no disruption on the control plane and with minimal disruption of traffic. This provides the following benefits:

- Eliminates network downtime during software image upgrades
- Reduces operating costs, while delivering higher service levels
- Allows fast implementation of new features.

During the ISSU, the backup Routing Engine is rebooted with the new software package and switched over to make it the new primary Routing Engine. The former primary Routing Engine can also be upgraded to the new software and rebooted.

[Table 34 on page 238](#) describes the devices and software releases that support ISSU.

Table 34: 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.	
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

Additionally you must note the following in connection with doing an ISSU:

- You can upgrade to a software version that supports unified ISSU from a software version that does not support unified ISSU only by means of a conventional upgrade. During the conventional upgrade, all line modules are reloaded, all subscribers are dropped, and traffic forwarding is interrupted until the upgrade is completed.
- The armed (upgrade) release must be capable of being upgraded to from the currently running release.
- All applications that are configured on the router must support unified ISSU and stateful SRP switchover.
- If one or more unified ISSU-challenged applications are configured and you proceed with a unified ISSU, the unified ISSU process forces a conventional upgrade on the router.



NOTE: We strongly recommend that you configure the Virtual IP on the dual Routing Engine device. Dual Routing Engine devices without Virtual IP configuration are not yet fully supported on Junos Space.

For complete details about the protocols, features, and PICs supported by ISSU, refer to the Unified ISSU System Requirements sections in the *Junos OS High Availability Configuration Guide*.

You can deploy a device image only onto devices or platforms supported by that device image. When you select an image for deployment, the list of the displayed devices contains only those devices that are supported by the selected device image.



NOTE: In Junos Space, an SRX Series cluster is represented as two individual devices with cluster peer information. When you deploy a device image on an SRX cluster, the image is installed on both cluster nodes.

To deploy device images:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Images**.

The Manage Images page appears.

2. Select the image that you want to deploy.

The selected image is highlighted.

3. Right-click the selected device image or go to the Actions drawer.

4. Click **Deploy Device Image** from the Actions drawer.

The Select Devices table at the top of the Deploy Image on Device page displays the devices that are supported by the selected device image. For a description of the fields in this table, see [Table 39 on page 242](#).

5. Select the devices on which you want to deploy the device image.

6. To specify different deployment options, select one or more of the check boxes in the Common Deployment Options and/or Conventional Deployment Options sections.

See [Table 35 on page 241](#) and [Table 36 on page 241](#) for a description of the deployment options.



NOTE: When you do a conventional upgrade of the device image on dual Routing Engines (RE), the image is first deployed on the backup Routing Engine followed by the primary Routing Engine. If deployment fails on the backup Routing Engine, the device image is not deployed on the primary Routing Engine.

7. (Optional) To perform an ISSU on a dual Routing Engine device, open the ISSU Deployment Options section, and check one or more of the check boxes. The ISSU option is enabled only if the selected device has a dual Routing Engine. This capability is shown in the Platform column in the Select Devices table in the upper part of the screen.

See [Table 37 on page 241](#) for a description of the ISSU deployment options.

8. To specify advanced deployment options, select one or more of the Select Advanced Deployment options check boxes. See [Table 38 on page 242](#) for a description of the advanced deployment options.

To configure the script parameters of scripts included in the script bundle:

- a. Select the prescript or postscript bundle that you want to configure, using the respective lists.

If there are no script bundles available, you can create script bundles using the Scripts workspace (see [“Creating a Script Bundle” on page 267](#)) and then re-select the script bundle during script deployment.

- b. Click the **Configure Scripts Parameters** link.

The Configure Script Bundle Parameters page appears. You can hover over the script parameters to view short descriptions about them.

- c. You can edit the value (success or failure) of script parameters using the icon shown below before deploying the script bundles on devices. The changes made to script parameters are saved only on the devices on which the script bundle is executed. The script parameters in the script bundle in Junos Space continues to reflect the original values.



- d. Click **Configure**.

Your changes are saved and the Deploy Image on Device page appears.

9. 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.

10. Click **Deploy**.

The selected image is deployed on the specified devices with the deployment options that you specified.

11. To view the result of deployment, navigate to the View Deploy Results page. See [“Viewing Device Image Deployment Results” on page 243](#).**Table 35: Common Deployment Options Description**

Common Deployment Options	Description
Use image already downloaded to device	Use the device image that is staged on the device for deployment.
Archive Data (Snapshot)	Collect and save device data and executable areas.
Remove the package after successful installation	Delete the device image from the device after successful installation.
Delete any existing image before download	Delete all device images with the same filename from the device before deploying the selected device image.

Table 36: Conventional Deployment Options Description

Conventional Deployment Options	Description
Check compatibility with current configuration	Verify device image compatibility with the current configuration of the device.
Load succeeds if at least one statement is valid	Ensure that the device image is loaded successfully even if only one of the statements is valid.
Reboot device after successful installation	<p>Reboot the device after deployment is successful. If the device is down, Junos Space 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.</p> <p>After rebooting the device, the status of the device is checked every 5 minutes to check whether the device is up.</p>
Upgrade Backup Routing Engine only	Deploys the image to only the backup Routing Engine.

Table 37: ISSU Deployment Options Description

ISSU Deployment Options	Description
Upgrade the former Master with new image	After the backup Routing Engine is rebooted with the new software package and a switchover occurs to make it the new primary Routing Engine, the former primary (new backup) Routing Engine is automatically upgraded. If you do not check this option, the former primary must be manually upgraded.
Reboot the former Master after a successful installation	The former primary (new backup) Routing Engine is rebooted automatically after being upgraded to the new software. If this option is not selected, you must manually reboot the former primary (new backup) Routing Engine.

Table 37: ISSU Deployment Options Description (*continued*)

ISSU Deployment Options	Description
Save copies of the package files on the device	Copies of the package files are retained on the device.

[Table 38 on page 242](#) describes the different advanced deployment options.

Table 38: Advanced Deployment Options Description

Advanced Deployment Options	Description
Execute script bundle before image deployment (pre scripts)	<p>With this option, you have the opportunity to configure scripts parameters after you have select a script bundle.</p> <p>Execute the selected script bundle before deploying the device image. This ensures that the scripts in the selected script bundle are executed before the device image is installed on the device.</p>
Select same pre script bundle for post script bundle	Execute the same script bundle on the device before and after device image deployment.
Execute script bundle after image deployment (post scripts)	<p>With this option, you have the opportunity to configure scripts parameters after you have select a script bundle.</p> <p>Execute the selected script bundle before deploying the device image. This ensures that the script bundle is executed after the device image is installed on the device.</p>
Deploy and Enable script bundle before execution	Deploy the selected script bundle, enable the scripts included in the script bundle, and then execute the script bundle on the device.
Disable scripts after execution	Execute the script bundle on the device and then disable the script bundle.

describes the **Select Devices** table fields.

Table 39: Select Devices Table Field Descriptions

Field	Description
Image Name	Name of the device image. (This field is above the table.)
Host Name	Identifier used for network communication between Junos Space 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.

- Related Documentation**
- [Device Images Overview on page 223](#)
 - [Uploading Device Images to Junos Space on page 233](#)
 - [Script Bundles Overview on page 231](#)

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. From the navigation ribbon, select **Device Images and Scripts > Manage Images > View Deploy Results**.

The View Deploy Results page displays the job Id, timestamp, job description, scripts executed, and the results of the device images that you deployed on devices, as shown in [Figure 107 on page 243](#).

Figure 107: View Deploy Results Page

Job Id	Timestamp	Job Description	Scripts Executed	Results
98545	May 27, 2011 6:38:22 AM IST	Selected deployment options: ->Use already downloaded device image. Total number of requests: 1 Success count : 0	false	SUCCESS
426018	May 27, 2011 7:38:03 AM IST	Selected deployment options: Total number of requests: 1 Success count : 0	true	FAILURE
426008	May 27, 2011 7:25:24 AM IST	Selected deployment options: Total number of requests: 1 Success count : 0	false	SUCCESS

Page 1 of 1 | Close

2. To view only the failures in deployment, select the **Show Failures** check box.
3. Click **Close** to return to the Manage Images page.

- Related Documentation**
- [Deploying Device Images on page 238](#)
 - [Staging Device Images on page 234](#)

Deleting Device Images

You can delete device images from Junos Space including deleting multiple device images simultaneously.

To delete device images from the Junos Space:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Images**.
The Manage Images page appears.
2. Select the image that you want to delete.

The selected image is highlighted.

To select multiple device images, click the **Multiple** tab, and select the images you want to delete.

3. Right-click the selected device image or go to the Actions drawer.

4. Select **Delete Device Images**.

The Delete Device Image dialog box displays the image filename and the image version number.

5. Click **Delete** to confirm the deletion.

The selected image is deleted from Junos Space and no longer appears on the Manage Images page.

**Related
Documentation**

- [Device Images Overview on page 223](#)
- [Deploying Device Images on page 238](#)
- [Staging Device Images on page 234](#)

Modifying Device Image Details

Junos Space 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. From the navigation ribbon, select **Device Images and Scripts > Manage Images**.

The Manage Images page appears.

2. Select the image that you want to modify. The selected image is highlighted.

3. Right-click the selected device image and select **Modify Device Image Details**.

The Modify Device Image Details dialog box appears.

Figure 108: Modify Device Image Details

Modify Device Image Details

Image name: jinstall-ex-4200-9.6R3.8-domestic-signed.tgz

Version: 9.6R3.8

Series: EX4200

Platforms: EX4200-24T, EX4200-24P, EX4200-48T, EX4200-48P, EX4200-24F

Description:

Modify Cancel

4. To modify the series, use the Series list and specify the series that the selected device image supports. The platforms that are part of the selected series are automatically displayed in the Platforms box and cannot be modified.

To add or modify the description, you can use a maximum of 256 characters within the Description box.

5. Click **Modify**.

Your changes are saved. These changes can be viewed on the device image detail and summary view.

Related Documentation

- [Device Images Overview on page 223](#)
- [Deploying Device Images on page 238](#)
- [Deleting Device Images on page 243](#)

CHAPTER 21

Configuration: Scripts

- [Importing a Script on page 247](#)
- [Modifying a Script on page 248](#)
- [Modifying Script Types on page 249](#)
- [Comparing Script Versions on page 250](#)
- [Deleting Scripts on page 251](#)
- [Deploying Scripts on Devices on page 252](#)
- [Verifying the Checksum of Scripts on Devices on page 253](#)
- [Enabling Scripts on Devices on page 255](#)
- [Removing Scripts from Devices on page 256](#)
- [Executing Scripts on Devices on page 257](#)

Importing a Script

Using Junos Space you can import scripts into the Junos Space server. To import scripts you must first save them on the local file system of your workstation or client, ensure that they are of the .slax or .xsl format, and also ensure that they are commit, op, or event scripts. After importing scripts, you can perform various tasks on them such as viewing their contents, exporting them, modifying them, comparing them, verifying their checksum, viewing verification results, enabling and disabling them on devices, removing them from devices, executing them on devices, and deploying them on one or more devices simultaneously.

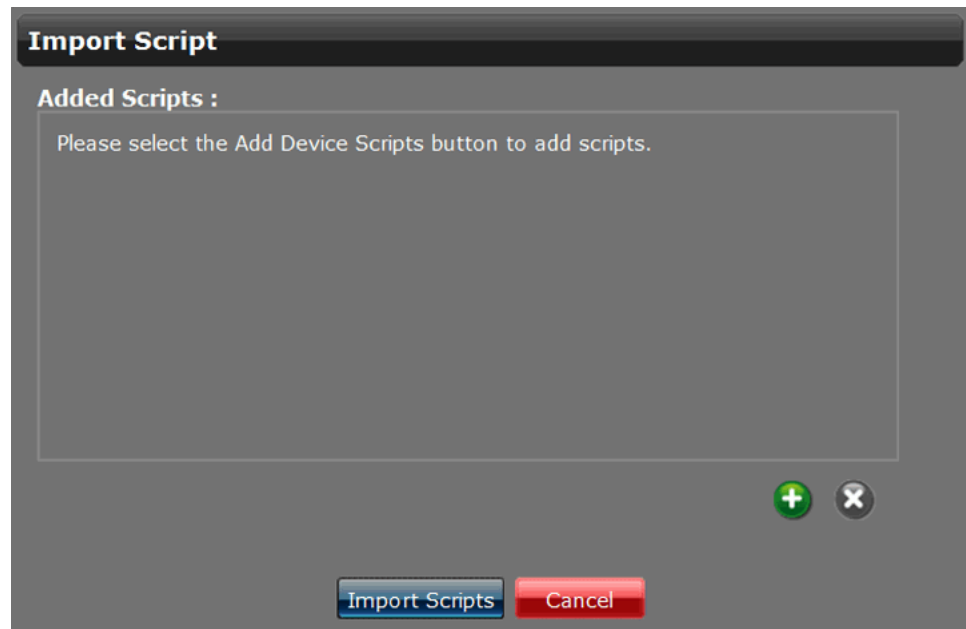
In earlier Junos OS releases, op scripts were run as event scripts by copying the op script to the `/var/db/scripts/event` folder and enabling it with event options and event policies. For subsequent releases, we recommend that you use dedicated event scripts in which the event options and policies specified in the script itself. In Junos Space, op scripts cannot be run as event scripts.

To import a script to Junos Space:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Scripts > Import Script**.

The **Import Script** dialog box appears as shown in [Figure 109 on page 248](#).

Figure 109: Import Scripts Dialog Box



2. Click **Browse**.

The **File Upload** dialog box displays the directories and folders on your local file system.

3. Locate the script that you want to upload , and click **Open**.
4. Click **Upload**.

The selected script is uploaded into Junos Space and displayed on the Manage Scripts page.

5. Click **Cancel** to return to the Manage Scripts page.

**Related
Documentation**

- [Viewing Script Details on page 275](#)

Modifying a Script

You can use Junos Space 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. To modify the script type for multiple scripts, see [“Modifying Script Types” on page 249](#).

To modify a script:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Scripts**.

The Manage Scripts page displays the scripts that you imported into Junos Space.

2. Select the script that you want to modify.
3. Right-click your selection or use the Actions drawer, and select **Modify**.

The **Modify Script** dialog box displays the details of the script, as shown in [Figure 110 on page 249](#).

Figure 110: Modify Script Dialog Box

Modify Script

Script name: add-node-bgp.slax

Type: Op Script

Version: 1.2

Script contents: /*
 * Script to add a node to the existing BGP mesh.
 * This script uses the remote-rpc mechanism available from 9.3 onwards.
 *
 * bgp-peer-group BGP peer group name
 * bgp-peer-type BGP peer type
 * local-address IP-address of local machine (This node)
 * local-as-number Local AS Number
 * peer-address IP-address of one of the peer
 */

Comments: Script is imported for the first time

Note: Changes made to the script contents will be saved as a new version.

Modify Cancel

4. You can modify the script type, script version, script contents, and the comments about the script.

5. Click **Modify**.

Your changes are saved to the latest version of the script, and the old version of the script is retained. To verify these changes, you can view the details of this script. See [“Viewing Script Details” on page 275](#).

Click **Cancel** to withdraw your changes and return to the Manage Scripts page.

Related Documentation • [Deploying Scripts on Devices on page 252](#)

Modifying Script Types

Using Junos Space, you can modify the script type of multiple scripts simultaneously.

To modify the script type:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Scripts**.

The Manage Scripts page displays the scripts that you imported into Junos Space.

2. Select the script whose script type you want to modify.

3. Right-click your selection or use the Actions drawer, and select **Modify Scripts Type**. The **Modify Scripts Type** dialog box displays the details of the script.
4. Use the Bulk Actions list to select a common script type for all scripts. To modify script types of individual scripts, click the **Script Type** column heading and use the drop-down menu to make your changes.
5. Click **Apply**.
Your changes are saved and the Manage Scripts page appears.
6. (Optional) To verify, double-click the script that you modified and view the script type.

**Related
Documentation**

- [Viewing Script Details on page 275](#)
- [Deploying Scripts on Devices on page 252](#)

Comparing Script Versions

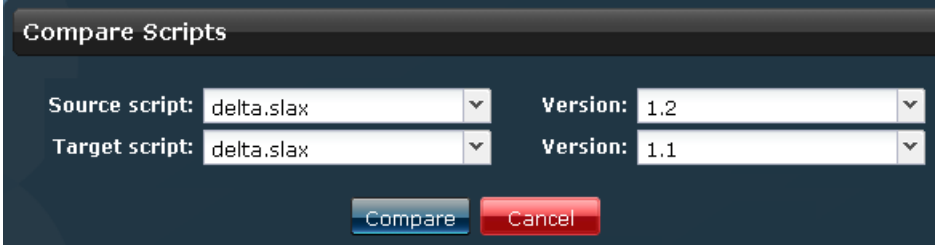
Using Junos Space you can compare two scripts and view their differences. This comparison can be done with two different scripts or between the same scripts of different versions.

To compare scripts:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Scripts**.
The Manage Scripts page displays the scripts that you imported into Junos Space.
2. Select the script that you want to compare.
3. Right-click your selection or use the Actions drawer, and select **Compare Script Versions**.

The **Compare Scripts** dialog box appears. [Figure 111 on page 250](#) is an example of the Compare Scripts dialog box where two same scripts of different versions are compared.

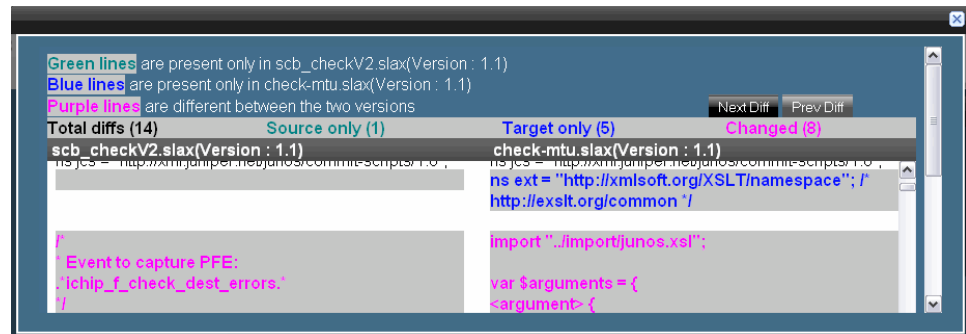
Figure 111: Compare Scripts Dialog Box



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 as shown in [Figure 112 on page 251](#). Use the **Next Diff** and **Prev Diff** buttons to navigate to the next change or the previous change, respectively.

Figure 112: Compare Scripts Window



The differences between the two scripts are represented using three different colors:

- Green— The green lines represent the changes that appear only in the source script.
- Blue— The blue lines represent the changes that appear only in the target script.
- Purple— The purple lines represent the changes that are different between the two scripts.

After the **Next Diff** and **Prev Diff** buttons, the total number of differences, the number of differences in the source script, the number of differences in the target script, and the number of changes are displayed.

7. Click **x** to close the window and return to the Manage Scripts page.

Related Documentation

- [Modifying a Script on page 248](#)
- [Deploying Scripts on Devices on page 252](#)
- [Scripts Overview on page 225](#)

Deleting Scripts

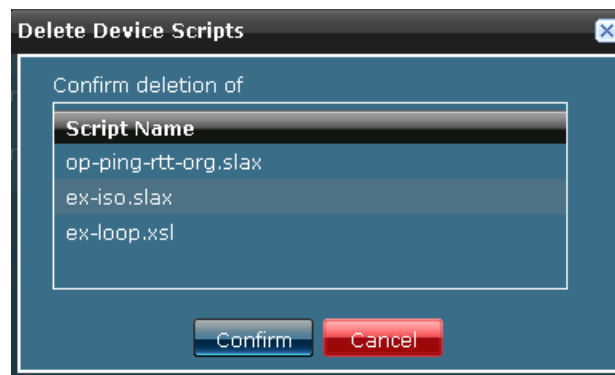
You can use Junos Space to delete the scripts that you import into the Junos Space server. When you delete a script, all versions of that script and the checksum verification results associated to that scrip are deleted.

To delete scripts:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Scripts**.
The Manage Scripts page displays the scripts that you imported into Junos Space.
2. Select the scripts that you want to delete.
3. Right-click your selection or use the Actions drawer, and click **Delete**.

The **Delete Device Scripts** dialog box lists the scripts that you chose for deletion.

Figure 113: Delete Device Scripts Dialog Box



4. Click **Confirm**.

The selected scripts are deleted and the **Jobs** dialog box displays a job ID link. You can click the link to view the status of the delete operation on the Manage Jobs page.

5. Click **Cancel** to return to the Manage Scripts page.

Related Documentation

- [Modifying a Script on page 248](#)

Deploying Scripts on Devices

You can use Junos Space to deploy scripts onto one or more devices. When you deploy a script, the latest version of the script file is transferred onto the device, and the MD5 checksum of the transferred file is checked against that of the script on Junos Space. If the result of the verification indicates that the script transferred onto the device is valid, then the script is enabled on the device. After you deploy scripts to devices, you can enable, disable, and execute them on those devices. You can remove the scripts from the device as well. Junos Space also enables you to schedule a time when you want the script to be deployed.

During script deployment, commit scripts are copied to the `/var/db/scripts/commit` directory on the device, op scripts are copied to the `/var/db/scripts/op` directory on the device, and event scripts are copied to the `/var/db/scripts/event` directory on the device. When you deploy scripts on dual Routing Engines, the scripts are copied to both Routing Engines, and in case of Virtual Chassis, the scripts are copied to all of the FPCs.



CAUTION: If the selected device already has a script with the same filename as the script that you have selected for deployment, then the deployed script overwrites the existing script.

To deploy a script:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Scripts**.

The Manage Scripts page displays the scripts that you imported into Junos Space.

2. Select one or more scripts that you want to deploy.

When you deploy a script, the latest version of the script is deployed onto the device.

3. Right-click your selection or use the Actions drawer, and click **Deploy Scripts on Devices**.

The **Deploy Scripts on Device(s)** dialog box displays the list of devices on which the script can be deployed, as shown in [Figure 114 on page 253](#).

Figure 114: Deploy Scripts On Device(s) Dialog Box

Deploy Scripts On Device(s)

Script name(s): op-ping-rtt-org.slax
ex-iso.slax

Select Devices

Host Name	IP Address	Platform	Serial Number	Software Version
<input checked="" type="checkbox"/> Sudhaker-M120	10.204.92.13	M120	JN108DEB7AEA	10.1R3.7
<input checked="" type="checkbox"/> 10.205.105.2	10.205.105.2	EX4200-48P	BQ0208473139	10.0R1.8

Page 1 of 1 | Displaying 1 - 2

☒ Schedule at a later time

Date and time: 07/21/10 12:02 AM IST

Deploy Cancel

4. Select the devices on which you want to deploy the script.
5. (Optional) To schedule a time for deployment, select the **Schedule at a later time** check box and specify the date and time when you want the script to be deployed.
6. Click **Deploy**.

The scripts are deployed on the selected devices, and the **Jobs** dialog box displays a job ID link. You can click the link to view the status of the deployment action on the Manage Jobs page.

7. Click **Cancel** to return to the Manage Scripts page.

Related Documentation

- [Verifying the Checksum of Scripts on Devices on page 253](#)
- [Operations Overview on page 229](#)

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 ensures that the transferred script is not corrupt. Junos

Space enables you to verify the checksum of multiple scripts that are deployed on the devices.

When you verify scripts that have multiple versions, the latest version of selected scripts are verified with the version of script that is available on the device. If the version of the script present on the device does not match the version that it is compared with, you will be notified by an error message.

To verify the checksum of a script:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Scripts**.

The Manage Scripts page displays the scripts that you imported into Junos Space.

2. Select the script whose checksum you want to verify.
3. Right-click your selection or use the Actions drawer, and select **Verify Checksum**.

The **Verify Checksum of Scripts on Device(s)** dialog box appears as shown in [Figure 115 on page 254](#).

Figure 115: Verify Checksum of Scripts on Device(s) Dialog Box

Host Name	IP Address	Platform	Serial Number	Software Version
Sudhaker-M120	10.204.92.13	M120	JN108DEB7AEA	10.1R3.7
10.205.105.2	10.205.105.2	EX4200-48P	BQ0208473139	10.0R1.8

4. Select the devices that have the script deployed on them.
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. You can click the link to view the status of the verification operation on the Manage Jobs page. To display the checksum verification results, see [“Viewing Verification Results” on page 277](#).

7. Click **Cancel** to return to the Manage Scripts page.

Related Documentation

- [Enabling Scripts on Devices on page 255](#)

Enabling Scripts on Devices

After you deploy scripts on devices, you can use Junos Space to enable these scripts on one or more devices simultaneously.

When you enable scripts that use Junos Space, 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. From the navigation ribbon, select **Device Images and Scripts > Manage Scripts**.
The Manage Scripts page displays the scripts that you imported into Junos Space.
2. Select one or more scripts that you want to enable on devices.
3. Right-click your selection or use the Actions drawer, and select **Enable Scripts on Devices**.

The Enable Scripts on Device(s) page appears.

Figure 116: Enable Scripts on Device(s) Dialog Box

Enable Scripts On Device(s)

Script name: ex-max-prefix.slax,

Select Devices

Host Name	IP Address	Platform	Serial Number	Software Version
<input type="checkbox"/> 10.204.92.13	10.204.92.13	M120	JN108DEB7AEA	10.2R1.8
<input type="checkbox"/> olive0	10.94.162.92	M120		10.2R1.8
<input type="checkbox"/> olive1	10.94.163.165	OLIVE		10.2R1.8

Page 1 of 1 | Displaying 1 - 3 of

☐ Schedule at a later time

Enable Cancel

4. Select the devices on which you want the script to be enabled.
5. 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 **Jobs** dialog box displays a link to the Job ID. You can click the link to view the status of this task on the Manage Jobs page.

Click **Cancel** to return to the Manage Scripts page.

Related Documentation

- [Executing Scripts on Devices on page 257](#)

Removing Scripts from Devices

You can use Junos Space to delete the scripts that you have transferred onto devices.



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. From the navigation ribbon, select **Device Images and Scripts > Manage Scripts**.
The Manage Scripts page displays the scripts that you imported into Junos Space.
2. Select the script that you want to remove from the device
3. Right-click your selection or use the Actions drawer, and select **Remove Scripts from Devices**.

The **Remove Scripts from Device(s)** dialog box lists the devices that the script is deployed on.

4. Select the devices from which you want the script to be removed.
5. Click **Remove**.

The script is removed from the selected devices, and a **Jobs** dialog box displays a job ID link. You can click the link to view the status of the script removal operation on the Manage Jobs page.

Click **Cancel** to return to the Manage Scripts page.

Related Documentation

- [Deploying Scripts on Devices on page 252](#)

Executing Scripts on Devices

You can use Junos Space to trigger the execution of op scripts on one or more devices simultaneously. Commit and event scripts are automatically activated after they are enabled. Commit scripts get triggered every time a commit is called on the device and event scripts are triggered every time an event occurs on the device or if a time is specified.



CAUTION: If the filename of the selected script matches that of any script present on the device, then the script on the device is executed regardless of its contents.

To execute an op-script on devices:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Scripts**.
The Manage Scripts page displays the scripts that you imported into Junos Space.
2. Select the op-script that you want to execute on a device.
3. Right-click your selection or use the Actions drawer, and select **Execute Script on Device(s)**.

The Execute Script on Device(s) page appears as shown in [Figure 117 on page 258](#).

Figure 117: Execute Script on Device(s) Dialog Box

Execute Script On Device(s)

Script name: setMacLimitBpduDrop.slax

Select Devices

Host Name	IP Address
10.204.92.13	10.204.92.13
olive0	10.94.162.92
olive1	10.94.163.165

Page 1 of 1 | Displaying 1 - 3 of

Parameters needed for script execution

Add Parameters Delete

Name	Value
Enter parameter name	Enter parameter value

☐ Schedule at a later time

Execute Cancel

4. Select the devices on which you want the script to be executed.
5. To specify the parameters for script execution, click **Add Parameters**, and specify the parameter name and value in the row that appears.
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 **Jobs** dialog box displays a link to the Job ID. You can click the link to view the status of this task on the Manage Jobs page.

Click **Cancel** to return to the Manage Scripts page.

Related Documentation

- [Enabling Scripts on Devices on page 255](#)

Configuration: Operations

- [Creating an Operation on page 259](#)
- [Modifying an Operation on page 262](#)
- [Running an Operation on page 263](#)
- [Copying an Operation on page 264](#)
- [Deleting an Operation on page 265](#)

Creating an Operation

In Junos Space, a device image is a software installation package that enables you to upgrade or downgrade from one Junos operating system (Junos OS) release to another. Scripts are configuration and diagnostic automation tools provided by Junos OS. Junos Space 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. From the navigation ribbon, select **Device Images and Scripts > Manage Operations > Create Operation**.

The Create Operations page appears.

2. Enter a name and description for the operation.
3. Click the Add (+) icon, and select **Script**, **Image**, or **Operation** from the list.

The **Select Scripts**, **Select Images**, or **Select Operations** dialog box appears depending on what you selected and displays all the Junos Space scripts, images, and operations, respectively, that you can include in the operation.

- To add a script, click the Add (+) icon, and select **Script** from the list. The **Select Scripts** dialog box appears.

Select the scripts and click **Add** to add your selections to the list.

You can edit the action that script should perform (**Stage** or **Execute**), and the **Set Return** parameters ([Figure 118 on page 260](#)).

Figure 118: Create Operation-Edit Script Dialog Box

Create Operation

Name: JUNOS 11.2 Upgrade MX

Description: Operation for upgrading JUNOS 11.2 software for MX devices

Name	Type	Action	Description
jun-op-show-ver-2-24-09.slax	Script		Script is imported for the first time
jun-op-show-chassis-res-2-24-09.slax	Script		Script is imported for the first time

Action: Stage

☒ Set Return Execute

☒ Success ☐ Failure

Set value:

Save Cancel

Create Cancel

- To add an image, click the Add (+) icon, and select **Image** from the list. The **Select Images** dialog box appears.

Select the images and click **Add** to add your selections to the list.

You can also edit the action that image should perform (**Stage** or **Deploy**), and various other deployment options ([Figure 119 on page 261](#)). See [“Deploying Device Images” on page 238](#) for more information.

Figure 119: Create Operation-Edit Image Dialog Box

Create Operation

Name: JUNOS 11.2 Upgrade MX
 Description: Operation for upgrading JUNOS 11.2 software for MX devices

Name	Type	Action	Description
jun-op-show-chassis-res-2-24-09.slax	Script		Script is imported for the first time
jinstall-11.2R2.4-domestic-signed.tgz	Image		MorMXorT

Action:

☒ Common Deployment Options

- ☐ Use image already downloaded to device
- ☐ Remove the package after successful installation
- ☐ Archive data (Snapshot)
- ☐ Delete any existing image before download

☒ Conventional Deployment Options

- ☐ Check compatibility with current configuration
- ☐ Reboot device after successful installation
- ☐ Load succeeds if at least one statement is valid
- ☐ Upgrade Backup Routing Engine only

☒ ISSU Deployment Options

- ☐ Upgrade the former Master with new image
- ☐ Save copies of the package files on the device
- ☐ Reboot the former Master after a successful

- To add an operation, click the Add (+) icon, and select **Operation** from the list. The **Select Operation** dialog box appears.

Select the operations and click **Add** to add your selections to the list.

Figure 120: Create Operation-Add Operation Dialog Box

Create Operation

Name: JUNOS 11.2 Upgrade MX
 Description: Operation for upgrading JUNOS 11.2 software for MX devices

Create/Edit Operation

Select Operations

Sorted by Creation Time

Operation Name	Description	Creation Time	Last Updated Time
op-1		Mon Nov 28 15:46:58 PST 2011	Mon Nov 28 15:46:58 PST 2011
op-2		Mon Nov 28 15:46:46 PST 2011	Mon Nov 28 15:46:46 PST 2011
op-1		Mon Nov 28 15:46:35 PST 2011	Mon Nov 28 15:46:35 PST 2011







Page 1 of 1 | Displaying 1 - 3 of 3 | Show 30 items



NOTE: You cannot edit a child operation.

- You can modify the list of selected scripts, images, and operations using the icons described in [Table 40](#) on page 262.

Table 40: Create Operation Dialog Box Icon Descriptions

Icon	Description
	Add scripts, image, and operations to the list.
	Delete the selected script, image, or operation from the list.
	Move the selected script, image, or operation to the row above.
	Move the selected script, image, or operation to the row below.
	Make a copy of the selected script, image, or operation, and include it in the operation.
	Edit the options for deploying or executing the scripts or images in the operation. For scripts, you can edit the action type, script parameters, and their values (success or failure). For images, you edit the image deployment options. See “Deploying Device Images” on page 238 for more information.
NOTE: You cannot edit a child operation	

- Click **Create** to create the operation and go the Manage 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 229](#)
 - [Modifying an Operation on page 262](#)
 - [Running an Operation on page 263](#)
 - [Copying an Operation on page 264](#)
 - [Viewing Operations Results on page 279](#)
 - [Deleting an Operation on page 265](#)

Modifying an Operation

Junos Space allows you to edit the parameters of an operation.

To modify an operation:

- From the navigation ribbon, select **Device Images and Scripts > Manage Operations**.
The Manage Operations page displays all the operations in the Junos Space database.
- Select the operation that you want to modify.
- Right-click your selection or use the Actions drawer, and select **Modify Operation**.

4. Modify the necessary parameters. See [“Creating an Operation” on page 259](#) for more information.

5. Click **Modify** to save your changes and go to the Manage Operations page.

To verify whether your changes are saved, double-click the operation and view its details.

**Related
Documentation**

- [Operations Overview on page 229](#)
- [Creating an Operation on page 259](#)
- [Running an Operation on page 263](#)
- [Copying an Operation on page 264](#)
- [Viewing Operations Results on page 279](#)
- [Deleting an Operation on page 265](#)

Running an Operation

Junos Space allows you to execute (or run) operations existing in the Junos Space database on devices.

To run an operation:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Operations**.
The Manage Operations page displays all the operations in the Junos Space database.
2. Select the operation that you want to execute.
3. Right-click your selection or use the Actions drawer, and select **Run Operation**.

The Run Operation page appears.

Figure 121: Run Operation Page

Operation Name: JUNOS 11.2 Upgrade MX

Select Devices

Host Name	IP Address	Platform	Serial Number	Software Version
sfo-re0	10.155.69.13	MX960 (Dual RE)	JN1118EBEAF	11.2R3.3

Page 1 of 1 | Displaying 1 - 1 of 1 | Show 30 items

Tag Selected Devices As [Apply Tag](#)

☒ Schedule at a later time

Date and time: 11/28/11 4:47 PM PST

[OK](#) [Cancel](#)

4. Select the devices on which you want to execute the operation.

You can search for specific devices by entering the name of the device in the Find Devices search box.

5. You can also specify a tag for the selected devices so that you can reuse the same group of devices to run a different operation.

6. Click **OK** to run your operation immediately.

You can also schedule a time for the operation to run by selecting the **Schedule at a later time** check box, specifying the date and time when you want to run the operation, and then clicking **Execute**.

Related Documentation

- [Operations Overview on page 229](#)
- [Creating an Operation on page 259](#)
- [Modifying an Operation on page 262](#)
- [Copying an Operation on page 264](#)
- [Viewing Operations Results on page 279](#)
- [Deleting an Operation on page 265](#)

Copying an Operation

You can use Junos Space to create copies of operations existing in the Junos Space database.

To create a copy of an operation:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Operations**.
The **Manage Operations** page displays the operations in Junos Space.
2. Select the operations that you want to copy.
3. Right-click your selection or use the Actions drawer, and click **Copy**.
The **Copy Operation** dialog box appears, prompting you to enter a new name for the operation.
4. Enter a new name for the operation in the **Destination Name** box.
5. Click **Copy** to create a copy of the operation and go back to the Manage Operations page.

Related Documentation

- [Operations Overview on page 229](#)
- [Creating an Operation on page 259](#)
- [Modifying an Operation on page 262](#)
- [Running an Operation on page 263](#)
- [Deleting an Operation on page 265](#)
- [Viewing Operations Results on page 279](#)

Deleting an Operation

You can use Junos Space to delete operations from the Junos Space database.

To delete an operation:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Operations**.
The Manage Operations page displays the operations in Junos Space.
2. Select the operations that you want to delete.
3. Right-click your selection or use the Actions drawer, and click **Delete Operation**.
The **Delete Operations** dialog box lists the operations that you chose for deletion.
4. Click **Confirm** to delete the operation.

The selected operations are deleted and the **Jobs** dialog box displays a job ID link. You can click the link to view the status of the delete operation on the Manage Jobs page.



NOTE: When you delete an operation, you do not delete the scripts, images or operations associated with it.

**Related
Documentation**

- [Operations Overview on page 229](#)
- [Creating an Operation on page 259](#)
- [Modifying an Operation on page 262](#)
- [Running an Operation on page 263](#)
- [Copying an Operation on page 264](#)
- [Viewing Operations Results on page 279](#)

Configuration: Script Bundles

- [Creating a Script Bundle on page 267](#)
- [Modifying a Script Bundle on page 268](#)
- [Deleting Script Bundles on page 270](#)
- [Deploying Script Bundles on Devices on page 270](#)
- [Executing Script Bundles on Devices on page 271](#)

Creating a Script Bundle

Junos Space 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 (see [“Importing a Script” on page 247](#)).

To create a script bundle:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Script bundles > Create Script Bundle**.

The Create Script Bundle page appears as shown in [Figure 122 on page 267](#).

Figure 122: Create Script Bundle page







Script Name	Script Parameters	Rule
-------------	-------------------	------

2. Enter a name and description for the script bundle.
3. Click the Add Scripts (+) icon to add scripts that need to be included into the script bundle.

The Select Scripts page displays all Junos Space scripts that you can include into the script bundle.

4. Select the scripts that you want to include in the script bundle.
The selected scripts are highlighted.
5. Click **Add**.
The selected scripts are included in the **Selected Scripts** section of the **Create Script Bundle** dialog box. You can modify the list of selected scripts using the icons described in [Table 41 on page 268](#).

Table 41: Create Script Bundle Dialog Box Icon Descriptions

Icon	Description
	Add scripts to the script bundle.
	Delete the selected script from the script bundle.
	Move the selected script to the row above.
	Move the selected script to the row below.
	Make a copy of the selected script and include it in the script bundle.
	Edit the value (success or failure) of script parameters. This option is disabled when commit scripts are selected.

6. Click **Submit**.
The script bundle is created and displayed on the Manage Script Bundles page.
7. To verify whether the script bundle is created with your specifications, double-click the script bundle and view its details.

- Related Documentation**
- [Deploying Script Bundles on Devices on page 270](#)
 - [Modifying a Script Bundle on page 268](#)
 - [Scripts Overview on page 225](#)

Modifying a Script Bundle

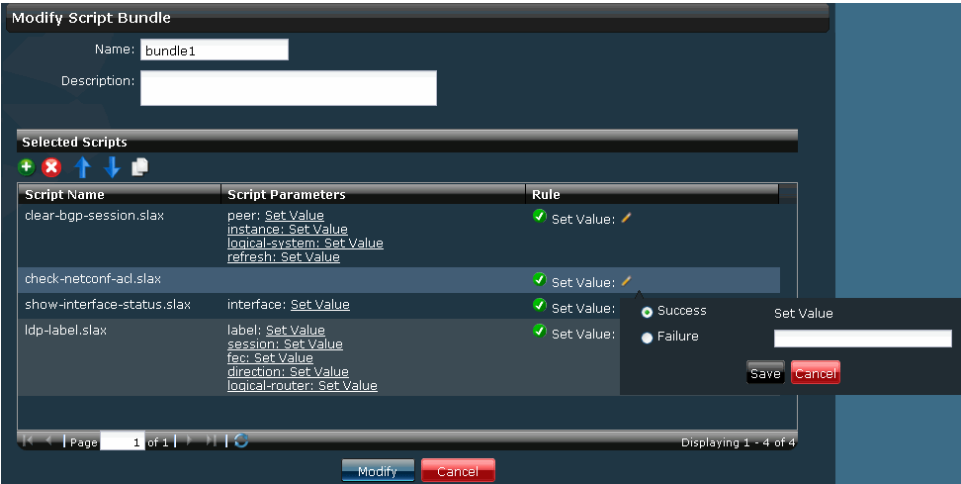
Junos Space allows you to modify a script bundle name, description, number of scripts included in the script bundle, and script parameter value (success or failure) of every script included in the script bundle.

To modify script bundles:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Script bundles**.

The Manage Script Bundles page displays all Junos Space script bundles.
2. Select the script bundle that you want to modify.
3. Right-click your selection or use the Actions drawer, and select **Modify Script Bundle**.
The **Modify Script Bundle** dialog box appears as shown in [Figure 123 on page 269](#).

Figure 123: Modify Script Bundle page



4. Make your changes to the name, description, number of scripts included in the script bundle, and value (success or failure) of every script included in the script bundle. To modify the scripts use the icons described in [Table 42 on page 269](#).

Table 42: 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. This option is disabled when commit scripts are selected.

5. Click **Modify**.
Your modifications are saved and the Manage Script Bundles page appears.
6. To verify whether your changes are saved, double-click the script bundle and view its details.

**Related
Documentation**

- [Deploying Script Bundles on Devices on page 270](#)
- [Executing Script Bundles on Devices on page 271](#)
- [Scripts Overview on page 225](#)

Deleting Script Bundles

Junos Space enables you to delete multiple script bundles.

To delete script bundles:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Script bundles**.

The Manage Script Bundles page displays all Junos Space script bundles.
2. Select the script bundles that you want to delete.
3. Right-click your selection or use the Actions drawer, and select **Delete Script Bundles**.
The **Delete Script Bundles** dialog box displays the names of the selected script bundles.
4. Click **Delete** to confirm.
The selected script bundles are deleted and the Manage Script Bundles page appears.
5. To verify whether the script bundles are deleted, view the list of scripts in the Manage Script Bundles page.

**Related
Documentation**

- [Creating a Script Bundle on page 267](#)
- [Executing Script Bundles on Devices on page 271](#)
- [Scripts Overview on page 225](#)

Deploying Script Bundles on Devices

Junos Space allows you to deploy 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 deploy script bundles on dual Routing Engines, the script bundles are copied to both Routing Engines, and in case of Virtual Chassis, the script bundles are copied to all of the FPCs.

To deploy script bundles on devices:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Script bundles**.
The Manage Script Bundles page displays all Junos Space script bundles.
2. Select the script bundles that you want to deploy on devices.
3. Right-click your selection or use the Actions drawer, and select **Deploy Script Bundles**.
The **Deploy Script Bundle On Device(s)** dialog box appears as shown in [Figure 124 on page 271](#).

Figure 124: Deploy Script Bundle On Device(s) Dialog Box

Deploy Script Bundle On Device(s)

Bundle Name: bundle1

Select Devices

Host Name	IP Address	Platform	Serial Number	Software Version
jotter	10.204.92.13	M120	JN108DEB7AEA	11.2B3
SN-MX80	10.205.50.196	MX80-48T	E4008	11.1R1.14
ex-2200-50-185	10.205.50.185	EX2200-24T-4G	CW0210403326	11.2B2.1
srx3600_50_76	10.205.50.76	SRX3600	AB3510AA0021	11.2B3.2
SN_SRX210H_1	10.205.50.186	SRX210H	AD4310AA0472	10.4R1.9

Page 1 of 1

Displaying 1 - 21 of 21

☒ Schedule at a later time

Date and time: 05/25/11 4:11 AM IST

Deploy Cancel

4. Select the devices on which you want to deploy the script bundles.
5. 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.
6. Click **Deploy**.
The selected scripts are deployed and a **Jobs** dialog box displays a job id link, which you can click to view the status of the script bundle deployment.
7. Click **OK**.
The script bundles are deployed on the selected devices and the Manage Script Bundles page appears.

Related Documentation

- [Modifying a Script Bundle on page 268](#)
- [Executing Script Bundles on Devices on page 271](#)
- [Scripts Overview on page 225](#)

Executing Script Bundles on Devices

Junos Space allows you to execute script bundles on devices. When you execute script bundles, Junos Space 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.

To execute script bundles on devices:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Script bundles**.

The Manage Script Bundles page displays all Junos Space script bundles.

2. Select the script bundles that you want to execute on devices.
3. Right-click your selection or use the Actions drawer, and select **Execute Script Bundles on devices**.

The **Execute Script Bundle On Devices(s)** dialog box appears as shown in [Figure 125 on page 272](#).

Figure 125: Execute Script Bundle On Devices(s) Dialog Box

Execute Script Bundle On Device(s)

Bundle Name: bundle1

Select Devices

Host Name	IP Address
jotter	10.204.92.13
<input checked="" type="checkbox"/> nms3-f	10.204.92.69
<input checked="" type="checkbox"/> puram	10.204.92.86
<input checked="" type="checkbox"/> access-sw-2	10.205.50.115
<input checked="" type="checkbox"/> 10.205.50.119	10.205.50.119
<input checked="" type="checkbox"/> sr3600_50_75	10.205.50.75

Page 1 of 1 | Displaying 1 - 21 of 21

☒ Deploy & Enable Scripts before Execution

[Update Script Parameters/Rule](#)

☐ Schedule at a later time

Execute Cancel

4. Select the devices on which you want to execute the selected scripts.
5. To redeploy the scripts before execution, select the **Deploy & Enable Scripts before Execution** check box.
6. 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 continues to reflect the original values.

To edit the script parameter values before execution:

1. Click the **Update Script Parameters/Rule** link. The **Configure Script Bundle Parameters** dialog box appears.
2. Use the Edit icon to set the script parameter value to Success or Failure, and click **Save**.
3. Click **Configure**. Your changes are saved and the **Enable Script Bundle On Devices(s)** dialog box displays your previous selections.
7. 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.

8. Click **Enable**.

The script bundle is enabled on the selected devices and a **Jobs** dialog box displays a job id link, which you can click to view the status of script bundle execution.

9. Click **OK**.

The script bundles are executed on the selected devices and the Manage Script Bundles page appears.

**Related
Documentation**

- [Modifying a Script Bundle on page 268](#)
- [Deploying Script Bundles on Devices on page 270](#)
- [Scripts Overview on page 225](#)

Administration: Scripts

- [Viewing Script Details on page 275](#)
- [Viewing Verification Results on page 277](#)
- [Exporting Scripts in Tar Format on page 278](#)

Viewing Script Details

Using Junos Space, 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. From the navigation ribbon, select **Device Images and Scripts > Manage Scripts**.

The Manage Scripts page displays the scripts that you imported into Junos Space.

2. Double click the script whose details you want to view.

The **View Script Details** dialog box displays the script name, type, format, creation time, version, comments and the contents of the script as shown in

[Figure 126 on page 276](#).

Figure 126: Script Details Dialog Box



Table 43 on page 276 describes the fields displayed in the Script Details dialog box.

Table 43: Script Details Dialog Box Fields

Control	Description
Name	Name of the script file.
Type	Type of script. The values are: <ul style="list-style-type: none"> • Commit script • Op script • Event script
Format	Format of the script file. The values are: <ul style="list-style-type: none"> • XSL • SLAX
Creation Time	Date and time when the script was created.

Table 43: Script Details Dialog Box Fields (*continued*)

Control	Description
Version	The version number of the script. When you modify a script, the changes are saved in the latest version of the script.
Script Contents	The contents of the script.
Comments	Text that describes the script that is entered by the user.

Related Documentation

- [Exporting Scripts in Tar Format on page 278](#)

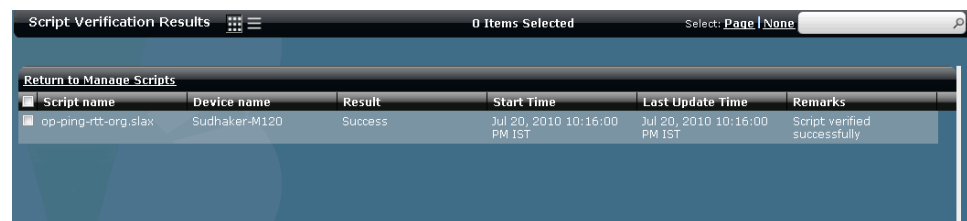
Viewing Verification Results

You can use Junos Space to view the results of the checksum verification task. When a verification failure occurs, the results indicate the reason for failure. When you delete a script, the checksum verification results associated to that scrip are also deleted.

To view the verification results:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Scripts**.
The Manage Scripts page displays the scripts that you imported into Junos Space.
2. Select the script whose verification result you want to view.
3. Right-click your selection or use the Actions drawer, and select **View Verification Results**.

Figure 127: Script Verification Results Dialog Box



The **Script Verification Results** page displays the results of the checksum verification, as shown in [Figure 127 on page 277](#).

[Table 44 on page 277](#) describes the fields on the Script Verification Results page.

Table 44: 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.

Table 44: Script Verification Results Page Fields (*continued*)

Field Name	Description
Result	Result of the verification. The values are: <ul style="list-style-type: none"> • Success • Failed
Start Time	Time when the verification was initiated.
Last Update Time	Latest time when the verification was updated.
Remarks	Errors encountered during the verification. This field is blank when the verification is successful.

4. Click the **Return to Manage Scripts** link to return to the Manage Scripts page.

Related Documentation • [Executing Scripts on Devices on page 257](#)

Exporting Scripts in Tar Format

You can use Junos Space to export the contents of multiple scripts and save them on your local file system.

To export the contents of scripts:

1. From the navigation ribbon, select **Device Images and Scripts > Manage Scripts**.
The Manage Scripts page displays the scripts that you imported into Junos Space.
2. Select the scripts that you want to export.
3. Right-click your selection or use the Actions drawer, and select **Export Scripts**.
The **Export Scripts** dialog box asks you for a confirmation.
4. Click **Export**.
The **File Open** dialog box enables you to save the script files in the tar format and the **Export Scripts Job Status** dialog box displays the status of this task graphically. To view the status of your job in the Job Manager, click the bar of the graph. You can also save the tar files by clicking the **Download** link.
5. Click **OK** and save the files on your local file system.
6. Unzip the files to view the contents of the script.

Related Documentation • [Scripts Overview on page 225](#)

Administration: Operations

- [Viewing Operations Results on page 279](#)

Viewing Operations Results

Using Junos Space, 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. From the navigation ribbon, select **Device Images and Scripts > Manage Operations > View Operation Results**.

The View Operation Results page appears ([Figure 128 on page 280](#)). The information appears according to the following parameters:

- Operation name
- Date of execution
- Summary of the result (such as the number of devices on which the operation was successfully executed)
- Execution status (scheduled, in progress, success, or failed)
- Job ID

Figure 128: View Operation Results Page

Device	Object	Object Type	Action	Result
JUNOS-11-2-Upgrade-Mix	junos-osp-11-2-Upgrade-Mix	Script	execute	SUCCESS
JUNOS-11-2-Upgrade-Mix	junos-osp-11-2-Upgrade-Mix-2-24-09-01	Script	execute	SUCCESS
JUNOS-11-2-Upgrade-Mix	junos-osp-11-2-Upgrade-Mix-2-24-09-01-01	Image	stage	INFO/ERROR
JUNOS-11-2-Upgrade-Mix	junos-osp-11-2-Upgrade-Mix-2-24-09-01-01-01	Script	execute	NA

2. Double-click an operation to open the **Operation Result Detail** dialog box, which displays information about the selected operation according to device name and result (success or failed), along with a summary of the operation. Child operations are automatically expanded in the Operation Result Detail of a device. The detail is a flattened list of script or image entries.

You can expand an individual row to view more information about the scripts, images, and child operations (operations within an operation) associated with that device. You can also expand the rows of child operations to see information about all the scripts and images associated with the operation. This way, you are able to monitor the status of each script or image associated with an operation and identify the causes of failed executions (if any).

3. Click **Close** to go back to the View Operation Results page.

Related Documentation

- [Operations Overview on page 229](#)
- [Creating an Operation on page 259](#)
- [Modifying an Operation on page 262](#)
- [Running an Operation on page 263](#)
- [Copying an Operation on page 264](#)
- [Deleting an Operation on page 265](#)

PART 5

Network Monitoring

- [Network Monitoring UI on page 283](#)

CHAPTER 26

Network Monitoring UI

- [Network Monitoring Workspace on page 283](#)

Network Monitoring Workspace

- [Network Monitoring Workspace Overview on page 284](#)
- [Network Monitoring Reports Overview on page 286](#)
- [Viewing the Node List on page 287](#)
- [Resyncing Nodes on page 288](#)
- [Searching in the Network Monitoring Workspace on page 288](#)
- [Tracking and Searching for Assets on page 289](#)
- [Viewing and Tracking Outages on page 290](#)
- [Viewing, Querying, and Acknowledging Events on page 291](#)
- [Viewing and Acknowledging Alarms on page 294](#)
- [Viewing, Configuring, and Searching for Notifications on page 297](#)
- [Creating Reports on page 299](#)
- [Viewing Reports on page 300](#)
- [Deleting Reports on page 304](#)
- [Viewing Charts on page 305](#)
- [Admin: Configuring Network Monitoring on page 305](#)
- [Configuring SNMP Community Names by IP on page 311](#)
- [Configuring SNMP Data Collection per Interface on page 312](#)
- [Managing and Unmanaging Interfaces and Services on page 313](#)
- [Managing Thresholds on page 313](#)
- [Configuring Notifications on page 317](#)
- [Configuring Scheduled Outages on page 321](#)

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.

Junos Space Network Application Platform has integrated a third-party tool for this purpose, OpenNMS, which is a network management application platform that provides solutions for enterprises and carriers.

OpenNMS is installed as part of Platform, which exposes some of the OpenNMS functionality through the Network Monitoring workspace.



CAUTION: Although additional OpenNMS 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 analyze and aggregate device-level performance data, and to detect device faults, the Network Monitoring workspace uses a collection of data from managed elements. Performance data is collected automatically if the SNMP settings are set properly for a discovered device.

- *Collection*
 - View historical performance data by using a graphical monitoring tool that allows customization of the parameters to be displayed and the devices to be monitored
 - Create graphs and charts
 - Create and export reports in PDF and HTML formats
 - Define advanced variables that require calculations for historical performance monitoring
 - Allow raw data to be rolled up into processed data, allowing data to be processed from a more-specific to a less-specific level (for example, data collected at a quarter hourly interval can be rolled into hourly data, hourly data can be rolled into daily data, daily can be rolled into weekly data, and weekly data can be rolled into yearly data)
- *Thresholds*
 - Set thresholds for performance data values—including specifying warning and error levels
 - Create threshold graphs
 - Generate threshold-crossing alarms that can be displayed or forwarded
- *Faults*

- Receive SNMP traps directly from devices and other enterprise management systems (EMSs)
- Forward traps to other EMSs
- Generate and display events and alarms
- Get basic correlation with alarms; for example, clearing alarms, deduplicating alarms
- Detect device faults based on data collected from devices

You can perform the following tasks from the Network Monitoring workspace:

- Node List: List all the devices under monitoring (see [“Viewing the Node List” on page 287](#))
- Search: Search for devices (see [“Searching in the Network Monitoring Workspace” on page 288](#))
- Outages: View unavailable (down) services (see [“Viewing and Tracking Outages” on page 290](#))
- Events: View events (see [“Viewing, Querying, and Acknowledging Events” on page 291](#))
- Alarms: View alarms (see [“Viewing and Acknowledging Alarms” on page 294](#))
- Notifications: Display notices received by users (see [“Viewing, Configuring, and Searching for Notifications” on page 297](#))
- Assets: Search asset information and assets inventory (see [“Tracking and Searching for Assets” on page 289](#))
- Reports: View reports (see *Working With Reports*)
- Charts: View charts (see [“Viewing Charts” on page 305](#))
- Admin: Perform system administration (see [“Admin: Configuring Network Monitoring” on page 305](#))

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.

Related Documentation

- [Network Monitoring Reports Overview on page 286](#)

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 286](#)
- [Key SNMP Customized \(KSC\) Performance Reports, Node Reports, and Domain Reports on page 286](#)
- [Database Reports on page 286](#)
- [Statistics Reports on page 286](#)

Resource Graphs

Resource graphs provide an easy way to represent visually the data collected from managed nodes throughout your network. You can display critical SNMP performance, response time, and so forth.

You can narrow your selection of resources by entering a search string in the Name contains box. This invokes a case-insensitive substring match on resource names.

Key SNMP Customized (KSC) Performance Reports, Node Reports, and Domain Reports

KSC reports enable you to create and view SNMP performance data using prefabricated graph types. The reports provide a great deal of flexibility in time spans and graph types. You can save KSC report configurations so that you can refer to key reports in the future.

Node reports show SNMP data for all SNMP interfaces on a node.

Domain reports show SNMP data for all SNMP interfaces in a domain. You can load node reports and domain reports into the customizer and save them as a KSC report.

You can narrow your selection of resources by entering a search string in the Name contains box. This invokes a case-insensitive substring match on resource names.

Database Reports

Database reports provide a graphical or numeric view of your service-level metrics for the current month-to-date, previous month, and last 12 months by categories.

Statistics Reports

Statistics reports provide regularly scheduled statistical reports on collected numerical data (response time, SNMP performance data, and so forth).

Related Documentation

- [Network Monitoring Workspace Overview on page 284](#)
- [Creating Reports on page 299](#)
- [Deleting Reports on page 304](#)
- [Viewing Reports on page 300](#)

- [Viewing the Node List on page 287](#)
- [Viewing Managed Devices on page 63](#)
- [Resyncing Nodes on page 288](#)
- [Searching in the Network Monitoring Workspace on page 288](#)

Viewing the Node List

Junos Space is monitored by default using the built-in SNMP manager, OpenNMS. The Junos Space node is listed in the OpenNMS node list, and referred to hereafter as the Junos Space 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 288](#)).

The Node List page displays a list of all the nodes in your network. You can also display the interfaces for each node. The top level of the Node List displays only the hostname of each device. Click the hostname of the desired device to see:

- SNMP Attributes
- Availability
- Node Interfaces—IP Interfaces, Physical Interfaces (where applicable)
- General (status and detailed information)
- Surveillance Category Memberships
- Notification
- Recent Events
- Recent Outages

Each of these items has links enabling you to drill deeper into the corresponding aspect of the node's performance.

For each node, you can also view events, alarms, outages, asset information, rescan, access the admin options for it, and schedule outages for it.

Related Documentation

- [Network Monitoring Workspace Overview on page 284](#)
- [Viewing Managed Devices on page 63](#)
- [Resyncing Nodes on page 288](#)
- [Viewing and Acknowledging Alarms on page 294](#)
- [Viewing, Configuring, and Searching for Notifications on page 297](#)
- [Tracking and Searching for Assets on page 289](#)

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 63](#)).

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 284](#)
 - [Viewing the Node List on page 287](#)
 - [Viewing Managed Devices on page 63](#)

Searching in the Network Monitoring Workspace

To search for nodes or asset information, use the Search task in the Network Monitoring workspace—select **Network Monitoring > Search**. The Search page has two sections, Search for Nodes and Search Asset Information.

To quickly search for nodes:

- To display the entire node list, click **All nodes** in the Search for Nodes section.
- To display a list of all nodes and their interfaces, click **All nodes and their interfaces** in the Search for Nodes section.
- To display a list of all nodes that have asset information assigned, click **All nodes with asset info** in the Search Asset Information section. The asset information fields are very comprehensive, ranging from address to circuit ID to date installed, to lease expiry date to number of power supplies installed.

You can search for nodes using these criteria:

- **Name containing**—Searching by name is case-insensitive and inclusive. For example, searching on serv would find serv, Service, Reserved, NTSERV, or UserVortex.
 - The *underscore* character (`_`) acts as a single-character wildcard.

- The *percent* character (%) acts as a multiple-character wildcard.
- **TCP/IP address**—Allows you to separate the four octets (fields) of a TCP/IP address into separate searches.
 - A single *asterisk* (*) acts as a wildcard for an octet.
 - Ranges are indicated by two numbers separated by a *dash* (-)
 - *Commas* (,) are used for list demarcation.

For example, the following searches are all valid and would each create the same result set---all TCP/IP addresses from 192.168.0.0 through 192.168.255.255:

- 192.168.**
- 192.168.0-255.0-255
- 192.168.0,1,2,3-255.*
- **ifAlias, ifName, or ifDescr contains**—Finds nodes with interfaces that match the given search string. This is a case-insensitive inclusive search similar to the **Name containing** search. To find an exact match, select **equals** instead of **contains**.
- **Providing service**—Finds nodes providing a particular service. To search for a node providing a particular service, select the service from the Providing service list.
- **MAC Address like**—To find interfaces with hardware (MAC) addresses matching the search string, use this case-insensitive partial string match. For example, you can find all interfaces with a specified manufacturer's code by entering the first 6 characters of the MAC address. Octet separators (dash or colon) are optional.
- **Foreign Source like**—To find a node with a foreign source IDs, use this partial string match.

To quickly search for all nodes with asset information assigned, click **All nodes with asset info**.

You can search for assets using these criteria:

- **Category**—Find assets associated with a particular category.
- **Field**—Search for a specific asset field.
- **Containing text**—Find assets containing the search string. This is a case-insensitive inclusive search similar to the **Name containing** search.

Related Documentation

- [Network Monitoring Workspace Overview on page 284](#)
- [Viewing the Node List on page 287](#)
- [Viewing Managed Devices on page 63](#)

Tracking and Searching for Assets

The OpenNMS 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 OpenNMS 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 OpenNMS system:

- Import the data from another source.
- Enter the data manually.

Once you begin adding data to the OpenNMS system's assets inventory page, any node with an asset number (for example, bar code) is displayed on the lower half of this page, providing you with a one-click mechanism for tracking the current physical status of that device.

If you want to search for particular assets by category, simply select the desired category in the Assets in category list and click **Search** to retrieve a list of all assets associated with that category.

For a complete list of nodes, whether or not they have associated asset numbers, click **All nodes with asset info** link.

Related Documentation

- [Network Monitoring Workspace Overview on page 284](#)
- [Viewing the Node List on page 287](#)
- [Viewing Managed Devices on page 63](#)
- [Resyncing Nodes on page 288](#)
- [Searching in the Network Monitoring Workspace on page 288](#)

Viewing and Tracking Outages

To track outages, discovered services are polled. If a service does not respond, a service outage is created, which in turn creates notifications.

To view and track outages, select **Network Monitoring > Outages**.

To get details for a particular outage, enter its ID in the Outage ID box and click **Get details**.

Alternatively, to view all outages still extant, click **Current outages**. To view both current and resolved outages, click **All outages**.

To view other outage types from these Outages pages, change the display by selecting from the Outage type list. You can sort on each of these column headings by clicking them:

- ID
- Node
- Interface
- Service

- Down
- Up

You can also return to the results by clicking **Bookmark Results**. Your browser's favorite or bookmark dialog box opens.

Related Documentation

- [Network Monitoring Workspace Overview on page 284](#)
- [Viewing the Node List on page 287](#)
- [Viewing Managed Devices on page 63](#)
- [Resyncing Nodes on page 288](#)

Viewing, Querying, and Acknowledging Events

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

Events signal network or systems-related issues. Acknowledging an event enables you to take responsibility for resolving the problem that triggered it. All events are visible to all users. By default, the Events page displays outstanding, or unacknowledged, events.

The Events task contains the functions described below.

The breadcrumbs at the top of each of these pages contain links taking you back to previous pages. Listings frequently extend over multiple pages, between which you can navigate using the **First**, **Previous**, and **Next** links at the top and bottom left of the pages. On the bottom left of the pages is the number of events on the page, and the number of results on the current page out of the total list.

You can sort on each of the column headings on list pages. You can also return to the results by clicking **Bookmark Results**. Your browser's favorite or bookmark dialog box opens.

- [Events Landing Page on page 291](#)
- [Advanced Event Search on page 292](#)
- [Viewing the Events List on page 292](#)
- [Viewing Event Details on page 293](#)

Events Landing Page

To search for, view, query, and 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 292](#).
- 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 293](#).

- To perform an advanced search, click **Advanced Search** to go to the Advanced Event Search section. The Advanced Event Search section can be used to search the event list on multiple fields. See [“Advanced Event Search” on page 292](#).

Advanced Event Search

Enter values into any of the following fields to narrow down the search:

- Event Text Contains
- Node Label Contains
- TCP/IP Address Like
- Severity

For a service, select from the Service list.

To select events by time, first select the box for the time range that you want to limit.

To select events in a time period, select both boxes and then select the beginning and end of the range time from the lists.

You can determine the order in which found events are displayed by selecting from the Sort By list.

Determine the quantity of events displayed by selecting from the Number of Events Per Page list.

Viewing the Events List

Select **Network Monitoring > Events** and click **All events** in the Event Queries section to display a list of events. By default, the Events page displays outstanding events.

- To see all events, click **View all events** at the top of the page. Clicking Advanced Search takes you to the Advanced Event Search section (see [“Advanced Event Search” on page 292](#)).
- 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**—Acknowledged 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 293](#)).
- **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 288](#)). 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 288](#)). You can choose to view only events on the same interface as the selected event, or view all events except those on that interface.
- **Service**—The name of the service affected, where applicable.
- **UEI**—[Unique Event Identifier] You can choose to view only events with the same UEI or all events except those with the same UEI. You can also edit notifications for the event by clicking on the link of that name, which takes you to the Build the rule section for notifications (see [“Configuring Notifications” on page 317](#)).
- **Log message**—The log message.

Viewing Event Details

Select **Network Monitoring > Events**, enter its ID in the Event ID field and click **Get details**. The Event *event ID* section displays the following items:

- **Severity**—Severity of event. Degrees of severity are color-coded and labeled:
 - **CRITICAL**: Numerous devices are affected; fixing the problem is essential.
 - **MAJOR**: Device is completely down or in danger of going down. Immediate attention required.
 - **MINOR**: Part of a device (service, interface, power supply, and so forth) has stopped. Attention required.
 - **WARNING**: Might require action. Should possibly be logged.
 - **INDETERMINATE**: No severity could be associated.
 - **NORMAL**: Informational message. No action required.
 - **CLEARED**: Indicates that a prior error condition has been corrected and service is restored.
- **Time**—Time when event occurred.
- **Node and Interface**—Both of these values are clickable, targeting the Nodes section and the Nodes and their interfaces section respectively on the Search page.
- **Acknowledged By and Time Acknowledged**—Acknowledger of event and the time of acknowledgement.
- **Service**—Service affected, where applicable.
- **UEI**—Unique Event Identifier. UEIs enable disk usage to be handled differently from other events with high-threshold types, which means you can choose to be notified by

e-mail of high disk usage only, instead of getting notified of all events of the threshold type high.

- Log Message—The full error message.
- Description—The explanation for the log message.
- Operator Instructions—Instructions for resolving the issue that triggered the event, if available.

**Related
Documentation**

- [Network Monitoring Workspace Overview on page 284](#)
- [Viewing the Node List on page 287](#)
- [Viewing Managed Devices on page 63](#)
- [Resyncing Nodes on page 288](#)
- [Searching in the Network Monitoring Workspace on page 288](#)

Viewing and Acknowledging Alarms

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

There are two basic categories of alarm, acknowledged and outstanding. Acknowledging an alarm indicates that you have taken responsibility for addressing the corresponding network or systems-related issue. Any alarm that has not been acknowledged is considered outstanding and is therefore visible to all users on the Alarms page, which displays outstanding alarms by default.

If an alarm has been acknowledged in error, you can find the alarm and unacknowledge it, making it available for someone else to acknowledge.

When you acknowledge, clear, escalate, or unacknowledge an alarm, this information is displayed in the alarm's detailed view. You can click the alarm ID to view the 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 295](#)
- [Acknowledging Alarms on page 296](#)

- [Clearing Alarms on page 296](#)
- [Escalating Alarms on page 297](#)
- [Unacknowledging Alarms on page 297](#)
- [Viewing Acknowledged Alarms on page 297](#)

Viewing Alarms

To view alarms:

1. Select **Network Monitoring > Alarms**.

2. Click one of the following links:

- All alarms (summary)
- All alarms (detail)
- Advanced Search

The Alarms page appears with the list of alarms. By default, the first view for all alarms, both summary and details, shows outstanding alarms, as indicated by the content of the Search constraints box.

3. (Optional) Use the toggle control (the minus sign) in the Search constraints box to show acknowledged alarms.

4. (Optional) You can refine the list of alarms by either or both of the following:

- Entering something 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.

Click **Search**.

Links at the top of the page, under its title, provide access to further functions:

- View all alarms
- Advanced Search
- Long Listing/Short Listing

[Table 45 on page 295](#) describes the information displayed in the columns of the Alarms page. An X indicates the data is present in the Short Listing or Long Listing displays.

Table 45: 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 <i>alarm ID</i> section of the Alarms page.
Severity	Color-coding only	X	Toggle enables you to show only alarms with this severity, or not to show alarms with this severity.

Table 45: Information Displayed in the Alarms List (*continued*)

Data	Short Listing	Long Listing	Comments
UEI		X	Toggle enables you to show only events with this UEI, or not to show events with this UEI.
Node	X	X	Toggles enable you to show only alarms on this IP address, or not to show alarms for this interface.
Interface		X	
Service		X	
Count	X	X	Click the count to view the Events page for the event that triggered this alarm.
Last Event Time	X	X	Mouse over this to see the event ID. Toggles enable you to show only alarms occurring after this one, or only alarms occurring before this one.
First Event Time		X	
Log Msg	X	X	

- **Severity Legend**—Click to display a table in a separate window showing the full explanations and color coding for the degrees of severity.
- **Acknowledge/Unacknowledge entire search**—Click to perform the relevant action on all alarms in the current search, including those not shown on your screen.

Acknowledging Alarms

To acknowledge an alarm:

1. Select the alarm's **Ack** check box. To select all alarms, at the bottom of the page, click **Select All**.
2. At the bottom of the page, select **Acknowledge Alarms** from the list on the left, and click **Go**.

The alarm is removed from the default view of all users.

Clearing Alarms

To clear an alarm:

1. Select the alarm's **Ack** check box. To select all alarms, at the bottom of the page, click **Select All**.
2. At the bottom of the page, select **Clear Alarms** from the list on the left, and click **Go**.

Escalating Alarms

To escalate an alarm:

1. Select the alarm's **Ack** check box. To select all alarms, at the bottom of the page, click **Select All**.
2. At the bottom of the page, select **Escalate Alarms** from the list on the left, and click **Go**.

The alarm is escalated by one level.

3. (Optional) To view the severity to which an alarm has been escalated, click the alarm's ID.

Unacknowledging Alarms

To unacknowledge an alarm:

1. Display the list of acknowledged alarms by toggling the Search constraint box so that it is showing 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 297](#)

Viewing, Configuring, and Searching for Notifications

When the system detects important events, one or more notices are sent automatically to a pager, an email address, or both. In order to receive notices, users must have their notification information configured in their user profile (see [“Admin: Configuring Network Monitoring” on page 305](#)), notices must be switched on, and an important event must be received.

From the Network Monitoring / Notification page, you can:

- Check **Your outstanding notices** to display all unacknowledged notices sent to your user ID.
- View **All outstanding notices** to display all unacknowledged notices for all users.
- View **All acknowledged notices** to provide a summary of all notices sent and acknowledged for all users.
- 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 detail**.



NOTE: This 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 298](#)

Notification Escalation

Once a notice is sent, it is considered outstanding until someone acknowledges receipt of the notice via the Network Monitoring / Notification / Detail page, which you reach by entering a notice ID in the **Notice** field on the Network Monitoring / Notification page.

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 305.

Related Documentation

- [Network Monitoring Workspace Overview on page 284](#)
- [Viewing the Node List on page 287](#)
- [Viewing Managed Devices on page 63](#)
- [Resyncing Nodes on page 288](#)
- [Searching in the Network Monitoring Workspace on page 288](#)

Creating Reports

You can configure key SNMP customized (KSC) performance reports, node reports, domain reports by selecting **Network Monitoring > Reports**.

- [Creating Key SNMP Customized Performance Reports, Node Reports, Domain Reports on page 299](#)
- [Creating a New KSC Report from an Existing Report on page 299](#)

Creating Key SNMP Customized Performance Reports, Node Reports, Domain Reports

To create a new KSC report:

1. Select **Network Monitoring > Reports > KSC Performance, Nodes, Domains**.
2. From the Node and Domain Interface Reports section, select a resource for the report.
3. Under the Customized Reports section, click **Create New > Submit**

The Customized Report Configuration page is displayed.

4. In the Title text box, enter a name for the report.
5. (Optional) To add a graph to the report:
Select **Add New Graph**.
 - a. Select a resource from the Resources section.
 - b. Select **Choose Child Resource** to select the resource you want to use in a graph.
 - c. Select the check box for the specific node resources you want to view, or click **Select All** to select all the displayed node resources.
6. (Optional) To allow global manipulation of the report timespan, select **Show Timespan Button**.
7. (Optional) To allow global manipulation of report prefabricated graph type, select **Show Graphtype Button**
8. (Optional) Select the number of graphs to show per line in the report.
9. To save the report, click **Save**.

Creating a New KSC Report from an Existing Report

To create a new KSC report from an existing report:

1. Select **Network Monitoring > Reports > KSC Performance, Nodes, Domains**.
2. Under the Resources section, select the KSC report that you want to use to create a new report and click **Create New from Existing > Submit**.

The Customized Report Configuration page is displayed.

3. Select a resource.
4. In the Title text box, enter a new name for the report.

5. (Optional) Customize the report by adding graphs and specifying the number of graphs per line.
6. Click **Save**.

Related Documentation

- [Network Monitoring Workspace Overview on page 284](#)
- [Network Monitoring Reports Overview on page 286](#)
- [Viewing Reports on page 300](#)
- [Deleting Reports on page 304](#)
- [Viewing the Node List on page 287](#)
- [Viewing Managed Devices on page 63](#)
- [Resyncing Nodes on page 288](#)
- [Searching in the Network Monitoring Workspace on page 288](#)

Viewing Reports

Select **Network Monitoring > Reports** to view the following types of reports:

- Resource graphs that provide SNMP performance data collected from managed nodes on your network
- Key SNMP customized (KSC) performance reports, node reports, domain reports. You can generate KSC reports to view SNMP performance data using prefabricated graph types.
- Database reports that provide graphical or numeric views of service level metrics
- Statistics reports that provide regularly scheduled reports on response time, SNMP node-level performance and interface data, and OSPF area data

Viewing Resource Graphs

To view a resource graph:

1. Select **Network Monitoring > Reports > Resource Graphs**.
2. Select the resource node for which you want to generate a standard performance report or custom performance report.
The Node Resources page is displayed.
3. To select the specific node resources data that you want to view, choose one of the following options:
 - To view data for a subset of node resources:
 - a. Click the **Search** option
 - b. Enter a text string to identify the node resources you want to view.

- c. Click **OK**.
- d. Select the check box for the specific node resources you want to view, or click **Select All** to select all the displayed node resources.
 - To view data for all listed node resources, click **Select All**.
4. To display graphical data for the all the selected node resources, click **Graph Selection**.
5. In the Time Period field, specify the period of time (last day, last week, last month, custom) which the report should cover.

The statistical data is refreshed to reflect the time period specified.

Viewing Key SNMP Customized (KSC) Performance Reports, Node Reports, Domain Reports

To view a KSC report:

1. Select **Network Monitoring > Reports > KSC Performance, Nodes, Domains**.
2. Select the resource node for which you want to view a standard performance report or custom performance report.

The Custom View Node Report is displayed.

3. (Optional) To customize the Node Report view:
 - To override the default time span, in the Override Graph Timespan list, select number of hours, days, or months, or select by quarter, or year.
 - To override the default graph type, from the Override Graph type list, select number of hours, days or months, by quarter or by year.
4. Select **Update Report View** to refresh the report.
5. Select **Exit Report Viewer** to exit the report view or select **Customize This Report** to make additional updates to the report.

Viewing Database Reports

To view database reports:

1. Select **Network Monitoring > Reports > Database Reports > List reports**.
The Local Report Repository page is displayed.
2. Select on a report page number or select **Next** or **Last** to scroll through the available reports to locate the database report you want to view.
3. To execute a report, from the row that lists the report, select the arrow icon from the Action column.
The Run Online Report page is displayed.
4. In the Report Format field, select either PDF or comma-separated values (CSV) format for the report from the list.
5. Select **run report**.

For PDF, the report is displayed in the selected format. For CSV, you are prompted to either open or save the file.

Sending Database Reports

To send database reports:

1. Select **Network Monitoring > Reports > Database Reports > List reports**.

The Local Report Repository page is displayed.

2. Select on a report page number or select **Next** or **Last** to scroll through the available reports to locate the database report you want to send.
3. You can send a report to file system or e-mail the report.

- To execute a report, in the row that lists the report, select the arrow icon from the Action column.

The Run Online Report page is displayed.

- a. From the Report Format list, select either PDF or comma-separated values (CSV) format for the report from the list.
- b. Select **run report**.

For PDF, the report is displayed in the selected format. For CSV, you are prompted to either open or save the file.

- To send a report to a file system or e-mail the report, select the Deliver report icon from the Action column.

The Report Parameters page is displayed.

- a. From the report category field, select a category (Network Interfaces, Email Servers, Web Servers, Database Servers, and so forth)
 - b. From the end date field, select the end date and time for the report.
 - c. Select **Proceed**.
- The Report Delivery Options page is displayed.
- d. In the name to identify this report field, specify a name for the report.
 - e. (Optional) To send the report through e-mail, select the email report check box.
 - f. In the format field, select the format type (HTML, PDF, SVG).
 - g. In the recipient field, enter the name of the person to whom the report will be sent.
 - h. (Optional) To save a copy of the report select the **save a copy of this report** check box.
 - i. Select **Proceed**.

The Report Running page is displayed.

- j. Select **Finished** to close the page and return to the Local Report Repository page.

Viewing Pre-run Database Reports

To view database reports:

1. Select **Network Monitoring > Reports > Database Reports > View and manage pre-run reports**.

All the pre-run reports are displayed in a table.

2. From the view report column, select the **HTML**, **PDF**, or **SVG** link to specify the format in which you want to view the report.

The database report is displayed.

Viewing Statistics Reports

To view statistics reports:

1. Select **Network Monitoring > Reports > Statistics Reports**.

The Statistics Report List page displays a list of all available reports in a table.

2. To search for specific information in statistics reports, enter search text in the blank field directly above a Statistics Report column, and select **Filter**.

All available statistics reports that match the filter text you specified are displayed in the Statistics Report List page.

3. To clear the filtered information and restore the original list of statistics reports, select **Clear**.

All available statistics reports are again displayed in the Statistics Report List page.

4. To view complete information for a specific statistics report, click the Report description link from the Statistics Report List page.

The statistics report is displayed and includes Parent resources and resource graphs with SNMP interface data.

Generating a Statistics Report for Export

To generate a statistics report as a PDF file or Excel spreadsheet:

1. Select **Network Monitoring > Reports > Statistics Reports**.

The Statistics Report List page displays a list of all available reports in a table.

2. In the Report Description column, select the report link.

The statistics report is displayed and includes all information for that report, including parent resources and resource graphs with SNMP interface data.

3. Choose PDF or Excel as the format for the statistics report:

- To generate the statistics report in PDF format, in the top-right corner of the Statistics Report, select the Export PDF icon.

The File Download window is displayed.

- To generate the statistics report as an Excel spreadsheet, in the top-right corner of the Statistics Report, select the Export Excel icon.

The File Download window is displayed.

4. From the File Download window, select **Open** to view the statistics report or select **Save** to save the statistics report.

Related Documentation

- [Network Monitoring Workspace Overview on page 284](#)
- [Network Monitoring Reports Overview on page 286](#)
- [Creating Reports on page 299](#)
- [Deleting Reports on page 304](#)
- [Viewing the Node List on page 287](#)
- [Viewing Managed Devices on page 63](#)
- [Resyncing Nodes on page 288](#)
- [Searching in the Network Monitoring Workspace on page 288](#)

Deleting Reports

To delete key SNMP customized (KSC) reports and database reports, select **Network Monitoring > Reports**.

- [Deleting Key SNMP Customized Reports on page 304](#)
- [Deleting Pre-run Database Reports on page 304](#)

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 284](#)
- [Network Monitoring Reports Overview on page 286](#)
- [Creating Reports on page 299](#)
- [Viewing Reports on page 300](#)
- [Viewing the Node List on page 287](#)
- [Viewing Managed Devices on page 63](#)
- [Resyncing Nodes on page 288](#)
- [Searching in the Network Monitoring Workspace on page 288](#)

Viewing Charts

To view charts, select **Network Monitoring > Charts**.

This page displays by default:

- Alarms Severity Chart, showing the counts of both alarms and events, distinguishing between major, minor, and critical severities.
- Last 7 Days Outages, showing the counts of outages per service.
- Node Inventory, showing the counts of nodes, interfaces, and services.

Admin: Configuring Network Monitoring

This topic contains the following tasks:

- [Configuring Users, Groups, and Roles on page 305](#)
- [OpenNMS System: System Information on page 309](#)
- [OpenNMS System: Instrumentation Log Reader on page 310](#)
- [Notification Status on page 311](#)

Configuring Users, Groups, and Roles

To configure user permissions to perform network monitoring tasks for specified categories of network assets, such as routers, switches, and production devices, you must perform the following tasks:

1. Add users and their information to the system, and set their duty schedules, that is, the times when they can receive notifications. For more information, see [“Viewing, Configuring, and Searching for Notifications” on page 297](#).

2. Add new groups and assign and unassign users to groups. You must create at least one group before you can assign any users. Categories of equipment such as routers or switches can be assigned only to groups. Users in the group to which the production category has been assigned can monitor the production network. Both users and groups can be assigned duty schedules.
3. Configure roles that define On Call schedules for users. Assign roles to groups.

The default user is the Default administrator. Do not delete this user.

- [Adding Users on page 306](#)
- [Modifying and Deleting Users on page 307](#)
- [Adding Groups on page 307](#)
- [Configuring Roles on page 308](#)
- [Assigning Roles to Groups on page 309](#)

Adding Users

To add a user:

1. Select **Configure Users, Groups and Roles > Configure Users > Add New User**.

The New User page appears.

2. Enter a user ID and a password in the fields of those names, confirm the password, and click **OK**.

The Modify User page appears.

3. (Optional) Add any necessary details to the user profile.



NOTE: Even if you do not add details, you must click **Finish (Step 4)** to create a user.

- Full Name
- Comments
- Email
- Pager Email
- XMPP Address (for instant messages using the Jabber XMPP protocol)
- Numeric Service (for pagers that cannot display text messages)
- Numerical PIN — The Telephone PIN is an optional numeric field used to authenticate called users.
- Text Service (for alphanumeric pagers)
- Text PIN
- Work Phone
- Mobile Phone

- Home Phone
- Duty Schedules

Duty schedules determine when users should receive notifications. A duty schedule consists of a list of days for which the time applies and a time range (military time: days run from 0000 to 2359). If your duty schedules span midnight, or if your users work multiple, non-contiguous time periods, configure multiple duty schedules. To do this, select the number of duty schedules to add from the drop-down box next to **Add This Many Schedules**, and click **Add This Many Schedules**. To create a duty schedule spanning midnight, enter the first schedule from the start time to 2359 on one day, and enter a second duty schedule that begins at 0000 and ends at the end of that user's coverage. To remove configured duty schedules, select the appropriate check boxes in the Delete column and click **Remove Checked Schedules**.

4. Click **Finish**.

Modifying and Deleting Users

The default user is the Default administrator. Do not delete this user.

To modify or delete a user:

1. Select **Network Monitoring > Admin > Configure Users, Groups and Roles > Configure Users**.

Click the User ID link to view detailed information about a user.

2. (Optional) To delete a user, click the appropriate trash can icon in the Delete column.
A message appears, asking you to click OK to confirm.

3. (Optional) To modify a user, click the appropriate edit icon.

The Modify User page appears.

4. (Optional) Edit any necessary details in the user profile. See Step 3 of the preceding procedure to add a user.
5. (Optional) To rename a user, select the user and click **Rename**.
6. Click **Finish**.

Adding Groups

To add a group, assign users to it, and assign a category to the group:

1. Select **Network Monitoring > Admin > Users and Groups**, and click **Configure Groups**.

The Group Configuration page appears.

2. Click **Add new group**.

The New Group page appears.

3. Enter a group name and, if desired, a comment in the fields of those names.
4. Click **OK**.

The Modify Group page appears.

5. In the Assign/Unassign Users section of the page, select a user from the Available Users list, and click the >> button under the list.

The user moves to the Currently in Group list.

You can move a user up and down the list by clicking **Move Up** or **Move Down**, and you can remove the user from the group by selecting the user ID and clicking the << button under the list.

6. To assign a category to a group, in the Assign/Unassign Categories section of the page, select a category for your group from the Available Categories list, and click the >> button under the list.

The category moves to the Currently in Group list.

You can move a category up and down the list by clicking **Move Up** or **Move Down**, and you can remove the category from the group by selecting the category and clicking the << button under the list.

7. To assign schedules for groups, see Step 3 of the procedure to add a user. Note that the schedules of a user must coincide with that of the group to which the user belongs. If a group with a weekend schedule contains a user with a weekday schedule, that user will not be able to do any work.
8. When you have finished assigning users to groups and categories to groups, click **Finish**.

Configuring Roles

This topic explains how to configure roles that define On Call schedules for users. Note that the ability to receive notifications does not necessarily coincide with being on call. However, a user who is on call needs to be able to receive notifications.

To configure roles:

1. Select **Network Monitoring > Admin > Configure Users, Groups and Roles**, and click **Configure Roles**.

The Role Configuration page appears.

2. To add a new role, click **Add New Role**.

The Edit Role page appears.

3. To name the role, select the text in the Name box, and replace it by entering the role name.
4. To select the role's supervisor, choose a user ID from the Supervisor list (Admin is the default). The supervisor does not have to be a member of the group to which the role is assigned. After the role is created, the name of the role's supervisor appears next to Currently On Call.

5. To enter a description, enter text in the Description field.
6. Currently On Call does not have a field unless the role has already been created. If the role has already been created, the On Call field displays the name of the role's supervisor, selected in Step 4.

Assigning Roles to Groups

To assign roles to groups:

1. Select **Network Monitoring > Admin > Configure Users, Groups and Roles**, and click **Configure Roles**.

The Role Configuration page appears.

2. Select the role that you want to assign.

The View Role page appears.

3. Click **Edit Details**.

The Edit Role page appears.

4. On the Edit Role page, select from the Membership Group list.

5. Click **Save**.

The View Role page appears, displaying the details for the role. You can edit the details by clicking **Edit Details**. This returns you to the previous Edit Role page.

6. When finished, you can either click **Done** to return to the Role Configuration page, or move on to the next step, setting the role schedule.

7. To set the role schedule on the View Role page, select the appropriate month and year by clicking the << or >> controls.

Note that the month and year can be changed in the next step, so that you could choose a period of several months or years.

8. To select the appropriate days of the month for a specific user in the group, click the + sign for any day and date.

The Edit Schedule Entry page appears.

9. Select the user from the User list, then select the Start Date, Start Time, End Date, and End Time from the respective lists.

10. Click **Save**.

The View Role page reappears.

11. Continue setting the role schedule for different groups as necessary, and when finished, click **Done**.

OpenNMS System: System Information

Select **Network Monitoring > Admin > System Information** to view the OpenNMS configuration and the system configuration on which OpenNMS is running.

- The OpenNMS Configuration section of the page lists the following information:
 - OpenNMS 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

OpenNMS System: Instrumentation Log Reader

Use the instrumentation log reader to find out how long each node is taking to collect data.

The input for the instrumentation log reader is the instrumentation log file produced by the OpenNMS system. To produce parsable data, the log file must be produced with DEBUG enabled.

To ensure service collector data is available, ensure that in the *log4j.properties* configuration file, the <Collectd> and <Instrumentation> appenders are set to log at DEBUG.

The log reader uses the timestamps of events occurring during data collection to compute the total amount of time a node is taking for data collection.

An instrumentation log entry has the following general format:

```
<timestamp> DEBUG [<thread-name>] <operation type> <event-type>: <optional  
service identifier> <optional error-info>
```

The output appears with the services listed in descending order by average collection time. The service whose collection time took the longest would therefore be at the top of the list.

To submit filtering criteria and reset them, select **Network Monitoring > Admin > Instrumentation Log Reader**.

The page displays Start Time, End Time, Duration, Total Services, and Threads Used.

The categories of information collected are:

- Service
- Collections
- Average Collection Time
- Average Time Between Collections
- Successful Collections
- Successful Percentage
- Average Successful Collection Time
- Unsuccessful Collections
- Unsuccessful Percentage
- Average Unsuccessful Collection Time
- Average Persistence Time
- Total Persistence Time

Notification Status

Notifications are sent out only if Notification Status is switched to On. This is a systemwide setting. The default setting is Notification Status Off. After you change the setting, click **Update**.

Related Documentation

- [Network Monitoring Workspace Overview on page 284](#)
- [Viewing the Node List on page 287](#)
- [Viewing Managed Devices on page 63](#)
- [Resyncing Nodes on page 288](#)
- [Searching in the Network Monitoring Workspace on page 288](#)
- [Viewing Charts on page 305](#)

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. OpenNMS is shipped with the *public* community string. If you have set a different *read* community on your devices, this is where you must enter it.

In the boxes on the left, enter in a specific IP address and community string, or a range of IP addresses and a community string, and other SNMP parameters. OpenNMS optimizes this list, so enter the most generic first (that is, the largest range) and the specific IP addresses last, because if a range is added that includes a specific IP address, the community name for the specific address is changed to be that of the range. For devices that have already been discovered and that have an event stating that data collection has failed because the community name changed, you might need to update the SNMP information on the interface page for that device (by selecting the Update SNMP link) for these changes to take effect.

To configure SNMP using an IP address:

1. Select **Network Monitoring > Admin > Configure SNMP Community Names by IP**, and enter in the First IP Address field either a single IP address, or the first one of a range.
2. If you are not entering a range of IP addresses, leave the Last IP Address field blank, otherwise enter the last IP address of the range.
3. In the Community String field, enter the community string you use for your devices. The default is *public*.
4. (Optional) Enter a timeout in the Timeout field.
5. Select the appropriate version from the Version list.
6. (Optional) Enter the number of retries in the Retries field.
7. (Optional) Enter the port number in the Port field.
8. Click **Submit**. The system displays a message telling you whether OpenNMS needs to be restarted for the configuration to take effect.

Related Documentation • [Network Monitoring Workspace Overview on page 284](#)

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 • [Network Monitoring Workspace Overview on page 284](#)

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 OpenNMS performs tests on this interface or service. If you want to explicitly enable or disable testing you can set that up here. A typical case is if a webserver is listening on both an internal and an external interface. If you manage the service on both interfaces, you will get two notifications if it fails. If you want only one, unmanage the service on one of the interfaces.

Select **Network Monitoring > Admin > Manage and Unmanage Interfaces and Services** to manage or unmanage your node, interface, and service combinations.

To change the status, you have these choices: **Apply Changes**, **Cancel**, **Select All**, **Unselect All**, or **Reset**.

Related Documentation • [Network Monitoring Workspace Overview on page 284](#)

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 313](#)
- [Modifying Thresholds on page 316](#)
- [Deleting Thresholds on page 317](#)

Creating Thresholds

To create a threshold:

1. Select **Network Monitoring > Admin > Manage Thresholds**.

The Threshold Configuration page appears and lists the threshold groups that are configured on the system.

2. To create a new threshold for a threshold group, select **Edit** next to the threshold group.

The Edit group page appears.

3. Select **Create New Threshold**.

The Edit threshold page appears.

4. To configure the threshold, specify appropriate values for the following threshold fields:
 - Type—Specify high, low, relativeChange, absoluteChange, rearmingAbsoluteChange.
 - Datasource—Specify a name for the datasource.
 - Datasource type—Specify a datasource type from the list.
 - Datasource label—Specify a type from the list.
 - Value—Use depends on the type of threshold.
 - Re-arm— Specify the name of a custom UEI to send into the events system when this threshold is re-armed. If left blank, it defaults to the standard thresholds UEIs.
 - Trigger—Specify the number of times the threshold must be exceeded in a row before the threshold is triggered.



NOTE: A trigger is not used for relativeChange thresholds.

- Description—(Optional) A description used to identify the purpose of the threshold.
- Triggered UEI— A custom UEI to send into the events system when the threshold is triggered. If a UEI is not specified, it defaults to the standard thresholds UEIs in the format *uei.opennms.org/<category>/<name>*.
- Re-armed UEI—A custom UEI to send into the events system when this threshold is re-armed. If left blank, it defaults to the standard thresholds UEIs.

5. Select **Save** to create the threshold in Junos Space.
6. (Optional) To configure a resource filter for a threshold:
 - a. Configure a filter operator to define the logical function to apply for the threshold filter to determine whether or not to apply the threshold. An OR operator specifies that if the resource matches any of the filters, the threshold is processed. An AND operator specifies that the threshold is processed only when a resource match all the filters.
 - b. Specify a field name for the filter the filter operator to define the logical function to apply for the threshold filter to determine whether or not to apply the threshold.
 - c. Specify the mathematical expression with data source names that is evaluated and compared to the threshold values.
 - d. Select the **Add** action to add the filter to a threshold.

To create an expression-based threshold:

1. Select **Network Monitoring > Admin > Manage Thresholds**.
The Threshold Configuration page appears and lists the threshold groups that are configured on the system.
2. To create a new threshold for a threshold group, select **Edit** next to the threshold group.
The Edit group page appears.
3. Select **Create New Expression-based Threshold**
The Edit expression threshold page appears.
4. To configure the threshold, specify appropriate values for the following expression threshold fields:
 - Type—Specify high, low, relativeChange, absoluteChange, rearmingAbsoluteChange.
 - Expression—Specify a mathematical expression that includes the datasource names which are evaluated and compared to the threshold values.
 - Datasource type—Specify a datasource type from the list.
 - Datasource label—Specify a type from the list.
 - Value—Use depends on the type of threshold.
 - Re-arm— Specify the name of a custom UEI to send into the events system when this threshold is re-armed. If left blank, it defaults to the standard thresholds UEIs.
 - Trigger—Specify the number of times the threshold must be exceeded in a row before the threshold is triggered.



NOTE: A trigger is not used for relativeChange thresholds.

- Description—(Optional) A description used to identify the purpose of the threshold.
 - Triggered UEI— A custom UEI to send into the events system when the threshold is triggered. If a UEI is not specified, it defaults to the standard thresholds UEIs in the format *uei.opennms.org/<category>/<name>*.
 - Re-armed UEI—a custom UEI to send into the events system when this threshold is re-armed. If left blank, it defaults to the standard thresholds UEIs.
5. Select **Save** to create the expression threshold in Junos Space.
 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 284](#)

Configuring Notifications

- [Configuring Event Notifications on page 317](#)
- [Configure Destination Paths on page 319](#)
- [Configure Path Outages on page 320](#)

Configuring Event Notifications

You can configure an event to send a notification whenever that event is triggered. You can add, edit, and delete event notifications.

To add a notification to an event:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Event Notifications**.
2. Click **Add New Event Notification**.
3. Select the event UEI that will trigger the notification.

4. Click **Next**.
5. Build the rule that determines whether to send a notification for this event, based on the interface and service information specified in the event.
6. You can validate the rule results or skip the rule results validation:
 - To validate the rule results:
 - a. Click **Validate rule results**.
 - b. Click **Next**.
 - c. Specify a name for the notification, choose the destination path, and enter the information required to send with the notification.
 - d. Click **Finish**.
 - To skip the rule results:
 - a. Click **Skip results validation**.
 - b. Specify a name for the notification, choose the destination path, and enter the information required to send with the notification.
 - c. Click **Finish**.

To edit an existing event notification:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Event Notifications**.
2. Click the **Edit** button that is located to the left of the event notification you want to modify.
3. Select the event UEI that will trigger the notification.
4. Click **Next**.
5. Build the rule that determines whether to send a notification for this event, based on the interface and service information specified in the event.
6. (Optional) Click **Reset Address and Services** if you want to clear the changes that you have entered.
7. You can validate the rule results or skip the rule results validation:
 - To validate the rule results:
 - a. Click **Validate rule results**.
 - b. Click **Next**.
 - c. Specify a name for the notification, choose the destination path, and enter the information required to send with the notification.
 - d. Click **Finish**.

- To skip the rule results:
 - a. Click **Skip results validation**.
 - b. Specify a name for the notification, choose the destination path, and enter the information required to send with the notification.
 - c. Click **Finish**.

To delete an existing event notification:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Event Notifications**.
2. Click the **Delete** button that is located to the left of the event notification you want to modify.
3. Click **Ok** in the delete notification confirmation dialog box to delete the notification.

Configure Destination Paths

You can configure a destination path that describes what users or groups will receive notifications, how the notifications will be sent, and who to notify if escalation is needed. A destination path defines a reusable list of contacts that you include in an event configuration.

To create a new destination path:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Destination Paths**.
2. Click the **New Path** button.
3. Specify appropriate values for the following fields:
 - Name field—Specify a name for the destination path.
 - Initial Delay—From the list, select the number of seconds to wait before sending notifications to users or groups.
 - Initial targets—Select the users and groups to whom the event notification will be sent.
4. Click the **Add Escalation** button to specify users and groups to whom event notification will be sent.
5. Choose the commands to use (for example, callHomePhone, callMobilePhone, or callMobilePhone) for each user and group.
6. Click **Next**.
7. Click **Finish** when you have finished editing the destination path.

To modify an existing destination path:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Destination Paths**.
2. Under Existing Paths, select the existing destination path that you want to modify.
3. Click **Edit**.
4. You can make changes to any of the following fields:
 - Initial Delay—From the list, select the number of seconds to wait before sending notifications to users or groups.
 - Initial targets—Add users and groups to whom the event notification should be sent and remove users and groups to whom the event should not be sent.
5. Click the **Add Escalation** button to specify users and groups to whom event notification will be sent.
6. Choose the commands to use (for example, callHomePhone, callMobilePhone, or callMobilePhone) for each user and group.
7. Click **Next**.
8. Click **Finish** when you have finished modifying the destination path.

To delete a destination path:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Destination Paths**.
2. Under Existing Paths, select the existing destination path that you want to delete.
3. Click **Delete**.
4. Click **Ok** to confirm that you want to delete the selected destination path.

Configure Path Outages

You can configure a path outage that describes what users or groups will receive notifications, how the notifications will be sent, and who to notify if escalation is needed. A destination path defines a reusable list of contacts that you include in an event configuration.

To create a new path outage:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Path Outage**.
2. Click the **New Path** button.
3. Specify appropriate values for the following fields:
 - Critical Path—Enter the critical path IP address.
 - Critical Path Service—From the list, select the ICMP protocol.
 - Initial targets—Select the users and groups to whom the event notification will be sent.

4. Build the rule that determines which nodes are subject to this critical path.
5. Select the **Show matching node list** check box to show the list of nodes that match.
6. Choose the commands to use (for example, callHomePhone, callMobilePhone, or callMobilePhone) for each user and group.
7. Click **Validate rule results** to validate the rule.
8. Click **Finish** when you have finished configuring the path outage.

**Related
Documentation**

- [Network Monitoring Workspace Overview on page 284](#)

Configuring Scheduled Outages

You can configure scheduled outages to suspend notifications, polling, thresholding and data collection (or any combination of these) for any interface/node for any length of time.

To create a scheduled outage:

1. Select **Network Monitoring > Admin > Scheduled Outages**.
2. Specify a name for the scheduled outage.
3. Click **Add new outage** to create the scheduled outage.
4. Build the rule that determines which nodes are subject to this critical path.
5. Specify appropriate values for the following fields:
 - Node Labels—From the list, select the node labels to add.
 - Interfaces—From the list, select the interfaces to add.
 - Outage type—From the list, select daily, weekly, monthly, or (time) specific.
 - Time—Specify one or more days and times for the outage.
6. Specify that the outage applies to one or more of the following categories:
 - Notifications
 - Status polling
 - Threshold checking
 - Data collection

**Related
Documentation**

- [Network Monitoring Workspace Overview on page 284](#)

PART 6

Device Configuration Files

- [Managing Configuration Files on page 325](#)

CHAPTER 27

Managing Configuration Files

- [Managing Configuration Files Overview on page 326](#)
- [Viewing Configuration File Statistics and Inventory on page 327](#)
- [Backing Up Configuration Files on page 328](#)
- [Deleting Configuration Files on page 330](#)
- [Restoring Configuration Files on page 331](#)
- [Comparing Configuration Files on page 332](#)
- [Editing Configuration Files on page 334](#)
- [Exporting Configuration Files on page 336](#)
- [Tagging, Viewing Tags, and Untagging Configuration Files on page 337](#)
- [User Privileges in Configuration File Management on page 337](#)

Managing Configuration Files Overview

Centralized configuration file management enables you to maintain copies of your device configuration files within Junos Space, storing multiple versions of any given configuration file. It therefore provides for device configuration recovery. It also facilitates maintaining configuration consistency across multiple devices.

Because each commit command on a device creates a new version on that device, backup copies may not be kept long. No more than 49 copies can be stored on a device. Junos Space provides backups with longer lifecycles.



NOTE: Version management for configuration files in Junos Space is therefore independent from the configuration file versioning on devices.

The configuration file management workspace handles three types of configuration file:

- Running configuration—The configuration file currently in effect on the device. The running configuration file is labeled Version 0.
- Candidate configuration—The new, not yet committed, configuration file that will become the running configuration.
- Backup configuration—The configuration file for recovery or rollback purposes. A backup configuration file is created by a commit command and the oldest backup (version 49) is deleted. The most recent backup configuration file is labeled Version 1.

A potential workflow for an individual file or device in this workspace could be:

- Backup device and thus bring device's running configuration under Junos Space management
- Edit a copy of the backup configuration to create a candidate configuration
- Verify edits by comparing the initial backup version of the configuration file with the edited version
- Restore the candidate configuration to the device
- Export the initial backup to a zip file
- Delete the initial backup from Junos Space.

Stored configurations can be viewed by double-clicking the item on the Manage Configuration Files page.

A dialog box appears, displaying the file in a non-editable format. You can select the version you want to view from the **Version** list.

The status bar near the bottom of the dialog box shows the current page number, the total number of pages in the file, and provides paging controls and a Refresh button. Below that is the Comments area.

To perform an action on a configuration file, either select one and select an action from the Actions drawer, or right-click a configuration file and select an action from the right mouse-click menu. You can perform the following actions:

- [Deleting Configuration Files on page 330](#)
- [Restoring Configuration Files on page 331](#)
- [Comparing Configuration Files on page 332](#)
- [Editing Configuration Files on page 334](#)
- [Exporting Configuration Files on page 336](#)
- [Tagging, Viewing Tags, and Untagging Configuration Files on page 337](#)

Viewing Configuration File Statistics and Inventory

The Config Files statistics page, which is directly under the Config Files workspace, displays two bar charts, showing:

- The Configuration file count by device family
- The most frequently revised configuration files.

In both cases, mouse over the graphic to display the contents in a tooltip.

All configuration files in Junos Space are displayed on the **Manage Config Files** inventory landing page. You can toggle between the icon view and the tabular view. View stored configurations either by clicking **Details** on a thumbnail, or by double-clicking an entry in the tabular view or a thumbnail in the icon view.

The following information appears for each configuration file:

- Host Name
- IP Address
- Platform
- Serial Number of Device
- Software Version

Related Documentation

- [Backing Up Configuration Files on page 328](#)
- [Managing Configuration Files Overview on page 326](#)
- [Managing Tags Overview on page 491](#)

Backing Up Configuration Files

Backing up a configuration file in the Config Files workspace means importing the configuration file from the device, and storing it in Junos Space.

Backing up your device configurations is therefore the prerequisite for configuration file management (see [“Managing Configuration Files Overview”](#) on page 326).

Only devices that have been previously discovered can have their configuration files backed up. The backup function will skip over any devices that cannot be reached. In the Job Manager, under Job Status, a skipped-over configuration file backup will show up as Failed.

The backup function will check for differences before creating a new version of a configuration file. If no changes are detected, the device will be skipped over. However, its status will be shown as Success.



NOTE: The backup function checks for differences between the configuration on the device and the backup configuration stored in Junos Space. Therefore, even if no change has been made to a device's configuration, if you edit its configuration file and then make another backup, a new version will be created. To illustrate: the first backup will be version 1, the edited configuration file will be version 2, and the second backup will be version 3.

A configuration file backup generates an audit log entry.

To back up your device configuration files to Junos Space, follow this procedure:

1. In Network Application Platform, navigate to **Config Files > Manage Config Files > Backup Config Files**.

The **Backup Config Files** page appears, displaying all the devices managed by Junos Space, with the following information:

- Host Name
- IP Address
- Platform
- Serial Number
- Software Version

Since the table displays one device (record) per row, a single page may not be sufficient to list all your devices.

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 between the pages and refreshing them. The right side of the status bar indicates how many records are currently displayed and the total number of records.

2. Select the device(s) you want to back up. To back up all of them, select the check

box in the column header next to Host Name.

3. To back up, choose one of the following options:

- Immediately
- Schedule for a Later Time—This results in one backup per device
 - a. Select the check box next to the Schedule at a Later Time label or click the arrow next to the Schedule at a Later Time label to display the corresponding fields.
 - b. Select a date from the field on the left, and a time from the field on the right. The time zone displays to the right of the time field. The time zone is set on and for the Junos Space server.
- Repeat—This results in scheduled repetition, i.e., multiple backups per device
 - a. Select the check box next to the Repeat label or click the arrow next to the Repeat label to display the corresponding fields.
 - b. Choose Minutes, Hours, Days, Weeks or Years from the dropdown list.
 - c. To set the frequency of the repetition, enter the appropriate whole number in the upper field.
 - d. If necessary, set the End Time:

Select the check box next to the End Time label or click the arrow next to the End Time label to display the corresponding fields.
 - e. Select a date from the field on the left, and a time from the field on the right. The time zone displays to the right of the time field. The time zone is set on and for the Junos Space server.

4. Click **Backup**.

The Backup Configuration Files dialog box appears, announcing that it has successfully scheduled backup of the selected devices, and giving you a job ID link to view details.

5. Click **OK**.

The Manage Configuration Files page reappears, displaying the backup files. If you display the data in tabular form, the page shows the following headers:

- Config File Name—This is the device name with .conf file ending.
- Device Name
- Latest Revision—This is always 1.
- Creation Date
- Last Updated Date

Click any header to reveal the down arrow, which you can click to choose the mode of sorting, or adding or deleting column headers.

- Related Documentation**
- [Managing Configuration Files Overview on page 326](#)
 - [Deleting Configuration Files on page 330](#)
 - [Restoring Configuration Files on page 331](#)
 - [Comparing Configuration Files on page 332](#)
 - [Editing Configuration Files on page 334](#)
 - [Exporting Configuration Files on page 336](#)
 - [Tagging, Viewing Tags, and Untagging Configuration Files on page 337](#)
 - [Viewing Audit Logs on page 359](#)

Deleting Configuration Files

This topic gives the procedure for deleting device configuration files from Junos Space.

To delete a configuration file, do the following:

1. In Network Application Platform, navigate to **Config Files > Manage Config Files**.

The Manage Configuration Files page displays all the configuration files saved in Junos Space.

2. Select the check box of a configuration file and select **Delete** from the Actions Drawer.

A message appears, asking you to confirm deletion.

3. Click **Delete**.

The Manage Configuration Files page reappears, displaying any remaining configuration files.

- Related Documentation**
- [Managing Configuration Files Overview on page 326](#)
 - [Restoring Configuration Files on page 331](#)
 - [Comparing Configuration Files on page 332](#)
 - [Editing Configuration Files on page 334](#)
 - [Exporting Configuration Files on page 336](#)
 - [Tagging, Viewing Tags, and Untagging Configuration Files on page 337](#)

Restoring Configuration Files

Restoring a configuration file means either merging the contents of a configuration file on Junos Space with the existing configuration on the device, or overriding the device's running configuration with a candidate configuration (a configuration file edited in the Config Files workspace) or a backup from Junos Space.

A restore action generates an audit log entry.

To restore a device configuration file from Junos Space to a device,

1. Navigate to **Config Files > Manage Config Files**.
2. Select the device whose configuration you want to restore. (To restore all of them, in the tabular view, select the check box in the column header next to **Config File Name**.)

The **Restore Config File(s)** dialog box appears, displaying the name of the selected file, the name of the device, the version which is to be restored to the device, and the type of restore. By default, the latest version will be merged.

3. Select the appropriate version from the dropdown list that appears when you click next to the version number displayed in the **Versions** column.
4. Select the appropriate type of restore from the dropdown list that appears when you click next to the term displayed in the **Type** column.
5. You can either restore immediately or schedule the restoration for a later time.
 - Immediately—Click **Restore**.
 - Schedule at a Later Time
 - a. Select the check box next to the **Schedule at a Later Time** label or click the arrow next to the **Schedule at a Later Time** label to display the corresponding fields.
 - b. Select a date from the field on the left, and a time from the field on the right. The time zone displays to the right of the time field. The time zone is set on and for the Junos Space server.
 - c. Click **Restore**.

The **Restore Configuration Files** dialog box appears, announcing the successful scheduling of the restoration, and presenting a link to the job ID so that you can view details.

A successful restore action will be indicated by the word Success in the status column of the Job Manager. If a device cannot be reached, it will be skipped over, and the job status will indicate failure.

6. Click **OK** to dismiss the dialog box.
7. (Optional) Verify your work either by double-clicking the configuration file name on the Manage Configuration Files page, or by doing another backup, then comparing versions (see [“Comparing Configuration Files” on page 332](#)).

Related Documentation

- [Managing Configuration Files Overview on page 326](#)
- [Deleting Configuration Files on page 330](#)
- [Comparing Configuration Files on page 332](#)
- [Editing Configuration Files on page 334](#)
- [Exporting Configuration Files on page 336](#)
- [Tagging, Viewing Tags, and Untagging Configuration Files on page 337](#)
- [Viewing Audit Logs on page 359](#)

Comparing Configuration Files

The Compare feature enables you to view entire device configurations side by side, the total number of diffs run, the date and time of the last commit, and the number of changes made. Using the Compare feature does not generate an audit log entry.

You can compare the following:

- The configuration file of one device to the configuration file of another device. By default, the latest versions are compared.
- Two versions of the same configuration file. The default comparison is between the latest version and the previous version.
- An earlier version of the configuration file of one device with a later version of the configuration file of another device.

Any choices other than those listed above will result in a grayed-out menu.

To compare device configuration files in Junos Space, follow this procedure:

1. In Network Application Platform, navigate to **Config Files > Manage Config Files**.

The Manage Configuration Files page appears, displaying all the configuration files managed by Junos Space.

2. Select one of the configuration file you want to compare.
3. Select **Compare Config File Versions** from the Actions drawer.

The Compare Config Files dialog box appears.

4. For the source, select a configuration file from the Source config file list and a version from the Version list.

For the target, select a configuration file from the Target config file list and a version from the **Version** list.

Click **Compare**.

The Compare Config Files dialog box displays the two configuration files side by side, with their file names and their versions in a dark gray bar underneath the legend at the top of the page. The legend references the following:

- Total diffs—Black text is content common to both files
- Source—Content in the file on the left that is not contained in the file on the right.
- Target—Content in the file on the right that is not contained in the file on the left.
- Changed—Hot pink text is content unique to its respective file.

The status bar shows the current page number and the total number of pages. It also provides controls for moving from page to page and for refreshing the display.

The date and time of the last commit is shown in hot pink.



NOTE: The Compare function sets each configuration parameter in one file or version side by side with the same parameter in the other. This may lead to multiple pages of configuration for a single parameter in one file, whereas the same parameter in the other file may be only a couple of lines.

5. (Optional) To locate differences in configuration, click **Prev Diff** or **Next Diff**.
6. To finish viewing a comparison, click **Close** at the bottom of the page.

Related Documentation

- [Managing Configuration Files Overview on page 326](#)
- [Deleting Configuration Files on page 330](#)
- [Restoring Configuration Files on page 331](#)
- [Editing Configuration Files on page 334](#)
- [Exporting Configuration Files on page 336](#)
- [Tagging, Viewing Tags, and Untagging Configuration Files on page 337](#)

Editing Configuration Files

This action enables a very advanced user to edit the configuration file of the selected device in a text editor. It is therefore very different from the Device Configuration Editor available as an Action in the Devices workspace (**Network Application Platform > Devices > Manage Devices**). See [“Editing Device Configuration Overview” on page 68](#)). The Edit Config Files action in the Config Files workspace has no validation and no sanity check.

Editing a configuration file generates an audit log entry (see [“Viewing Audit Logs” on page 359](#)); however, unlike configuration files edited in the Devices workspace, files edited in the Config Files workspace are not saved as change requests, instead, they are saved as versions.

To edit a configuration file using the Edit Config File action in the Config Files workspace:



NOTE: This facility neither validates your work, nor submits it to a sanity check. To get those features, use the Edit Device Configuration action in the Devices workspace.

1. In Network Application Platform, navigate to **Config Files > Manage Config Files** and select the device whose configuration you want to edit.

If no configuration files are displayed on the page, you must first back up the discovered devices (see [“Backing Up Configuration Files” on page 328](#)).

2. Select **Edit Config File** from the Actions drawer.

The Edit Config File page appears. It displays the name of the file you selected, the time at which the file was created, the version, and the contents.

3. Select a version to use as a baseline from the **Version** list.

A version can be either a backup of a device configuration, or an edited copy of that initial backup. For an explanation of versioning in this context, see [“Backing Up Configuration Files” on page 328](#).)

The selected version appears in the text editor. Note that there are usually both vertical and horizontal scroll bars, and that a configuration usually has multiple pages. The status bar at the bottom displays the page you are on and the total number of pages. It also holds paging controls and a Refresh icon.

For ease of orientation, the pagination of the configuration file remains the same, even if you add or remove large quantities of text. The parameters that were on page 5 when you began editing are still on page 5 when you finish.

4. (Optional) To find a specific parameter, go through the file page by page. The browser's Search function does not work in the text editor.
5. Enter your changes, using the Copy/Paste function if required.



NOTE: Do not click **Modify** until you have finished editing.

6. (Optional) List the changes you have made (or anything else) in the Comments field. You cannot create a comment unless you have made changes. It is advisable to enter something in this field to distinguish the current version from a backup taken from the device itself.

7. When finished making all changes, click **Modify**

The Manage Configuration Files page reappears, displaying the edited configuration file still selected.

8. (Optional) Verify your work by double-clicking the device from the Manage Configuration Files page.

A dialog box appears, displaying the file in a non-editable format. You can select the version from the dropdown list. By default, the edited version appears.

Here again, the pagination, Comments area, and controls are the same as they are in the text editor you used to make your changes.

Alternatively, you could compare versions of the file (see [“Comparing Configuration Files” on page 332](#)).

To deploy the edited configuration file, you must use the Restore action (see [“Restoring Configuration Files” on page 331](#)).

Related Documentation

- [Managing Configuration Files Overview on page 326](#)
- [Deleting Configuration Files on page 330](#)
- [Restoring Configuration Files on page 331](#)
- [Comparing Configuration Files on page 332](#)
- [Exporting Configuration Files on page 336](#)
- [Tagging, Viewing Tags, and Untagging Configuration Files on page 337](#)
- [Viewing Audit Logs on page 359](#)

Exporting Configuration Files

The Export action enables you to save one or more configuration files to a zip file on your local computer.



NOTE: Your browser security settings must be set to allow downloads. If the browser interrupts the download with a warning and then tries to restart the download by refreshing, the export will be aborted, and the zip file removed.

Exporting a configuration file generates an audit log entry.

To export a configuration file to a zip file,

1. Navigate to **Config Files > Manage Config Files** and select one or more configuration files.
2. Select **Compare Config File Versions** from the Actions drawer.

The Export Config File(s) dialog box opens, displaying the name of the file, the device name, and the configuration file versions stored. By default, the latest version is selected.

3. Select the appropriate version from the dropdown list that appears when you click next to the version number displayed in the Versions column.
4. Click **Export**.

The Generating ZIP archive dialog box appears, displaying a progress bar showing when the zip file is ready for downloading, at which point, the Opening deviceConfigFiles.zip dialog box opens.

5. Save the zip file to your computer before closing the progress bar or the OpeningdeviceConfigFiles.zip dialog box, because the generated zip file is removed from the server immediately after the download is complete, or when either of these two dialog box is closed. Refreshing or exiting the browser will also remove the zip file from the server.

Related Documentation

- [Managing Configuration Files Overview on page 326](#)
- [Deleting Configuration Files on page 330](#)
- [Restoring Configuration Files on page 331](#)
- [Comparing Configuration Files on page 332](#)
- [Editing Configuration Files on page 334](#)
- [Tagging, Viewing Tags, and Untagging Configuration Files on page 337](#)
- [Viewing Audit Logs on page 359](#)

Tagging, Viewing Tags, and Untagging Configuration Files

- To tag configuration files, consult [“Tagging an Object” on page 495](#).
- To view tags on configuration files, consult [“Viewing Tags” on page 496](#).
- To untag configuration files, consult [“Untagging Objects” on page 497](#).

Related Documentation

- [Managing Configuration Files Overview on page 326](#)
- [Managing Tags Overview on page 491](#)
- [Managing Tags on page 492](#)
- [Filtering Inventory Using Tags on page 497](#)
- [Creating a Tag on page 498](#)

User Privileges in Configuration File Management

In Junos Space Users, there is a predefined role for configuration file management: Configuration File Manager. That predefined role enables the users to which it has been assigned the permission to :

- Backup Config Files
- Delete Config Files
- Restore Config Files
- Compare Config Files
- Export Config Files

If you want to restrict the Configuration File Manager's permissions to anything less than the full set listed above, you can create a role in the Config Files application workspace and assign the permissions specifically for each list item.

Related Documentation

- [Role-Based Access Control Overview on page 371](#)
- [Managing Configuration Files Overview on page 326](#)

PART 7

Job Management

- [Overview on page 341](#)
- [Administration on page 345](#)

Overview

- [Job Management Overview on page 341](#)

Job Management Overview

The Job Management workspace lets you monitor the status of all jobs that have been run in all Junos Space applications. A job is a user-initiated action that is performed on a Junos Space object, such as a device, service, or customer. All scheduled jobs can be monitored.

Typical jobs in Junos Space include device discovery, deploying services, prestaging devices, and performing functional and configuration audits. Jobs can be scheduled to occur immediately or in the future. For all jobs scheduled in Junos Space, you can view job status from the **Jobs** workspace. Junos Space maintains a history of job status for all scheduled jobs. When a job is scheduled from a workspace, Junos Space assigns a job ID that serves to identify the job (along with the job type) in the Manage Jobs inventory page.

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

- View status of all scheduled, running, canceled, and completed jobs
- Retrieve details about the execution of a specific job
- View statistics about average execution times for jobs, types of jobs that are run, and success rate
- Cancel a scheduled job or in-progress job (when the job has stalled and is preventing other jobs from starting)

Junos Space 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 software release. Job types are subject to change based on the licensed application in your Junos Space software release.

Table 46: Junos Space Job Types Per Application

Junos Space Application	Supported Job Types
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 347](#)
 - [Viewing Statistics for Scheduled Jobs on page 350](#)
 - [Canceling a Job on page 352](#)

CHAPTER 29

Administration

- [Viewing Your Jobs on page 345](#)
- [Viewing Scheduled Jobs on page 347](#)
- [Viewing Statistics for Scheduled Jobs on page 350](#)
- [Canceling a Job on page 352](#)
- [Viewing Job Recurrence on page 353](#)

Viewing Your Jobs

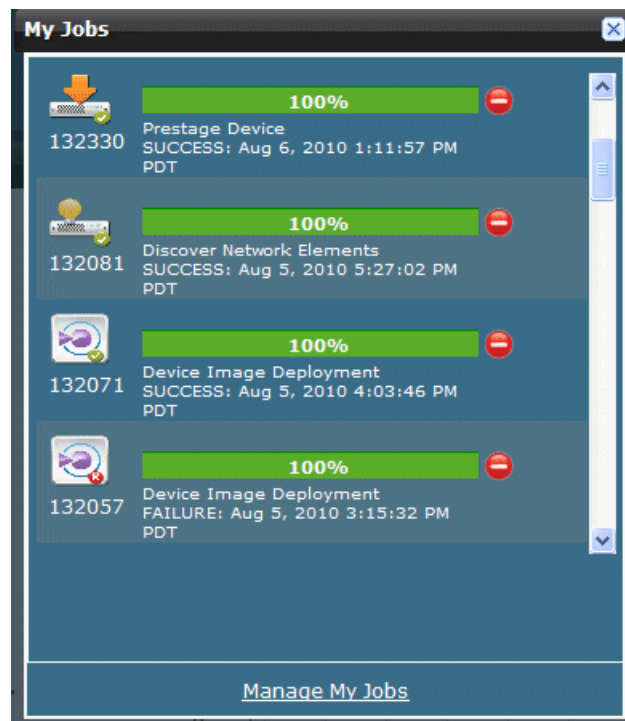
You can view all your completed, in-progress, and scheduled jobs in Junos Space. You can quickly access summary and detailed information about all your jobs, from any work space and from any task you are currently performing. You can also clear jobs from your list when jobs are no longer of interest to you.

To view the jobs that you have initiated:

1. In the banner of the Junos Space user interface, click the My Jobs icon.

The My Jobs report appears, as shown in the following example.

Figure 129: My Jobs Report



NOTE: The My Jobs report displays your 25 most recent jobs.

- To view jobs details, select one or more jobs in the My Jobs report and click **Manage My Jobs**.

The Manage Jobs inventory page displays a listing of all jobs that you initiated.

- To remove jobs from the My Jobs report:
 - To remove a job, click the Clear job icon that appears to the right of the job.



NOTE: Clearing a job from the My Jobs report does not affect the job itself, but only updates the My Jobs view.

Related Documentation

- [Viewing Statistics for Scheduled Jobs on page 350](#)
- [Canceling a Job on page 352](#)
- [Job Management Overview on page 341](#)

Viewing Scheduled Jobs

The Manage Jobs inventory page displays all jobs that have been scheduled to run or have run from each Junos Space application.

- [Changing the View on page 347](#)
- [Viewing Job Types on page 348](#)
- [Viewing Job Status Indicators on page 348](#)
- [Viewing Job Details, Status, and Results on page 349](#)
- [Performing Manage Jobs Commands on page 350](#)

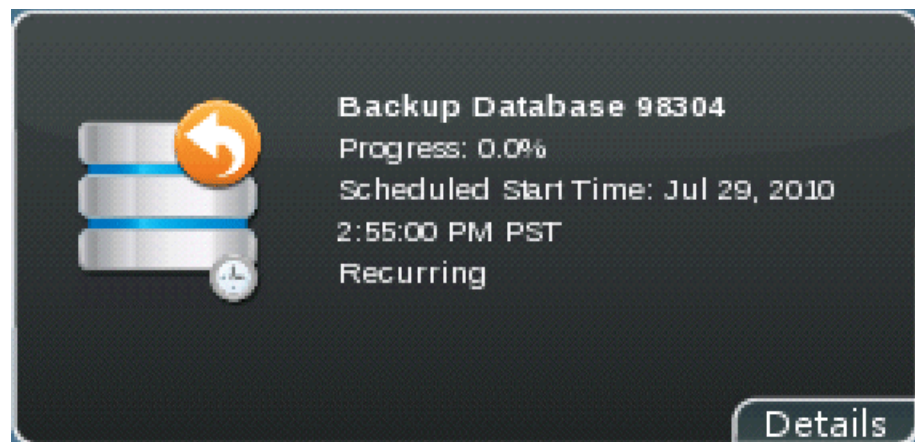
Changing the View

You can display jobs in two views: thumbnail and tabular. By default, Jobs appear on the page in thumbnail view.

In thumbnail view, jobs appear as icons listed in descending order by job ID. Each job has a title and job ID. To see more detailed job information, status, or results, double-click a job icon or move the zoom slider to the far right. The default zoom slider position is in the middle.



NOTE: A recurring database job appears as follows:



In tabular view, jobs appear in a table sorted by scheduled start time by default. Each job is a row in the Manage Jobs table.



NOTE: A recurring database backup job provides the following information in the Recurrence column of the Manage Jobs table.

Recurrence
Every 1 hour Starts: Jul 29, 2010 2:55:00 PM PST Ends by: Jul 29, 2010 9:55:00 PM PST

To change views:

- Click a view indicator at the right in the Manage Jobs page title bar.

Viewing Job Types

Job types tell you what tasks or operations have been performed throughout Junos Space applications. Each Junos Space application supports certain job types. You can search for a particular job type. You can also sort by job type in tabular view. For more information about how to manipulate inventory page data, see [“Inventory Pages Overview” on page 28](#).

To view job types:

- In thumbnail view, see the job icon and the job title. You can also mouse over a job icon to see its title.
- In tabular view, the job type appears as a column in the table. You can sort by

Viewing Job Status Indicators

Each job icon on the Manage Jobs inventory page in thumbnail view has a job status indicator. [Table 47 on page 348](#) defines each job status indicator.

Table 47: Job Icon Status Indicators






Job Status Indicator	Description
	The job completed successfully.
	The job failed.
	The job was canceled by a user.

Table 47: Job Icon Status Indicators (*continued*)

	The job is scheduled.
	The job is in progress. You can only cancel jobs that are in progress from the Actions drawer.

Viewing Job Details, Status, and Results

Job details display all of the information that is stored about a job. You can also view job status and results.

To view job status, results, or details:

- Double-click a job icon in thumbnail view or double-click a row in the table in tabular view.
- Move the zoom slider to the far right in thumbnail view.

[Table 48 on page 349](#) defines job information. All job information appears in the Job Details dialog, but not all of it appears in the Manage Jobs table. If a column is common to every job, for example, State and Percent, then it appears in both. But, if it's specific to each type of job, for example for Backup Database (Backup Date, Machine, and File Path), then it only appears in job details. Although the Details column for this job in Manage Jobs might show a subset of that information.

Table 48: Job Details and Columns in the Manage Jobs Table

Field	Description
Name	For most jobs, the name is the Job Type with the timestamp (in milliseconds) appended. However, for service-related jobs (Deploy Service, Decommission, Configuration Audit, and Functional Audit) jobs, the job name is supplied by the user as part of the workflow.
Backup Date	Date you backed up the database.
Comment	An optional descriptive note that describes or otherwise identifies the backup operation.
Machine	Name of the Junos Space server from which database backup occurred.
File Path	The pathname to the database backup file.
Percent	Percentage of job that has completed.
State	State of job execution: <ul style="list-style-type: none"> • SUCCESS—Job completed successfully • FAILURE—Job failed and was terminated. • IN PROGRESS—Job is in progress. • CANCELED—Job was canceled by a user.
Job Type	The supported job types. Job types depend on the installed Junos Space applications.

Table 48: Job Details and Columns in the Manage Jobs Table (*continued*)

Job ID	The numerical ID of the job.
Summary	The operations executed for the job.
Scheduled Start Time	The scheduled start time for the job (specified by a Junos Space user).
Scheduled Start Time (not displayed in default view)	Time when Junos Space begins execution of the job. In most cases, actual start time should be the same as the scheduled start time.
User	The log in username.
End Time (not displayed in default view)	Time that the job completed or was terminated, if job execution failed.

Performing Manage Jobs Commands

You can perform the following commands from the Manage Jobs Actions drawer:

- **Cancel Job**—Stop a scheduled job. See [“Canceling a Job” on page 352](#).
- **Delete Database Backup**—Delete a backup database backup file in the Manage Jobs inventory. See [“Deleting Database Backup Files” on page 443](#).
- **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 to view all occurrences of the schedule. See [“Viewing Job Recurrence” on page 353](#).
- **Tag It**—Apply a tag to a job to segregate, filter, and categorize jobs. See [“Tagging an Object” on page 495](#).
- **View Tags**—View tags applied to a job. See [“Viewing Tags” on page 496](#).
- **Untag It**—Remove a tag from a job. See [“Untagging Objects” on page 497](#).

Related Documentation

- [Viewing Statistics for Scheduled Jobs on page 350](#)
- [Job Management Overview on page 341](#)
- [Canceling a Job on page 352](#)

Viewing Statistics for Scheduled Jobs

The Platform Job Management 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 351](#)
- [Viewing the State of Jobs That Have Run on page 351](#)
- [Viewing Average Execution Times for Jobs on page 352](#)

Viewing the Types of Jobs That Are Run

Viewing Job Types—The Job Types pie chart displays the percentage of all Junos Space jobs that run of a particular type. Each slice in the pie chart represents a job type and the percentage of time a job type was run. The job type legend appears to the right identifying the job type titles according to colors. Scroll down the list to see all of the job types. The number of jobs that appear in the job types legend depend on the number of jobs that have run in all Junos Space applications. Mousing over a slice in the pie chart displays the job type title and the number of jobs that have run.

Viewing Job Types Details—Clicking a job type in the Job Types pie chart displays only those job types filtered on the Manage Jobs inventory landing page. For more information about the Manage Jobs page, see [“Viewing Scheduled Jobs” on page 347](#). The selected job types display in thumbnail view. Click **More** in the thumbnail displays that job's status by device name, IP address, job status, and description. Move the details slider at the top right of the Manage Jobs page to the far right or change to tabular view to see the job details data fields: percentage complete, state, job type, job ID summary selected start time, and user name.

To view all the data fields available for a job in Manage Jobs in tabular view:

1. Select the down arrow in a column heading to reveal sort and column selection options.
2. Select **Columns**. The Columns cascading menu appears. You see all of the possible job data fields to show or hide. Checked jobs columns appear on the Manage Jobs table. Job columns that are not checked are hidden and do not appear in the table.

Viewing the State of Jobs That Have Run

Viewing the Job State—The State of Jobs Run pie chart graphically displays the percentage of jobs that have either succeeded or failed. Mouse over the pie chart to see the number of jobs that have succeeded or failed.

Viewing Job State Details—Clicking a slice in the State of Jobs Run pie chart displays only those jobs that have either succeeded or failed filtered on the Manage Jobs page in thumbnail view. For more information about the Manage Jobs page, see [“Viewing Scheduled Jobs” on page 347](#). The selected job types display in thumbnail view. Click **More** in the thumbnail displays that job's status by device name, IP address, job status, and description. Move the details slider at the top right of the Manage Jobs page to the far right or change to tabular view to see the job details data fields: percentage complete, state, job type, job ID summary selected start time, and user name.

To view all the data fields available for a job in Manage Jobs in tabular view:

1. Select the down arrow in a column heading to reveal sort and column selection options.
2. Select **Columns**. The Columns cascading menu appears. You see all of the possible job data fields to show or hide. Checked jobs columns appear on the Manage Jobs table. Job columns that are not checked are hidden and do not appear in the table.

Viewing Average Execution Times for Jobs

Viewing the Average Execution Time per Completed Job—Each bar in the Average Execution Time per Completed Job bar chart represents a job type and the average execution time in seconds. Depending on the size of the Average Execution Time per Completed Job bar chart is on the Job Management statistics page, the name of the job type displays at the bottom of each bar.

Viewing Completed Job Details—Clicking a bar in the Average Execution Time per Completed Job bar chart displays only those jobs that have been executed on the Manage Jobs inventory page in thumbnail view. For more information about the Manage Jobs page, see “[Viewing Scheduled Jobs](#)” on page 347. The selected job types display in thumbnail view. Click **More** in the thumbnail displays that job’s status by device name, IP address, job status, and description. Move the details slider at the top right of the Manage Jobs page to the far right or change to tabular view to see the job details data fields: percentage complete, state, job type, job ID summary selected start time, and user name.

To view all the data fields available for a job in Manage Jobs in tabular view:

1. Select the down arrow in a column heading to reveal sort and column selection options.
2. Select **Columns**. The Columns cascading menu appears. You see all of the possible job data fields to show or hide. Checked jobs columns appear on the Manage Jobs table. Job columns that are not checked are hidden and do not appear in the table.

Related Documentation

- [Viewing Scheduled Jobs on page 347](#)
- [Job Management Overview on page 341](#)
- [Inventory Pages Overview on page 28](#)

Canceling a Job

From the Platform Job Management inventory page you can cancel jobs that:

- Are scheduled, but that you don’t want to run.
- Are in progress that are hanging or incapable of completing, and are preventing other jobs from starting.



NOTE: If Junos Space determines that the job operation is non-interruptible, the job runs to completion; otherwise the job is cancelled.



NOTE: Junos Space performs no cleanup on cancelled jobs.

To cancel a job:

1. From the navigation ribbon, navigate to Platform > Job Management > Manage Jobs. The Manage Jobs inventory page appears.
2. Select the job that you want to cancel.
3. Mouse over the Actions drawer to open it.
4. Select **Cancel Job**. When the Cancel Job operation completes, the inventory page displays the Job State CANCELLED. If a job is in a state that you can not cancel, The Cancel Job command is disabled in the Action drawer menu.

Related Documentation

- [Viewing Statistics for Scheduled Jobs on page 350](#)
- [Job Management Overview on page 341](#)
- [Viewing Scheduled Jobs on page 347](#)
- [Inventory Pages Overview on page 28](#)
- [Viewing Your Jobs on page 345](#)

Viewing Job Recurrence

You can view information about when a job recurs. For example, in Junos Space release 1.4, you can view the recurrence of a database backup job.

To view job recurrence information:

1. Navigate to **Platform > Administration > Manage Database**.
The Manage Database inventory 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**.

Related Documentation

- [Backing Up the Database on page 433](#)
- [Viewing Scheduled Jobs on page 347](#)
- [Viewing Audit Logs on page 359](#)

PART 8

Audit Logs

- [Overview on page 357](#)
- [Administration on page 359](#)

Overview

- [Junos Space Audit Logs Overview on page 357](#)

Junos Space Audit Logs Overview

Audit logs provide a record of Junos Space login history and user-initiated tasks that are performed from the user interface. From the Audit Logs workspace, you can monitor user login/logout activity over time, track device management tasks, view services that were provisioned on devices, and so forth. Junos Space audit logging does not record non-user initiated activities, such as device driven activities, and is not designed for debugging purposes. User-initiated changes made from the Junos Space CLI are logged but are not recorded as audit logs.

Administrators can sort and filter on audit logs to determine which users performed what actions on what objects at what time. For example, an Audit Log administrator can use audit log filtering to track the user accounts that were added on a specific date, track configuration changes across a particular type of device, view services that were provisioned on specific devices, or monitor user login/logout activity over time.

To use the audit log service to monitor user requests and track changes initiated by users, you must have the Audit Log Administrator role (see [“Managing Roles Overview” on page 393](#)).



NOTE: Audit Logging is not currently supported for Ethernet Design.

Over time, the Audit Log administrator will archive a large volume of Junos Space log entries. Such log entries might or might not be reviewed, but they must be retained for a period of time. The Archive Purge feature helps you manage your Junos Space log volume, allowing you to archive log files and then purge those log files from the Junos Space 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 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 364](#)
- [Viewing Audit Logs on page 359](#)
- [Exporting Audit Logs on page 367](#)

Administration

- [Viewing Audit Logs on page 359](#)
- [Viewing Audit Log Statistics on page 361](#)
- [Converting the Audit Log File UTC Timestamp to Local Time in Microsoft Excel on page 363](#)
- [Archiving and Purging Audit Logs on page 364](#)
- [Exporting Audit Logs on page 367](#)

Viewing Audit Logs

Audit logs are generated for login activity and tasks that are initiated from the Network Application Platform and Network Activate. The View Audit Logs page displays all tasks.

To view audit logs, you must have Audit Log Administrator privileges.



NOTE: Audit Logging is not currently supported by the Ethernet Design application.

You view audit logs in Junos Space only in tabular view. For more information about how to manipulate inventory page data, see [“Inventory Pages Overview” on page 28](#).

Viewing Audit Log Details

The Audit Log Details dialog box displays information about the task that was logged, including information about the objects affected by the task.

To view detailed audit log information:

- If an audit log entry does not include a job ID, double-click a table row for the audit log entry. The Audit Log Details dialog box displays information about the task that was logged, including information about the objects affected by the task. Click **OK** to close the Audit Log Detail dialog box.
- If an audit log entry includes a Job ID, click the Job ID link in the audit log row. The Job Manager Inventory view displays information about the job. If this job is recurring, then it will display information about all recurrences of this job. Click **Return to Audit Logs** to close the Job Manager inventory page and return to the audit logs table.

The fields displayed in the Audit Logs table are described in [Table 49 on page 360](#).

Table 49: Detailed Audit Logs Information and View Audit Log Table Columns

Field	Description
User Name	The login ID of the user that initiated the task.
User IP	The IP address of the client computer from which the user initiated the task.
Task	The name of the task that triggered the audit log.
Timestamp	Time is UTC time in database that is mapped to the local time zone of client computer.
Result	<p>The execution result of the task that triggered the audit log:</p> <ul style="list-style-type: none"> • Success—Job completed successfully • Failure—Job failed and was terminated. • Job Scheduled—Job is scheduled but has not yet started.
Job ID	For each job-based task, the audit log includes the job ID.
Description	A description of the audit log.

For both recurring and non-recurring jobs, such as a database backup, the Audit Logs table displays the following data described in [Table 50 on page 360](#).

Table 50: Audit Log Table Details for Recurring and Non-recurring Jobs

Field	Description
Job ID	The numerical ID of the job.
Percent	Percentage of job that has completed.
State	<p>State of job execution:</p> <ul style="list-style-type: none"> • SUCCESS—Job completed successfully • FAILURE—Job failed and was terminated. • IN PROGRESS—Job is in progress. • CANCELED—Job was canceled by a user.
Job Type	The supported job types. Job types depend on the installed Junos Space applications. In Junos Space 1.4, a recurring job type supported is Backup Database.
Summary	The operations executed for the job.
Scheduled Start Time	The scheduled start time for the job (specified by a Junos Space user).
Recurrence	The job recurrence interval, start time, and end time.

- Related Documentation**
- [Exporting Audit Logs on page 367](#)
 - [Viewing Audit Log Statistics on page 361](#)
 - [Junos Space Audit Logs Overview on page 357](#)
 - [Archiving and Purging Audit Logs on page 364](#)
 - [Inventory Pages Overview on page 28](#)
 - [Backing Up the Database on page 433](#)

Viewing Audit Log Statistics

The Audit log workspace statistics page provides two graphs: Audit Log Statistical Graph pie chart and the Top 10 Active Users in 24 Hours for the audit log administrator to monitor Junos Space tasks.

The Audit Log Statistical Graph pie chart displays all tasks that have been performed and logged in all Junos Space applications over a specific period of time. You can view Audit Log statistics by task type, user, workspace, and application.



NOTE: Audit Logging is not currently supported by the Ethernet Design application.

The Top 10 Active Users in 24 hours graph displays the top 10 Junos Space users who have performed the most tasks over 24 hours. The graph X axis represents the activities performed by a single user. Each active session for that user is represented by a bubble on the X axis. The graph Y axis represents hours. For example, if a single user performed six active sessions during the last 24 hours, the chart displays six bubbles on the X axis according to the hours on the Y axis.

Viewing the Dynamic Audit Log Statistical Graph

The Audit Log Statistical Graph is an interactive graph that allows the audit log administrator to view audit logs by selecting both category and time frame. The category determines the statistical graph that displays—task, user, workarea, or application. Each slice in the pie represents a task and its usage percentage of the whole. The tasks types also appear in a list box at the right of the pie chart. Mousing over a slice of the pie displays the number of times the task is invoked. The time frame specifies the period of time within which to show audit log data.

To use the Audit Log Statistical Graph:

1. Select a graph category:

- Task—shows all tasks that have been performed. Click each task slice to go to the next level chart showing the users who performed the selected task.

The graph path displays the path to show where you are located in the UI. Click Overview to go back to the top level chart. The task name in the path indicates the currently selected path.

Tasks display in terms of user name or IP address.

- User names display all users by name. Click a user to go to the inventory page filtered by task, user, and selected time frame.
 - IP address displays all IP address where users performed tasks. Click an IP address to go to the inventory page filtered by task, IP address, and selected time frame.
 - Users displays all users using the system within the time frame. 10 users display per chart. Click Others to go to the next page. Click the previous page link to go back.
 - Workspace displays all workspaces used in the time frame. Click a workspace slice to go to the inventory page filtered by workspaces.
 - Application displays all applications used. Click a pie slice to go to the inventory page filtered by application and selected time frame.
2. Select a time frame in days, weeks, or months to display audit log data in the pie chart. The default is Days. A time selection description displays just below the time frame area.
 - Days—Days mode displays the past seven days to the selected date. Select single or multiple days. Select multiple days by dragging the mouse
 - Weeks—Weeks mode displays the past five weeks, from past to most current on the right.
 - Months—Months mode displays the past 12 month, from past to most current on the right.

The current day, week, or month is highlighted.

3. Click a slice in the pie chart to view more detailed information. Tasks appear in tabular view by user name, user IP, task, timestamp, results, description, job ID, and level 2 description.

See [“Inventory Pages Overview” on page 28](#) for more information about manipulating the table data.

4. On the inventory page, click an audit log to view more detailed information. For a job-related log entry, there is a column for job-id, by clicking this link you will be led to a new table showing the corresponding Job info.

In the audit log detail view, if there are multiple affected objects for the log entry, the affected object detail always shows the first object detail. Clicking on any object in the list changes the object detail accordingly. If there is no affected object for this log entry, the affected object list is hidden and the object detail part is shown none.

5. Click Return to Audit Logs to go back to Audit Log View.

Viewing the Top 10 Active Users In 24 Hours Statistics

To view the Top 10 Active Users in 24 Hours graph:

1. In the Top 10 Active Users in 24 Hours graph, double-click a user’s bubble for a particular hour. The View Audit Log page appears with the jobs performed by that user.

Tasks appear by user name, user IP, task , timestamp, results, description, job ID, and level 2 description in tabular view. See [“Inventory Pages Overview” on page 28](#) for more information about manipulating the table data.

Related Documentation

- [Viewing Audit Logs on page 359](#)
- [Junos Space Audit Logs Overview on page 357](#)
- [Inventory Pages Overview on page 28](#)
- [Archiving and Purging Audit Logs on page 364](#)
- [Exporting Audit Logs on page 367](#)

Converting the Audit Log File UTC Timestamp to Local Time in Microsoft Excel

You can unzip an audit log *.gz file. You can open the extracted *.csv file as a spreadsheet in Microsoft Excel. In Microsoft Excel, you can convert the Coordinated Universal Time (UTC) timestamp column entries to local time.

To convert the UTC time to local time:

1. Retrieve the `JunosSpaceAuditLog_date_time_id.csv.gz` audit log file from where you archived it. If you archived the file locally, the file is located in `/var/lib/mysql/archive`.
 - Where *date* specifies the year, month, and day, in yyyy-mm-dd format
 - Where *time* specifies military, 24-hour time in hour, minutes, and seconds (hh-mm-ss) format
 - Where *id* is an auto-generated, 13-character random number that uniquely identifies each audit log archive file

For example, `JunosSpaceAuditLog_2010-03-04-00-00-00_xx...x.csv.gz`.

2. Unzip the audit log `*.csv` file.
3. Open the audit log `*.csv` file in Microsoft Excel.
4. To the left of the UTC Time column, insert a new column.
5. Label the column header **Local Time**.
6. Click the first cell of the new column.
7. Insert the following function: `=XX/ 86400000 + 25569 - X/24`
 - Where XX is the cell letter and row number where you want to insert the local time conversion function.
 - Where X represents the hours difference between your local time and the UTC time; divided by 24 hours.
8. Click Enter. The calculated local time appears.
9. Format the local time. Right-click the cell and select **Format Cells**. The Format Cells dialog box appears.
10. In the Category list box, select **Date**.
11. In the Type list box, select a date format that you want.
12. Click OK. The local time and date appears.
13. Copy or apply the cell function and formatting to the rest of the rows in the Local Time column. The rest of the local times appear as shown.

	A	B	C	D	E	F	G	H	I	J
1	ID	Version	Timestamp	Local Time	UTC Time	User IP	Application	Task	Result	Correlation Tag
2	1900817	0	1.26971E+12	3/27/10 12:58	40264.70696	10.150.113.211	Network Application Platform	Archive/Purge	Job Scheduled	81E07BEDEF597C8CA5ECCEB14347FA29
3	1900821	0	1.26971E+12	3/27/10 13:14	40264.71815	10.150.113.211	Network Application Platform	Logout	Success	\N
4	1966342	0	1.26971E+12	3/27/10 13:24	40264.72546	10.150.113.211	Network Application Platform	Login	Success	\N
5										

14. If you want to keep the original audit log file, save it as a different filename.

Related Documentation

- [Archiving and Purging Audit Logs on page 364](#)

Archiving and Purging Audit Logs

The administrator can archive and then purge all audit logs files up to a specified data and time from the Junos Space database. The administrator can archive audit logs to the local server or a remote server location.

The Junos Space archive file uses the following naming conventions:

`JunosSpaceAuditLog_date_time_id.csv.gz`, where *date* specifies the year, month, and day, in the format *yyyy-mm-dd*, *time* specifies hours, minutes, and seconds, in the format

hh-mm-ss, and *id* is a 13 character random number that uniquely identifies each audit log archive file.

This topic includes the following tasks:

- [Archiving Audit Logs To a Local Server and Purging the Database on page 365](#)
- [Archiving Audit Logs To a Remote Server and Purging the Database on page 366](#)

Archiving Audit Logs To a Local Server and Purging the Database

You can archive audit logs to the local server. The local server is the server that functions as the active node in the Junos Space fabric.

To archive Junos Space audit log files to the local server and then purge the audit logs from the database:

1. Navigate to Platform > View Audit Logs > Archive Purge. The Archive/Purge dialog box appears.
2. In the Archive Logs Before field, specify the date and time up which to archived and purged audit logs from the Junos Space database. You can only specify a date and time in the past.



NOTE: If you do not specify a date and time in the Archive Logs Before field, Junos Space archives then purges from the database all logs generated up to the time that you initiated the operation.

3. In the Archive Mode field, select **local** from the list.
4. Schedule the Junos Space Archive/Purge operation:
 - Clear the **Schedule at a later time** check box (the default) to initiate the Archive/Purge operation when you complete this procedure.
 - Select the **Schedule at a later time** check box to specify a later start date and time for the Archive/Purge operation.



NOTE: The selected time in the scheduler corresponds to Junos Space server time but using the local time zone of the client computer.

5. Click **Submit**.

The Audit Log Archive and Purge confirmation dialog box displays the audit log file name and the location where it will be saved.

6. Click **Continue** to archive and purge the audit logs.
7. To view job details for the Audit Log Archive/Purge operation, click on the Job Id in the Job Information dialog box; otherwise, click **OK** to close the dialog box.

Archiving Audit Logs To a Remote Server and Purging the Database

You can archive audit logs to remote network hosts or media.

To back up the Junos Space database to a remote host and then purge those logs from the Junos Space database:

1. Navigate to Platform > View Audit Logs > Archive Purge. The Archive/Purge dialog box appears.
2. In the Archive Logs Before field, select a date and time to specify the date *up to which* all audit logs are to be archived and then purged from the Junos Space database. You can only specify date and time in the past.



NOTE: If you do not specify a date and time in the Archive Logs Before field, Junos Space will archive and then purge from the database all logs generated up to the time that you initiated the operation.

3. In the Archive Mode field, select **Remote** from the list.
4. Enter a valid user name to access the remote host server.
5. Enter a valid password to access the remote host server.
6. Reenter the password you entered in the previous step.
7. Enter the IP address of the remote host server.
8. Enter a directory path on the remote host server for the archived log files.



NOTE: The directory path must already exist on the remote host server.

9. Schedule the Junos Space archive and purge operation:
 - Clear the **Schedule at a later time** check box (the default) to initiate the Archive/Purge operation when you complete this procedure.
 - Select the **Schedule at a later time** check box to specify a later start date and time for the Archive/Purge operation.



NOTE: The selected time in the scheduler corresponds to Junos Space server time but using the local time zone of the client computer.

10. Click **Submit**.

The Audit Log Archive and Purge dialog box displays the audit log file location and name and the remote server to which the files copy.

11. Click **Continue** to archive and purge the audit logs.

Junos Space displays the Audit Log Archive and Purge Job Information dialog box.

12. To view job details for the Archive/Purge operation, click the Job Id link.
13. Click **OK** to close the dialog box.

**Related
Documentation**

- [Junos Space Audit Logs Overview on page 357](#)
- [Viewing Audit Logs on page 359](#)
- [Exporting Audit Logs on page 367](#)

Exporting Audit Logs

You can export audit logs without purging them from the system.

There are three options for this:

- Export all audit logs
- Export audit logs filtered by date range
- Export audit logs as displayed on View Audit Logs table. On the View Audit Logs page, you can filter audit logs according to multiple criteria. The criteria you choose determine which audit log data will be exported. The filter determines which records appear in the table, and all the records in the table will be exported.

The audit logs are exported as CSV files. They are not removed from the database when they are exported.

1. Navigate to **Network Application Platform > View Audit Logs**.

The Audit Log Statistical Graph page appears.

2. From the Audit Log Statistical Graph page, select a time period and category: Task, User, Workspace, or Application.
3. Click the graph to view the filtered audit logs
4. Click the **Export** link at the top of the table and below the title bar.

The **Export Audit Log** page appears.

5. Select one of the following options and click **Export**.

- **Export all audit logs.**

The Date and Time selectors are disabled when you choose this option.

- **Export audit logs filtered by date range .**

The Date and Time widget selectors are enabled when you choose this option.

- **Export audit logs as displayed on View Audit Logs table**

This is the default selection. For instructions on how to filter the logs, see "[Viewing Audit Logs](#)" on page 359.

Your browser's Download dialog appears.

6. You can choose to open the exported file or to save it.

- Related Documentation**
- [Junos Space Audit Logs Overview on page 357](#)
 - [Viewing Audit Log Statistics on page 361](#)
 - [Archiving and Purging Audit Logs on page 364](#)

PART 9

Users

- [Role-Based Access Control on page 371](#)
- [User Accounts on page 381](#)
- [User Roles on page 393](#)

CHAPTER 32

Role-Based Access Control

- [Role-Based Access Control Overview on page 371](#)
- [Understanding How to Configure Users to Manage Objects in Junos Space on page 372](#)
- [Predefined Administrator Roles on page 373](#)

Role-Based Access Control Overview

Junos Space 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, services, and customers in Junos Space.

To access and manage Junos Space, 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 workspace and is unable to perform tasks.

Authentication

Through authentication, Junos Space validates users based on password and other security services. Junos Space supports local user authentication only. Each user password is saved in the Junos Space database and is used to validate a user during login.

RBAC Enforcement

With role-based access control (RBAC) enforcement, a Junos Space super administrator or user administrator controls the workspaces a user can access, the system resources users can view and manage, and the tasks available to a user within a workspace. RBAC is enforced in the Junos Space user interface navigation hierarchy by workspace, task group, and task. A user can only access 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 that is assigned the Device Manager role, which grants access privileges to all tasks in the **Devices** workspace, can access only the **Devices** workspace. No other workspaces are visible to this user unless other roles are assigned to this user.

RBAC Enforcement Not Supported for Getting Started Page

RBAC enforcement is not enabled for the contents of the Getting Started page. Consequently, a user who does not have certain access privileges can still view the steps displayed in the Getting Started page. For example, a user without privileges to manage devices will still see the Discover Devices step. However, when the user clicks on the step, Junos Space 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

- [Understanding How to Configure Users to Manage Objects in Junos Space on page 372](#)
- [Managing Permission Labels Overview on page 499](#)
- [Predefined Administrator Roles on page 373](#)
- [Creating Users on page 381](#)
- [Viewing User Statistics on page 391](#)
- [Viewing Users on page 386](#)

Understanding How to Configure Users to Manage Objects in Junos Space

Junos Space is shipped with a super administrator privilege level that has full access to the Junos Space system. When you first log in to Junos Space as default super administrator, you can perform all tasks and access all Junos Space system resources. The super administrator can create new users and assign roles to those users to specify which workspaces and system resources users can access and manage, and which tasks users can perform within each workspace.

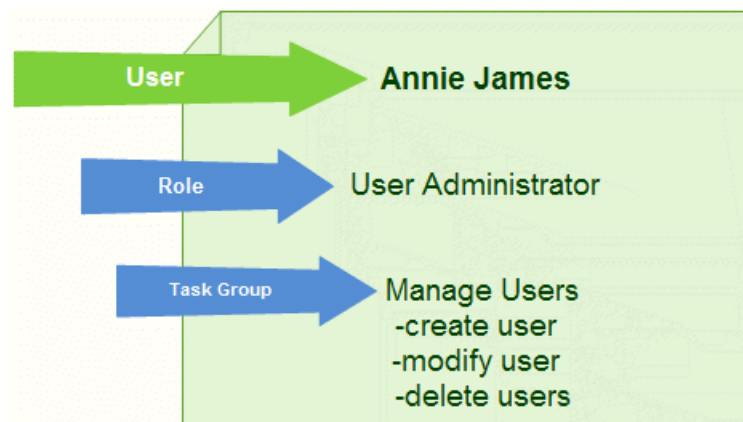
After you first set up Junos Space, you can disable the default super administrator user ID, if necessary. However, before doing so, you should first create another user with super administrator privileges.

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, services, customers) that Junos Space manages. For complete information on the predefined roles, see [“Predefined Administrator Roles” on page 373](#).

Users receive permission to perform tasks only through the roles that they are assigned. In most cases, a single role assignment enables a user to view and to perform tasks on the objects within a workspace. For example, a user assigned the Device Manager role can discover devices, resynchronize devices, view the physical inventory and interfaces for devices, and delete managed devices. A user that is assigned the User Administrator

role can create, modify, and delete other users in Junos Space, and assign and remove roles.

Typically a role contains one or more task groups. A *task group* provides a mechanism for grouping a set of related tasks that can be performed on a specific object. The following illustration shows the task group and associated tasks that are available to a user that is assigned the User Administrator role.



NOTE: You can assign multiple roles to a single user, and multiple users can be assigned the same role.

Related Documentation

- [Role-Based Access Control Overview on page 371](#)
- [Managing Permission Labels Overview on page 499](#)
- [Creating Users on page 381](#)
- [Viewing Users on page 386](#)
- [Viewing User Statistics on page 391](#)

Predefined Administrator Roles

Junos Space 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.



NOTE: The predefined roles that appear in the Junos Space release that you are using depend on the Junos Space applications that you have installed. For the most current predefined user roles, see the **Platform > Users > Manage Users > Create User** page or the **Platform > Users > Manage Roles** inventory page.

To assign roles to other users in Junos Space, 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 provides Read privileges on all objects associated with the task groups defined in a predefined role.

Table 51 on page 374 shows the Junos Space predefined roles and corresponding tasks available for installed Junos Space applications.



NOTE: For the latest Predefined roles, see **Platform > Users > Manage Users > Create User** or **Platform > Users > Manage Roles**.

Table 51: Predefined Roles for the Network Application Platform

Predefined Role	Task Group and Tasks	Application > Workspace
Audit Log Administrator	<ul style="list-style-type: none"> View Audit Logs Archive/Purge 	Platform > Audit Logs
Device Image Manager	<ul style="list-style-type: none"> Devices <ul style="list-style-type: none"> Manage Device Adapter <ul style="list-style-type: none"> Upload Adapter Install Adapter Delete Adapter Device Images <ul style="list-style-type: none"> Manage Images <ul style="list-style-type: none"> Upload Image MD5 Validation Result Delete Images Modify Images Stage Images Verify Checksum Deploy Images 	Platform > Devices
Device Images Read Only User	Manage Images	Platform > Device Images

Table 51: Predefined Roles for the Network Application Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Device Manager	<ul style="list-style-type: none"> Discover Devices <ul style="list-style-type: none"> Discover Targets Specify Probes Specify Credentials Manage Devices <ul style="list-style-type: none"> Delete Devices Change Device Credentials View Physical Inventory Export Physical Inventory View Interfaces Resynchronize with Network SSH to Device Secure Console Add Deployed Devices <ul style="list-style-type: none"> Add Device Deploy Devices <ul style="list-style-type: none"> Add Devices Connection Profiles <ul style="list-style-type: none"> Create 	Platform > Devices
Device Script Manager	<ul style="list-style-type: none"> Manage Scripts <ul style="list-style-type: none"> View Scripts Import Scripts Modify Script Delete Scripts Deploy Scripts on Device Verify Scripts on Device Enable Scripts on Device Disable Scripts on Device Remove Scripts from Device Execute Script on Device Export Script 	Platform > Scripts
Device Script Read Only User	<ul style="list-style-type: none"> Scripts <ul style="list-style-type: none"> Manage Scripts View Scripts Export Scripts 	Platform > Scripts
Job Manager	<ul style="list-style-type: none"> Manage Jobs <ul style="list-style-type: none"> Cancel Job View Recurrence 	Platform > Job Management

Table 51: Predefined Roles for the Network Application Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Super Administrator	Manage all Junos Space task groups and tasks (See Platform > Users > Create Users user interface for the current roles.)	Access all Junos Space workspaces (See Platform > Users > Manage Users > Create Users user interface for the current roles.)
Permission Label Administrator	Manage all Permission Label tasks	Platform > Administration
System Administrator	<ul style="list-style-type: none"> • Manage Fabric <ul style="list-style-type: none"> • Add Fabric Node • Manage Databases <ul style="list-style-type: none"> • Backup Database • Delete Database Backup • Restore Database • Troubleshoot Space • Manage Applications <ul style="list-style-type: none"> • Modify Application Settings • Add Application • Uninstall Application • Upgrade Application • Upgrade Platform • Manage Licenses <ul style="list-style-type: none"> • Upload License • Manage Tags <ul style="list-style-type: none"> • Share Tag • Rename Tags • Delete Tags • Apply Tag 	Platform > Administration
Tag Administrator	<ul style="list-style-type: none"> • Manage Tags <ul style="list-style-type: none"> • Rename Tag • Delete Tag • Share Tag • Create Tags 	Platform > Administration > Manage Tags
Template Design Manager	<ul style="list-style-type: none"> • Devices <ul style="list-style-type: none"> • Manage Template Definition <ul style="list-style-type: none"> • Create Template Definition • Modify Template • Clone Template • Publish Template • Delete Template 	Platform > Devices

Table 51: Predefined Roles for the Network Application Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Template Manager	<ul style="list-style-type: none"> • Manage Templates <ul style="list-style-type: none"> • Create Template • Modify Template • Clone Template • Deploy Template 	Platform > Devices
Topology Manager	<ul style="list-style-type: none"> • Topology Visualization <ul style="list-style-type: none"> • Discover Topology <ul style="list-style-type: none"> • Specify Target • Specify SNMP Probes • View Topology 	Platform > Topology Manager
User Administrator	<ul style="list-style-type: none"> • Manage Users <ul style="list-style-type: none"> • Create User • Modify User • Delete Users • Manage Roles <ul style="list-style-type: none"> • Create Role • Modify Role • Delete Role 	Platform > Users

[Table 52 on page 377](#) shows the Junos Space predefined roles for the Network Activate application.

Table 52: Predefined Roles for Network Activate Application

Predefined Role	Task Group and Tasks	Workspace
Service Designer	<ul style="list-style-type: none"> • Manage Service Definitions <ul style="list-style-type: none"> • Create Point-to-Point (P2P) Service Definition • Custom Service Definition • Create VPLS Service Definition • Publish Service Definition • Unpublish Service Definition 	Service Design

Table 52: Predefined Roles for Network Activate Application (*continued*)

Predefined Role	Task Group and Tasks	Workspace
Service Manager	<ul style="list-style-type: none"> • Manage Device Roles <ul style="list-style-type: none"> • Rules • Discovery Roles • Unassign NPE Role • Manage Device UNIs • Delete UNI • Add Device UNIs • Assign UNI • Assign Roles • Modify Loopback Address • Manage Device UNIs • Exclude from UNI Role • Exclude from NPE Role • Assign NPE Role 	Prestage Devices
Service Activator	<ul style="list-style-type: none"> • Manage Customers <ul style="list-style-type: none"> • Create Customer • Modify Customer • Delete Customers • Manage Service Orders <ul style="list-style-type: none"> • Create Point-to-Point (P2P) Service Order • Deploy Service Order • Delete Service Order • Create VPLS Service Order • Manage Services <ul style="list-style-type: none"> • Modify Service • Decommission Service • View Configuration Audit Results • Perform Configuration Audit • View Functional Audit Results • Perform Functional Audit • View Service Configuration 	Service Provisioning

Table 53 on page 379 shows the Junos Space predefined roles for the Service Now application.

Table 53: Predefined Roles for Service Now Application

Predefined Role	Task Group and Tasks	Workspace
Service Now Administrator	<ul style="list-style-type: none"> Administration <ul style="list-style-type: none"> Service Now Devices <ul style="list-style-type: none"> Add Devices Script Bundles <ul style="list-style-type: none"> Add Script Bundle Organizations <ul style="list-style-type: none"> Add Organization Global Settings <ul style="list-style-type: none"> SNMP Configuration Proxy Server Configuration Service Contract Device Groups <ul style="list-style-type: none"> Create Device Group Service Central <ul style="list-style-type: none"> Incidents <ul style="list-style-type: none"> View Tech Support Cases View End Customer Cases JMB Errors Information <ul style="list-style-type: none"> Messages Device Snapshots Notifications <ul style="list-style-type: none"> Create Notifications 	All workspaces
Service Now Unrestricted User	<ul style="list-style-type: none"> Administration <ul style="list-style-type: none"> Service Now Devices Service Central <ul style="list-style-type: none"> Incidents <ul style="list-style-type: none"> View Tech Support Cases JMB Errors Information <ul style="list-style-type: none"> Messages Device Snapshots Notifications <ul style="list-style-type: none"> Create Notifications 	Administration Service Central

Table 53: Predefined Roles for Service Now Application (*continued*)

Predefined Role	Task Group and Tasks	Workspace
Service Now Read Only User	• Administration	Administration
	• Service Now Devices	Service Central
	• Service Central	
	• Incidents	
	• View Tech Support Cases	
	• JMB Errors	
	• Information	
	• Messages	
	• Device Snapshots	
	• Notifications	

Table 54 on page 380 shows the Junos Space predefined roles for the Ethernet Design application.

Table 54: Predefined Roles for Ethernet Design Application

Predefined Role	Task Group and Tasks	Workspace
Network Engineer	• Port Profiles	EZ Campus Design
	• Create Port Profile	
	• Provision Port Profile	

Related Documentation

- [Role-Based Access Control Overview on page 371](#)
- [Understanding How to Configure Users to Manage Objects in Junos Space on page 372](#)
- [Managing Roles on page 394](#)
- [Creating a User-Defined Role on page 395](#)
- [Modifying User-Defined Roles on page 397](#)
- [Deleting User-Defined Roles on page 397](#)
- [Creating Users on page 381](#)
- [Viewing Users on page 386](#)
- [Viewing User Statistics on page 391](#)

CHAPTER 33

User Accounts

- [Creating Users on page 381](#)
- [Disabling and Enabling Users on page 385](#)
- [Viewing Users on page 386](#)
- [Modifying a User on page 387](#)
- [Deleting Users on page 389](#)
- [Changing User Passwords on page 389](#)
- [Clearing User Local Passwords on page 390](#)
- [Viewing User Statistics on page 391](#)

Creating Users

The Create User task allows the Super Administrator and the User Administrator to create Junos Space user accounts that specify the credentials and predefined roles allowing users to log in and use Junos Space applications, workspaces, and tasks. Each user account must include:

- Login ID
- Password
- First Name
- Last Name

For each user, you can assign roles that define the tasks and objects (devices, users, services, and so forth) that the user can access and manage. You can assign multiple roles to a single user and assign the same role to multiple users.



NOTE: If you do not use the Permission Labels feature, a user can access all the objects that the assigned role controls within the workspace.

You can also assign permissions to users to limit their access to only specified objects within the workspace that the assigned role controls (see [“Managing Permission Labels Overview” on page 499](#)).

The **Use Same Roles Assigned To** option allows you to quickly create multiple user accounts without having to reselect the same predefined roles. To see the available predefined user roles, open the **Create User** dialog box by navigating to **Platform > Users > Manage Users > Create User**.

User accounts are subdivided into three areas, General, Role Assignment, and Permission Assignment. There are links to these areas in the top right corner of the Create User page. You might need to scroll horizontally in order to see the links.

- [Creating a New User Account on page 382](#)

Creating a New User Account

To create a new user account:

1. Navigate to **Platform > Administration > Users > Create User** task.

The Create User dialog box appears.

2. In the Login ID box, enter a login ID for the new Junos Space user account.

This can be an email address. If it is, it is not mandatory that the login ID match the email 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 "." You cannot have two users with the same login ID.

3. (*Local mode*) Type and confirm the local password.

This password is required. The password must include at least two numbers or symbols and must be from 6 to 31 characters.



NOTE: All passwords in Junos Space are case-sensitive.

4. (*Remote Mode*) (Optional for emergency purposes. Assign only to a few privileged administrators.) If you selected Remote Authentication Server **Remote** or **Remote-Local** authentication modes using **Platform > Administration > Remote Authentication Server**, you can:

- a. Select the **Local Password** check box.

This action automatically expands the Local Password area.

- b. Type and confirm the local password.

Local password behaves differently in Remote versus Remote-Local cases:

- In Remote mode, local password is used only in the emergency case, where the authentication servers are unreachable and should probably be limited to a few privileged admins.
- In the Remote-Local mode, local password is mainly used for users who are intended to be managed locally, as opposed to other users who are authenticated by the

remote server. In the case where user authentication exists in both places, the local password functions as a secondary password.

5. *Remote-Local Mode* (Enable for local users in a mixed mode environment. Disable for Remote mode users. In the Confirm Password box, reenter the password you entered.
 - a. Select the **Local Password** check box.
This action automatically expands the Local Password area.
 - b. Type and confirm the local password.
6. In the First Name box, enter the user's first name.
The name cannot exceed 32 characters.
7. In the Last Name box, enter the user's last name.
The name cannot exceed 32 characters.
8. (Optional) In the Email box, enter the user's e-mail address.
This need not be the same as the login ID, if the login ID was an email address.
9. (Optional) In the Image File box, upload the user's photo ID:
 - a. Use the Browse button to locate the user's photo ID file.
You can upload **.bmp**, **.gif**, **.jpg**, and **.png** image file formats.
 - b. Click **Upload**.
Junos Space uploads and saves the photo ID file for the user account.



NOTE: If you do not want to assign the user roles or the permissions at this point, you can click **Create** to create the user account without assigning any roles. Later, you can navigate to the Manage Users workspace to modify the user account and assign roles. If you want to assign user roles now, proceed to the next step.

10. To assign roles to the new user, do one of the following:
 - Select the **Use Same Roles Assigned to** check box and select the name of an existing user whose roles you want to assign to the new user.



TIP: Enter one or more characters of the username in the Use Same Roles Assigned to search box to find the user and select the username. The assigned roles appear in the Selected roles list. You can modify the new user's role assignments by adding or removing roles from the Selected Roles column.

- Use the double list box to select predefined roles for the user. Select one or more roles from the Available list box. Selected roles appear in the Selected list box. Use the right arrow to move the selected roles to the Selected list box. Use the left arrow

to remove roles from the Selected list box back to the Available list box. You can also double-click a role to select or remove it. You see the details of selected roles appear in the right pane of the page.

You can also create user-defined roles for users. For more information, see [“Creating a User-Defined Role” on page 395](#).



NOTE: The minimum role required for configuring a user for IBM Systems Director and Junos Space Launch in Context (LiC) is Device Manager.

11. To assign permission labels to the new user, do one of the following:

- Select the **Use Same Permission Labels Assigned to** check box and select the name of an existing user whose permission labels you want to assign to the new user.



TIP: Enter one or more characters of the username in the Use Same Permission Labels Assigned to search box find the user and select the username. The assigned permission labels appear in the Selected list box. You can modify the new user's permission label assignments by adding or removing permission labels from the Selected column.

- Use the double list box to select permission labels for the user. Select one or more permission labels from the Available list box. Selected permission labels appear in the Selected list box. Use the right arrow to move the selected labels to the Selected list box. Use the left arrow to remove labels from the Selected list box back to the Available list box. You can also double-click a label to select or remove it. You see the details of selected labels appear in the right pane of the page.

You can also create permission labels for users. Do not forget to attach a newly created permission labels to an object as well as assigning it to a user. For more information, see [“Working With Permission Labels” on page 501](#).

12. Click **Create** to create the user account with the assigned roles and permissions, if applicable.

The new user account is created in the Junos Space database. You see the new user account on the Manage Users inventory page.

Disabling and Enabling Users

Disable a user to prevent she/he from logging in to the system.

By default, all users are enabled.

Super-users cannot be disabled.

The action of enabling or disabling a user generates an audit log entry.

On the Manage Users inventory landing page, user status appears as an icon in the thumbnail view, while in the tabular view, there is a status column showing icons for enabled or disabled status. The User Detail Summary page also indicates a user's status.

When a user is disabled, she/he sees the message “This account is disabled” when she/he tries to log in to the system. If the user is active at the time she/he is disabled, the system logs the user off and displays to the user a message saying that his/her account is disabled. In both cases, a disabled user's attempt to log in generates an audit log entry.

You cannot disable your own user account

To disable/enable one or more users:

1. Navigate to **Platform > Users > Manage Users**. The Manage Users inventory page appears, displaying all user accounts.
2. Select one or more users to disable/enable.



NOTE: If both the Enable and the Disable actions are grayed out, you have selected a super-user.

3. Select **Disable Users/Enable Users** from the Actions drawer.

The Disable/Enable Users confirmation dialog box appears, displaying the list of users to whom the selected action will be applied. Users you selected, but who do not appear in the list, will not have the action applied to them. Only those users who are not already in the state to which you want to convert them can be enabled or disabled. If you selected disabled users to disable again, a message appears, telling you how many users' status will not change.

4. Verify the list of users that you want to disable or enable, and click **Disable Users / Enable Users**.

All selected user accounts are disabled/enabled.

Related Documentation

- [Creating Users on page 381](#)
- [Modifying a User on page 387](#)
- [Viewing Users on page 386](#)
- [Junos Space Audit Logs Overview on page 357](#)

Viewing Users

The Manage Users inventory page displays all of the Junos Space users who have accounts. To add new users, you must have administrator privileges. Use **Platform > Users > Manage Users > Create User** to add a new user (see [“Creating Users” on page 381](#)). Users have Junos Space access based on predefined user roles (see [“Predefined Administrator Roles” on page 373](#)). For more information about how to manipulate inventory page data, see [“Inventory Pages Overview” on page 28](#).

- [Changing Views on page 386](#)
- [Viewing User Details on page 386](#)
- [Performing Manage User Commands on page 387](#)

Changing Views

You can display user in two views: thumbnail and tabular. By default, users appear on the page in thumbnail view.

In thumbnail view, users appear as icons listed in descending order alphabetically by user name. Each user has name.

In tabular view, users appear in a table sorted by username. Each user is a row in the Manage Users table.

To change views:

1. Navigate to **Platform > Users > Manage Users**. The **Manage Users** page appears.
2. Click a view indicator at the right of the **Manage Users** page title bar.

Viewing User Details

To view more detailed user information:

- Double-click a user icon in thumbnail view or double-click a row in the table in tabular view.
- Move the zoom slider to the far right. The default zoom slider position is in the middle.

[Table 55 on page 386](#) defines the user detailed information.

Table 55: Users Detailed Information and Columns in the Manage Users Table

Data	Description
Login ID	The login username.
First Name	The user first name.
Last Name	The user last name.
E-mail Address	The user e-mail account.

Table 55: Users Detailed Information and Columns in the Manage Users Table (*continued*)

Data	Description
Assigned Roles	The predefined user roles assigned to user.
Role Summary	The workspaces and tasks a user can perform based on the predefined user roles.

Performing Manage User Commands

- You can perform the following commands from the Manage Users Actions drawer:
- Modify User—See [“Modifying a User” on page 387](#)
 - Delete User—See [“Deleting Users” on page 389](#)
 - Clear Local Passwords—See [“Clearing User Local Passwords” on page 390](#)
 - Tag It—[“Tagging an Object” on page 495](#)
 - View Tags—[“Viewing Tags” on page 496](#)
 - Clear All Selections—Clears all selections that you selected using Select Page. You can also clear all selections by clicking Select None.

Related Documentation

- [Understanding How to Configure Users to Manage Objects in Junos Space on page 372](#)
- [Creating Users on page 381](#)
- [Deleting Users on page 389](#)
- [Modifying a User on page 387](#)
- [Viewing User Statistics on page 391](#)
- [Tagging an Object on page 495](#)
- [Viewing Tags on page 496](#)

Modifying a User

A Super Administrator or User Administrator can modify any user account in Junos Space. You can add or remove roles and modify any user settings except the Login ID and the permissions. To modify a user’s permissions, go to the Permission Labels task in the Administration workspace (see [“Working With Permission Labels” on page 501](#)

Each user account can have multiple roles and a role can be associated with multiple users.

To modify an existing user account:

1. Navigate to **Platform > Users > Manage Users**. The **Manage Users** inventory page appears.
2. From the inventory page, select the user account that you want to modify.



NOTE: You can modify only one user account at a time.

3. From the Actions drawer, select **Modify User**.

The **Manage Users** dialog box appears filled in with the existing user account information.

4. You can change the password, first name, last name, e-mail address, photo ID, and the selected roles.

- To change the password, you must include at least two numbers or symbols in the new password and the password must be from 6 to 31 characters. All passwords in Junos Space are case-sensitive.
- *(For Remote or Remote-Local Authentication Server configuration only)* If you selected Remote Authentication Server **Remote** or **Remote-Local** authentication modes using **Platform > Administration > Remote Authentication Server**:

- a. If you want to remove the local password, deselect the **Local Password** check box.

This action automatically collapses the **Local Password** area.

- b. If you want to change the local password, type and confirm a new local password.

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 change the user name, enter a new name in the First Name and/or Last Name boxes.
- To change the e-mail account, enter a new e-mail address in the Email box.
- To upload another image file:

- a. Use the **Browse** button to locate the new user photo ID file.

You can upload BMP, GIF, JPG, and PNG image file formats.

- b. Click the **Upload** button.

Junos Space updates the photo ID file for the user account.

- To add or remove role assignments:
 - 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.
 - 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.

5. Click **Modify** to save your changes to the user account.

Junos Space updates the user account with the changes you specified.

- Related Documentation**
- [Understanding How to Configure Users to Manage Objects in Junos Space on page 372](#)
 - [Creating Users on page 381](#)
 - [Deleting Users on page 389](#)
 - [Viewing Users on page 386](#)

Deleting Users

When a Junos Space 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. Navigate to **Platform > Users > Manage Users**.

The Manage Users inventory page appears, displaying all user accounts.

2. Select one or more users to delete.
3. In the Actions drawer, click **Delete Users**.

The Delete Users confirmation dialog box appears.

4. Verify the list of users that you want to delete and click **Delete**.

All selected user accounts are removed from the Junos Space database and the Manage Users inventory page.

- Related Documentation**
- [Creating Users on page 381](#)
 - [Modifying a User on page 387](#)
 - [Viewing Users on page 386](#)

Changing User Passwords

Users that are logged in to Junos Space can change their account password using the User Preferences icon in the Junos Space banner. You do not have to have any user roles configured to change your password.



WARNING: If you have a local password for remote or remote-local authentication modes, changing your password does that locally only. The change does not affect any passwords that a user administrator might have configured for you on a remote authentication server.



WARNING: If a user does not have a local password set, that user will not be able to set or change it.

To change your user password, follow these steps:

1. Click the User Preferences icon in the Junos Space banner. The User Preferences – Change Password dialog box appears.
2. Type your old password.
3. Type your new password.

The password must be 6 to 31 characters long, including two numbers or symbols.

4. Retype your password to confirm it.
5. Click **Change**. You are logged out of the system.

You have to log in again using your new password. Any open sessions are disabled until you log in again.

- Related Documentation**
- [Creating Users on page 381](#)
 - [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 Administration privileges.

To remove a user local password:

1. Navigate to **Platform > Users > Manage Users**.
The **Manage Users** inventory page appears.
2. Select one or more users for which you want to remove a local password.
3. Right-click and select **Clear Local Passwords** from the pop-up menu, or open the Actions drawer and select the command.
The **Delete Users** dialog box appears.
4. Click **Clear Passwords**.

- Related Documentation**
- [Viewing Users on page 386](#)
 - [Creating Users on page 381](#)
 - [Modifying a User on page 387](#)
 - [Creating a Remote Authentication Server on page 484](#)

Viewing User Statistics

You can view the percentage and the number of Junos Space users that have been assigned to a role.

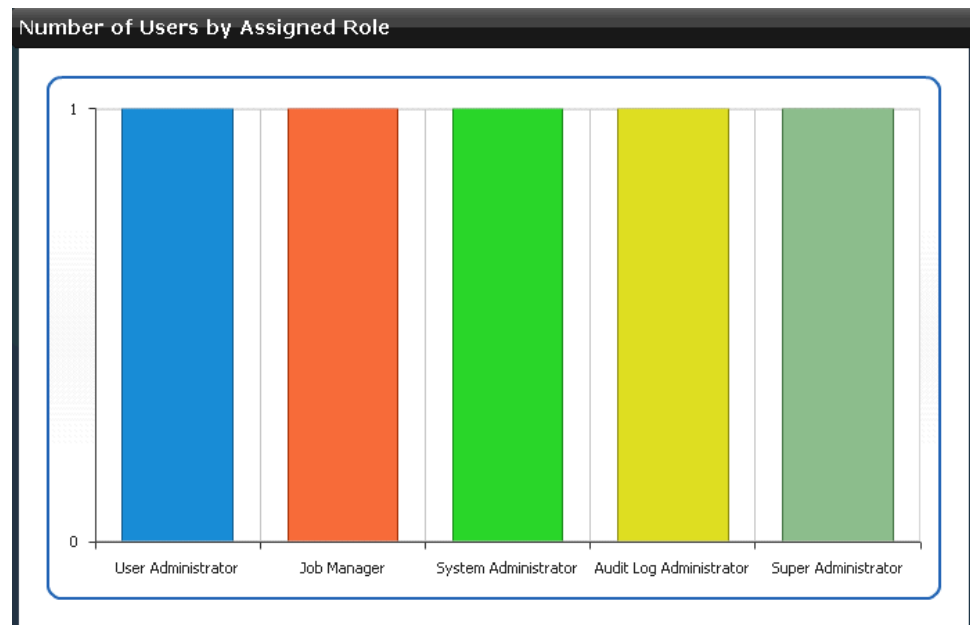
- [Viewing the Number of Users Assigned by Role on page 391](#)

Viewing the Number of Users Assigned by Role

To view the percentage of total users that have been assigned to a predefined role:

1. From the navigation ribbon, select the **Users** workspace.

Junos Space displays a bar chart showing users by assigned role.



The bar chart displays the number of users assigned to each role that has one or more assigned users.

2. To view the number of users assigned to a specific role, mouse over the role in the chart.
3. To display an inventory page of users assigned to a specific role, click on the segment of the chart that represents the role.

Related Documentation

- [Role-Based Access Control Overview on page 371](#)
- [Viewing Users on page 386](#)
- [Creating Users on page 381](#)
- [Deleting Users on page 389](#)

CHAPTER 34

User Roles

- [Managing Roles Overview on page 393](#)
- [Managing Roles on page 394](#)
- [Creating a User-Defined Role on page 395](#)
- [Modifying User-Defined Roles on page 397](#)
- [Deleting User-Defined Roles on page 397](#)

Managing Roles Overview

Roles define the application workspace tasks a user is assigned by the Super Administrator and User Administrator to perform in Junos Space. Users represent an individual in a security domain who is authorized to log into Junos Space 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 Users” on page 381](#) and [“Predefined Administrator Roles” on page 373](#). 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 **Platform > Users > Manage Roles** task allows the Super Administrator or User Administrator to manage all roles by performing the following user role tasks:

- View all predefined and user-defined roles on the **Platform > Users > Manage Users** inventory page. See [“Managing Roles” on page 394](#).
- Create user-defined roles from the **Platform > Users > Manage Roles > Create Role** task. See [“Creating a User-Defined Role” on page 395](#).
- Modify user-defined roles using **Modify Role** in the **Platform > Users > Manage Users** inventory page Actions drawer. See [“Modifying User-Defined Roles” on page 397](#).
- Delete user-defined roles using **Delete Roles** in the **Platform > Users > Manage Users** inventory page Actions drawer. See [“Deleting User-Defined Roles” on page 397](#).

- Tag predefined and user-defined roles to group them for performing actions all at once. Use **Tag It** in the **Platform > Users > Manage Users** inventory page Actions drawer. See [“Tagging an Object” on page 495](#).
- View all tags that exist on roles using **View Tags** in the **Platform > Users > Manage Roles** inventory page Actions drawer. See [“Viewing Tags” on page 496](#)

Related Documentation

- [Role-Based Access Control Overview on page 371](#)
- [Predefined Administrator Roles on page 373](#)
- [Creating Users on page 381](#)
- [Managing Roles on page 394](#)
- [Creating a User-Defined Role on page 395](#)
- [Modifying User-Defined Roles on page 397](#)
- [Deleting User-Defined Roles on page 397](#)

Managing Roles

A role is a description of tasks a user can perform in Junos Space to allow access to application workspaces. The **Platform > Users > Manage Roles** inventory page allows the Super Administrator or the User Administrator to view all predefined and user-defined roles that exist for Junos Space applications. The administrator should understand all predefined roles and create any user-defined roles before creating users.

Viewing User Role Details

The **Manage Roles** inventory page displays all predefined and user-defined roles in both thumbnail and tabular views. To switch between views, click the thumbnail and tabular view icons at the right of the **Manage Roles** page title.

In thumbnail view, a user role is represented as a selectable object. Visual cues indicate whether the role is predefined or user-defined.

In tabular view each role is represented by a row in the table. Roles are listed in the table in ascending alphabetical order by role title, description, and tasks assigned. You can show or hide table columns and sort records in ascending or descending order.

In both thumbnail and tabular views, 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 in both thumbnail and tabular views:

1. Double-click a role.

The Role Details Summary page appears.

The page displays the workspace, and workspace tasks.

2. Click the expander button **[+]** to view subtasks.
3. Click **OK**.

Performing Manage Roles Commands

The commands you can perform on predefined and user-defined roles are located in the Actions drawer or by right-clicking that role. You can only perform the **Modify Role** and **Delete Roles** commands on read-writeable user-defined roles. You can not manipulate read-only predefined roles. To perform a command, you must first select the role.

The following commands are included in the **Modify Role** Actions drawer:

- **Modify Role**—Modify the selected user-defined role title, description, and application workspace task. You can not modify predefined roles. For more information, see [“Modifying User-Defined Roles” on page 397](#).
- **Delete Roles**—Delete the selected user-defined role. You can not delete predefined roles. For more information, see [“Creating a User-Defined Role” on page 395](#).
- **Tag It**—Tag one or more selected inventory objects, see, see [“Tagging an Object” on page 495](#).
- **View Tags**—View a list of tags that exist on a selected inventory object. For more information, see [“Viewing Tags” on page 496](#).
- **Untag It**—Untag a tag that has been applied to an inventory object, see [“Untagging Objects” on page 497](#).
- **Clear All Selections**—Clear any user role selections you made on the Manage Roles inventory page. Use the Select: Page in the Manage Roles page title bar to select all roles at once.

Related Documentation

- [Role-Based Access Control Overview on page 371](#)
- [Predefined Administrator Roles on page 373](#)
- [Creating Users on page 381](#)
- [Creating a User-Defined Role on page 395](#)
- [Modifying User-Defined Roles on page 397](#)
- [Deleting User-Defined Roles on page 397](#)

Creating a User-Defined Role

Junos Space provides a number of read-only predefined roles you, the Super Administrator, System Administrator, or User Administrator can use to create user log in, access, and perform tasks in application workspaces. You can also create read-write user-defined roles that conform to user responsibilities and access privileges required on your network. You can modify and delete only user-defined roles that you create. You cannot modify or delete predefined roles.

To create a user-defined role:

1. Select **Platform > Users > Manage Roles > Create Role**.

The Create Role page appears, allowing you to select workspaces and associated tasks from all deployed applications.

2. In the Title text box, type a user-defined role name.

The role title can not exceed 32 characters. The title can only contain letters, numbers, and can include a hyphen (-), underscore (_), or period (.).

3. In the Description box, type a user-defined role description.

The role description can not exceed 256 characters

4. Select an application workspace from the application workspace selection ribbon.

Mouse over an application workspace icon to view the application and workspace name. You can select one or more workspaces per user-defined role. An expandable/collapsible tree of associated tasks appear below the selection ribbon for you to modify specific tasks you want included in the Task Summary pane.

5. Select the specific task(s) you want for the user-defined role. All application workspace tasks are by default deselected in the task tree.

Only the currently edited application workspace node is expanded in the Task Summary pane; previously selected workspace nodes are collapsed. You can expand other workspace nodes manually.

Selecting the top node or workspace selects or deselects the whole task tree. Selecting any task node automatically selects its decedents. Selecting any task node automatically selects its parent and grand parent.

Only the currently active task tree appears in the Task Summary pane.

In the Task Summary pane, the top level application node in the tree is bold-italic; the second level workspace tree node is bold.

6. Click **Create**.

The user-defined role is created, saved, and appears in the Manage Roles inventory page.

Scroll down or search to view it.

You cannot create or save a user-defined role when the workspace tasks are not selected.

Related Documentation

- [Predefined Administrator Roles on page 373](#)
- [Managing Roles on page 394](#)
- [Modifying User-Defined Roles on page 397](#)
- [Deleting User-Defined Roles on page 397](#)
- [Creating Users on page 381](#)

Modifying User-Defined Roles

The Super Administrator and the User Administrator can modify user-defined roles that have been created. You can modify the role description, application workspace, and the selected tasks. You can not modify the role title or predefined roles.

To modify a user-defined role:

1. Navigate to **Platform > Users > Manage Roles**.

The Manage Roles inventory page appears displaying all existing predefined and user-defined roles.

2. Select the user-defined role you want to modify.
3. Select **Modify Role** from the Actions drawer.
4. Modify the part of the user-defined role that you want: description, application workspace, or tasks.

The role title can not exceed 32 characters. The title can only contain letters, numbers, and can include a hyphen (-), underscore (_), or period (.).

The role description can not exceed 256 characters

5. Click **Modify**.

The modified user-defined role is updated in the Manage Roles inventory page.

Related Documentation

- [Predefined Administrator Roles on page 373](#)
- [Creating Users on page 381](#)
- [Managing Roles on page 394](#)
- [Managing Roles Overview on page 393](#)
- [Creating a User-Defined Role on page 395](#)
- [Deleting User-Defined Roles on page 397](#)

Deleting User-Defined Roles

The Super Administrator and the User Administrator can delete user-defined roles from the **Manage Roles** inventory page only if they are not being used by other users. You can not delete pre-defined roles.

To delete a user-defined role:

1. Select **Platform > Users > Manage Roles**.

The **Manage Roles** inventory page appears displaying all existing predefined and user-defined roles.

2. Select the user-defined role(s) you want to delete.

3. Select **Delete Roles** from the Actions drawer.

The Delete Roles dialog box appears.

4. Confirm deletion of the selected user defined role(s). Select the role(s).
5. Click **Delete**.

The role is deleted from the Manage Roles inventory page. If the role is used by other Junos Space users, you cannot delete the role. A warning message appears.

**Related
Documentation**

- [Predefined Administrator Roles on page 373](#)
- [Managing Roles on page 394](#)
- [Creating a User-Defined Role on page 395](#)
- [Managing Roles Overview on page 393](#)
- [Modifying User-Defined Roles on page 397](#)
- [Creating Users on page 381](#)

PART 10

Administration

- [Overview on page 401](#)
- [Fabric on page 405](#)
- [Manage Databases on page 431](#)
- [Manage Licenses on page 445](#)
- [Manage Applications on page 451](#)
- [System Troubleshooting on page 469](#)
- [Authentication Servers on page 479](#)
- [Managing Tags on page 491](#)
- [Managing Permission Labels on page 499](#)
- [Managing DMI Schemas on page 505](#)

Overview

- [Junos Space Administrators Overview on page 401](#)
- [Maintenance Mode Overview on page 402](#)

Junos Space Administrators Overview

Junos Space administrators can serve different functional roles. A CLI administrator installs and configures Junos Space appliances. A maintenance-mode administrator performs system-level tasks, such as troubleshooting and database restore operations. After appliances are installed and configured, users are created from the Junos Space user interface to access workspaces and manage applications, users, devices, services, customers, and so forth.

[Table 56 on page 401](#) shows the Junos Space administrators and the tasks that can be performed.

Table 56: Junos Space Administrators

Junos Space Administrator Function	Description	Tasks
CLI administrator	<p>An administrator responsible for setting up and managing system settings for Junos Space appliances from the serial console.</p> <p>The CLI administrator name is "admin".</p> <p>The CLI administrator password can be changed from the console system settings menu.</p>	<ul style="list-style-type: none">• Install and configure basic settings for Junos Space appliances.• Change network and system settings for appliances, for example:<ul style="list-style-type: none">• Change CLI administrator password.• Set routing• Set DNS servers• Change time options• Expand VM drive size (Junos Space Virtual Appliances only)• Retrieve log files for troubleshooting

Table 56: Junos Space Administrators (*continued*)

Maintenance mode administrator	<p>An administrator responsible for performing system-level maintenance on Junos Space.</p> <p>The maintenance mode administrator name is "maintenance".</p> <p>The maintenance mode password is configured from the serial console when you first configure a Junos Space appliance.</p>	<ul style="list-style-type: none"> • Restore Junos Space to previous state by using a database backup file. • Shut down Junos Space nodes by entering maintenance mode. • Retrieve log files for troubleshooting. • Exit Maintenance mode and explicitly start up Junos Space system.
Junos Space user interface users	<p>A Junos Space user that is assigned one or more predefined roles. Each role assigned to a user provides specific access and management privileges on the objects (applications, devices, users, jobs, services, customers) available from a workspace in the Junos Space user interface.</p>	<p>For complete information about the predefined roles that can be assigned to a Junos Space user, see "Predefined Administrator Roles" on page 373.</p>

- Related Documentation**
- [Maintenance Mode Overview on page 402](#)
 - [Role-Based Access Control Overview on page 371](#)
 - [Understanding How to Configure Users to Manage Objects in Junos Space on page 372](#)

Maintenance Mode Overview

In Junos Space, Maintenance mode is a special mode that the administrator uses to perform database restore or debugging tasks while all nodes in the fabric are shutdown and the Junos Space web proxy is running.

The Junos Space system goes into Maintenance mode in the following cases:

- Junos Space goes down.

The system will go into Maintenance mode when Junos Space is down on all nodes in the fabric. Users attempting to log in when the system is in Maintenance mode are redirected to the maintenance mode log in screen. Users who logged in to Junos Space before the shutdown and attempt to perform an action in the user interface are also redirected to the maintenance mode log in screen.

- An authorized Junos Space administrator initiates a Restore Database from Backup action.

When a user initiates a Restore database action, Junos Space prompts the user for user name and password to enter maintenance mode, as shown in the Authentication Required dialog box. After the user is authenticated, Junos Space initiates the restore database operation and the system remains in Maintenance mode until the database is restored and the user exits maintenance mode.

- An authorized Junos Space administrator upgrades the Platform software.

When a user initiates a software upgrade, Junos Space prompts the user for user name and password to enter maintenance mode, as shown in the Authentication Required dialog box. After the user is authenticated, Junos Space 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 in maintenance mode, the Maintenance Mode Actions menu displays the tasks a user can perform in Maintenance Mode.

Figure 130: Maintenance Mode Actions Menu

- [Restore Database from Backup](#)
This action leads user to select a database backup file and overwrite the current database
- [Download Troubleshooting Data and Logs](#)
This action allows user to download Space logs for troubleshooting
- [Log Out and Remain in Maintenance Mode](#)
This action logs out the current user so that another administrator can login and manage in maintenance mode
- [Log Out and Exit from Maintenance Mode](#)
This action returns Space to normal operational mode

When a user exits maintenance mode, Junos Space is restarted. After several minutes, the system returns to normal operational mode, and Junos Space users can log in to the user interface.

Maintenance Mode Access and System Locking

An authorized Junos Space administrator puts the system into maintenance mode by initiating a Restore database action (see [“Restoring a Database in Maintenance Mode” on page 440](#)).

Only one Maintenance mode administrator can access Maintenance mode at a time. When an administrator logs in to Maintenance mode, Junos Space locks the page. When a second administrator attempts to log in to Maintenance mode while the first administrator is logged in, Junos Space displays a message indicating that another administrator is currently logged in to the system and that Maintenance Mode is locked. The Maintenance mode lock releases when the first administrator logs out or the lock times out. If the logged-in administrator is inactive, the maintenance mode lock is released after 5 minutes at which time another administrator can log in.

Maintenance Mode User Administration

The user name for the maintenance mode administrator is “maintenance”.

The password for the maintenance mode administrator is set from the Junos Space system console during the initial installation/configuration of a Junos Space appliance or virtual appliance.

A Junos Space administrator connects to an appliance that is already in maintenance mode by using the URL `https://ip-address/maintenance`, where *ip-address* is the Web access IP address for the appliance.

**Related
Documentation**

- [Restoring a Database in the User Interface on page 437](#)
- [Restoring a Database in Maintenance Mode on page 440](#)
- [Backing Up the Database on page 433](#)
- [Database Backup and Restore Overview on page 431](#)

CHAPTER 36

Fabric

- [Fabric Management on page 405](#)

Fabric Management

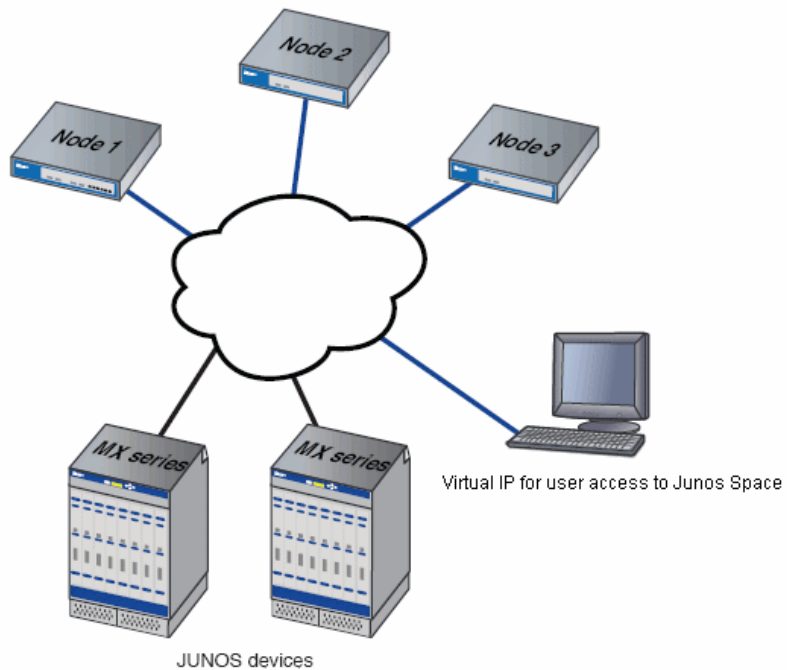
- [Fabric Management Overview on page 405](#)
- [Adding a Node to an Existing Fabric on page 409](#)
- [Adding a Fabric Node on page 411](#)
- [Viewing Nodes in the Fabric on page 412](#)
- [Configuring Node Network Settings on page 415](#)
- [Shutting Down or Rebooting a Node From Junos Space on page 420](#)
- [Deleting a Node on page 421](#)
- [Understanding Overall System Condition and Fabric Load on page 422](#)
- [Monitoring Nodes in the Fabric on page 424](#)
- [Creating a System Snapshot on page 425](#)
- [Deleting a System Snapshot on page 428](#)
- [Restoring the System to a Snapshot on page 428](#)

Fabric Management Overview

You can deploy Junos Space appliances 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 software that runs on the operating system. Each Junos Space appliance or virtual appliance that you install and configure is represented as a single node in the fabric. You can add nodes without disrupting the services that are running on the fabric. When you add nodes to the fabric, you can manage and monitor the nodes from the Administration workspace. To add, manage, and monitor nodes in the fabric, a fabric administrator connects to a single virtual IP address, as shown in the illustration.

Figure 131: Fabric Nodes



NOTE: All appliances (nodes) in a fabric must be from same Junos Space release. For example, a fabric comprises Junos Space Release 1.1 appliances or Junos Space Release 1.2 appliances, but not both.

Single Node Functionality

When the fabric comprises a single appliance, all devices in the managed network connect to the appliance. When you install and configure the first appliance, Junos Space automatically creates a fabric with one node. By default, a fabric that consists of a single node provides complete Junos Space management functionality, with the following *node functions* enabled for the node:

- Load Balancer— for processing HTTP requests from remote browsers and NBI clients
- Database— for processing database requests (create, read, update, and delete operations)
- Application Logic— for processing back-end business logic (Junos Space service requests) and DML workload (device connectivity, device events, and logging)



NOTE: A fabric that comprises a single node provides no workload balancing and no backup if the appliance goes down.

Multinode Functionality

As your network expands with new devices, services, and users, you can add Junos Space appliances to handle the increased workload. When you install and configure the first appliance, Junos Space automatically creates a fabric with one node. For each additional appliance you install and configure, you must add a node to logically represent the appliance in the fabric. Each node that you add to the fabric increases the resource pool for the node functions to meet the scalability and availability requirements of your network. By default, Junos Space 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 node functions distribute workload across operating nodes according to the following load-distribution rules:

- **Load Balancer**— When a node that functions as the active load balancer server is down, all HTTP requests are automatically routed to the standby load balancer server that is running on a separate node.
- **Database**— When a node that functions as the active database server is down, all database requests (create, read, update, and delete) are routed to the node that functions as the standby database server.
- **Application Logic (DML and business logic)**— Device connections and user requests are distributed among the nodes, and device-related operations are routed to the node to which the device is connected.

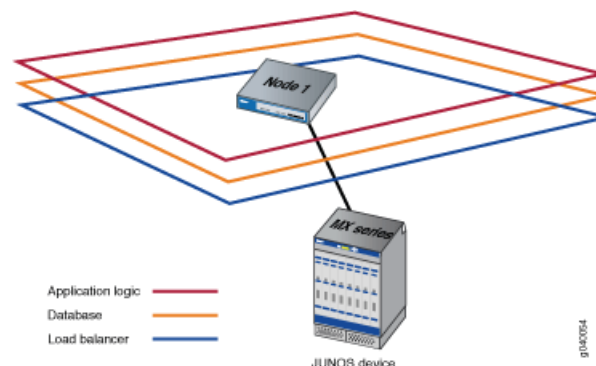
Junos Space uses the following algorithm to ensure that the number of devices connected to a node does not exceed the threshold limit for each node:

$$\text{Threshold Limit} = [(\text{number of devices in database}) / (\text{number of nodes running})] + 2$$

The following workflow describes how the node functions are enabled across the fabric as nodes are added:

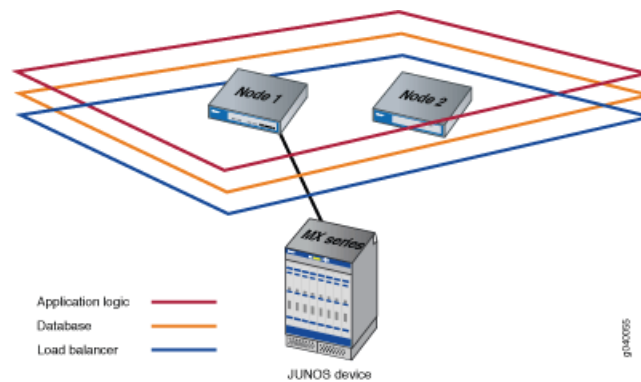
- **First node up:** The load balancer, database, and application logic functions are enabled on the node. Each node function provides both scalability and high availability. The following illustration shows all functions enabled on fabric comprising one node.

Figure 132: Fabric with One Node



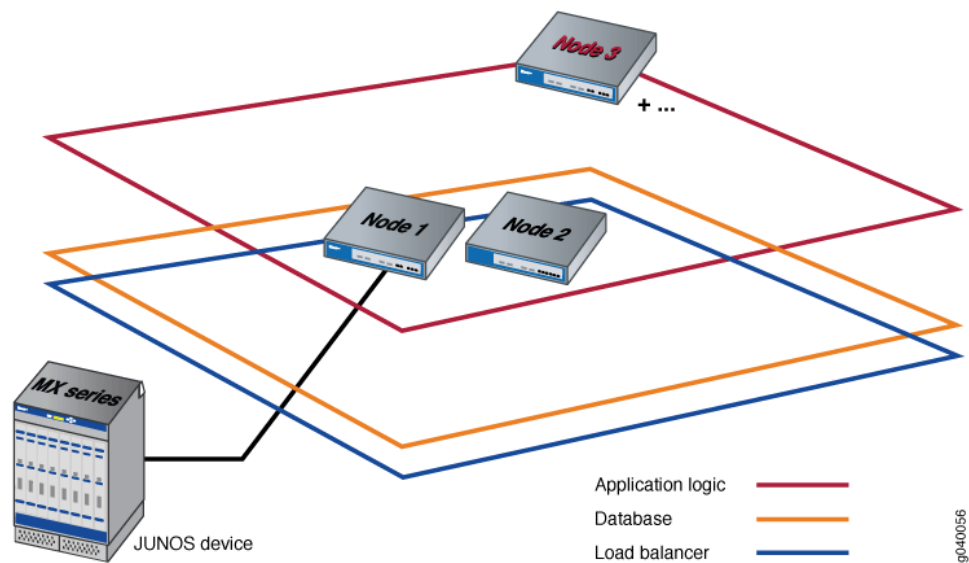
- Add second node: When a second node is added to the fabric, the first node functions as the active load balancer server and active database server, and the second node functions as the standby load balancer server and standby database server. The load balancer and application logic node functions provide scalability and high availability. The database node function on the second node provides high availability only. The following illustration shows the functions enabled on a fabric comprising two nodes.

Figure 133: Fabric with Two Nodes



- Add third node: Only the application logic functionality is enabled on the third node to provide equal distribution of device connections and user requests across all nodes, and route device-related operations to the node to which the device is connected. The application logic functionality provides both scalability and high availability. The following illustration shows the functions enabled on a fabric comprising three nodes.

Figure 134: Fabric with Three Nodes



NOTE: For the third node and each subsequent node added to the fabric, only the application logic functionality is enabled.

Node Function Availability

In a fabric comprising two or more nodes, Junos Space provides failover when a node functioning as the active server (load balancer server or database server) goes down. By default, Junos Space marks a particular node down and routes failover requests to the node that Junos Space designates as standby server. Junos Space uses a heartbeat mechanism to check whether the nodes in the fabric are running. When a node functioning as the active server fails (the appliance physically crashes or stops sending heartbeats), the node functioning as the standby server takes over all resources that were managed by the node functioning as active server.

Related Documentation

- [Viewing Nodes in the Fabric on page 412](#)

Adding a Node to an Existing Fabric

You can install one or more Junos Space appliances to create a scalable fabric. A Junos Space *appliance* can be either a JA1500 Junos Space Appliance or a Junos Space Virtual Appliance. Each Junos Space appliance that you install is represented as a single node in the fabric. As the number of devices on your network expands, you can add nodes to the fabric to manage the increased workload. By default, the Junos Space fabric contains a single node that provides complete Junos Space management functionality. When you install and configure the first appliance, Junos Space automatically adds the first node to the fabric and uses the logical node name that you assign to the appliance when you configure the appliance in the command line interface. For each additional appliance that you install and configure, you must add the node in Junos Space to represent the appliance in the fabric.

Before you begin, the following prerequisites must be in place:

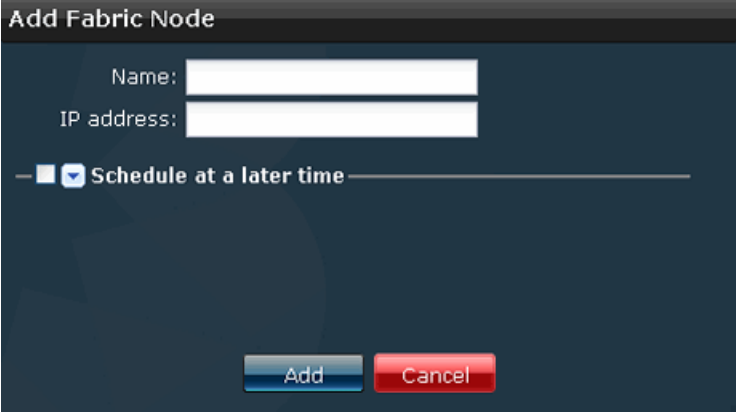
- Multicast needs to be enabled on the switches to which Space nodes are connected;
- IGMP-Snooping needs to be disabled on the switches to which Space nodes are connected. By default IGMP-snooping is enabled on most of the switches.

To add a node to the Junos Space fabric:

1. From the navigation ribbon, select the **Administration** workspace.
2. From the navigation ribbon, select the Manage Fabric icon.
3. From the navigation ribbon, select the **Add Fabric Node** task.

The Add Fabric Node dialog box appears.

Figure 135: Add Fabric Node Dialog Box



The dialog box is titled "Add Fabric Node". It contains two input fields: "Name:" and "IP address:". Below these fields is a checkbox labeled "Schedule at a later time" which is currently checked. At the bottom of the dialog are two buttons: "Add" (blue) and "Cancel" (red).



NOTE: Before you add a node to the Junos Space fabric, make sure that no jobs are pending. No new jobs will be scheduled to run until the add node job has completed.

4. In the Name box, enter a name for the node.
5. In the IP address field, enter the IP address of the Junos Space appliance.



NOTE: This is the IP address for interface eth0 that you specified during the basic configuration of the appliance.

6. Schedule the Add Fabric Node operation:
 - Clear the **Schedule at a later time** check box (the default) to initiate the add node operation when you complete step 7 of this procedure.
 - Select the **Schedule at a later time** check box to specify a later start date and time for the add node operation.



NOTE: The selected time in the scheduler corresponds to Junos Space server time but is mapped to the local time zone of the client computer.

7. Click **Add** to add the node to the fabric.

The node is added to the fabric and appears in the Junos Space user interface and database. When you add a node, the node functions are automatically assigned by Junos Space. By default, the first and second 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 service requests), and DML workload (device connectivity, device events, and logging)

By default, the third node, and all subsequent nodes, added to a fabric perform only the Application Logic function.

Adding a Fabric Node

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 management functionality. When you install and configure the first appliance, Junos Space automatically adds the first node to the fabric and uses the logical node name that you assign to the appliance when you configure the appliance in the command line interface. For each additional appliance that you install and configure, you must add the node in Junos Space to represent the appliance in the fabric.

- [Adding a Fabric Node on page 411](#)

Adding a Fabric Node

You can add one or more nodes to the existing Junos Space fabric, but you can add only one node at a time.

To add a fabric node:

1. Navigate to Platform > Administration ? Manage Fabric > Add Fabric Node. The Add Fabric Node dialog box appears.



NOTE: Before you add a node to the Junos Space fabric, make sure that no jobs are pending. No new jobs will be scheduled to run until the add node job has completed.

2. In the Name box, enter a name for the node.
3. In the IP address box, enter the IP address of the JA1500 Junos Space appliance or Junos Space Virtual appliance.
4. In the Schedule at a later time area of the Add Fabric Node dialog box, schedule when you want to add a fabric node:
 - Clear the **Schedule at a later time** check box (the default) to initiate the add node 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 add node operation.



NOTE: The selected time in the scheduler corresponds to Junos Space server time but is mapped to the local time zone of the client computer.

5. Click **Add** to add the node to the fabric.

The node is added to the fabric and appears in the Junos Space user interface and database. When you add a node, the node functions are automatically assigned by Junos Space. By default, the first and second 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 service requests), and DML workload (device connectivity, device events, and logging)

The third node (and all subsequent nodes) added to a fabric perform only the Application Logic function.

Related Documentation

- [Fabric Management Overview on page 405](#)
- [Viewing Nodes in the Fabric on page 412](#)
- [Understanding Overall System Condition and Fabric Load on page 422](#)

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 Monitoring inventory page refreshes every 10 seconds, by default.

- [Changing Views on page 412](#)
- [Viewing Fabric Node Details on page 413](#)
- [Performing Fabric Node Actions on page 415](#)

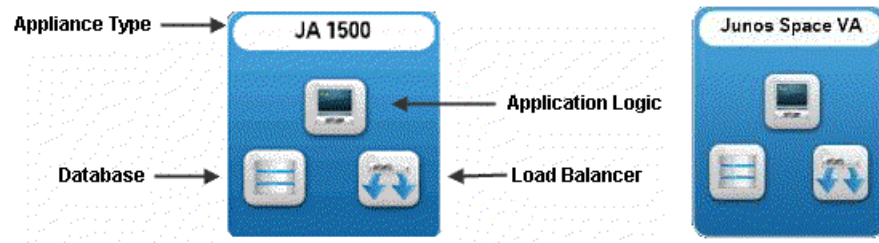
Changing Views

You can display fabric monitoring in two views: thumbnail and tabular. By default, fabric monitoring objects appear in thumbnail view.

In thumbnail view, fabric monitoring appears as icons listed in descending order alphabetically by node name. Each fabric has a node name.

Each node in the fabric is represented by a thumbnail, which indicates whether the node is a JA1500 Junos Space Appliance (JA1500) or a Junos Space Virtual Appliance (Junos Space VA), and the node functions (database, load balancer, or application logic) that

run (whether up or down) on the appliance. For example, icons for the JA1500 Junos Space appliance and virtual appliance are shown.



In tabular view, 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 **Platform > Administrator > Manage Fabric**. The **Manage Fabric** page appears.
2. Click a view indicator at the right of the Manage Fabric page title bar.

Viewing Fabric Node Details

To view detailed runtime and status information for a node:

- Double-click a node in either thumbnail or tabular views. The **View Node Details** page appears.
- In Fabric Monitoring thumbnail view, move the zoom slider to the far right.

[Table 57 on page 413](#) describes the node information displayed in each column in the table and from the detailed view.

Table 57: Fields for the Fabric Monitoring Inventory Page

Field	Description
Node Name	The 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	The IP address for the node.
Device Connection IP	The 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	The percentage of CPU resource utilized by the node; from 0 to 100%. <ul style="list-style-type: none"> • Unknown—The percentage of CPU utilized is unknown, for example, because the node is not connected.

Table 57: Fields for the Fabric Monitoring Inventory Page (*continued*)

Field	Description
% RAM	<p>The percentage of memory resource utilized by the node; from 0 to 100%.</p> <ul style="list-style-type: none"> Unknown—The percentage of memory utilized is unknown, for example, because the node is not connected.
% Disk	<p>The percentage of the /var directory utilized by the node; from 0 to 100%.</p> <ul style="list-style-type: none"> Unknown—The percentage of the /var directory utilized by the node is unknown, for example, because the node is not connected.
App Logic	<p>Application Logic function status for the node.</p> <ul style="list-style-type: none"> UP— Application Logic function is running on node. DOWN—Application Logic function enabled on the node but is not running. Unknown—Status for the application logic function is unknown, for example, because the node is not connected. N/A— Application Logic function is not configured to run on the node. (Master)—The configured primary node in the fabric.
Database	<p>Database function status for the node.</p> <ul style="list-style-type: none"> UP—Database function is running on node. DOWN—Database function that is enabled on the node but is not running. Unknown—Status for the Database function is unknown, for example, because the node is not connected. N/A—Database function is not configured to run on the node. <p>NOTE: By default, the Database function is enabled on no more than two nodes in the fabric.</p>
Hardware Model	<p>Model of Junos Space Appliance.</p> <p>NOTE: Hardware model appears when you double-click a thumbnail or table row for a detailed view of the node.</p> <p>NOTE: Hardware model only applies for a Junos Space physical appliance.</p>
Load Balancer	<p>Load Balancer function for the node.</p> <ul style="list-style-type: none"> UP – Load Balancer function is running on the node. DOWN – Load Balancer function that is enabled on the node is not running. Unknown – Status for the Load Balancer function is unknown, for example, because the node might not be connected. N/A – Load Balancer function is not running because it is not configured to run on the node. <p>NOTE: By default, the Load Balancer function is enabled on no more than two nodes in the fabric.</p> <ul style="list-style-type: none"> (VIP)—The configured virtual IP node in the fabric.
Serial Number	<p>Serial Number for the Junos Space appliance.</p> <p>NOTE: Serial number appears when you double-click a thumbnail or table row for a detailed view of the node.</p>

Table 57: Fields for the Fabric Monitoring Inventory Page (*continued*)

Field	Description
Software Version	Junos Space Release Version.

NOTE: Software version appears when you double-click a thumbnail or table row for a detailed view of the node.

For more information about manipulating data on the Fabric Monitoring inventory page, see [“Inventory Pages Overview” on page 28](#)

Performing Fabric Node Actions

To perform an action:

- Select a node by clicking its check box in either view and select an action from the Action Drawer.
- Right-click a node and select an action from the pop-up menu.

From the Fabric Monitoring inventory page, you can perform the following actions:

- Shut Down Node—Shuts down or reboots fabric nodes (appliances or virtual machine hosts) when you move them or reconfigure their network settings. See [“Shutting Down or Rebooting a Node From Junos Space” on page 420](#).
- Delete Node—Removes node from the Junos Space fabric directly if there is a physical or virtual appliance failure. See [“Deleting a Node” on page 421](#).
- Tag It—Apply a tag to a fabric node. See [“Tagging an Object” on page 495](#).
- View Tags—View tags applied to a fabric node. See [“Viewing Tags” on page 496](#).
- Untag It—Remove a tag from a fabric node. See [“Untagging Objects” on page 497](#).
- Clear All Selections—Clears the selection from all objects selected on the inventory page.

Related Documentation

- [Understanding Overall System Condition and Fabric Load on page 422](#)
- [Fabric Management Overview on page 405](#)
- [Inventory Pages Overview on page 28](#)

Configuring Node Network Settings

The Junos Space fabric consists of one or multiple nodes. Network settings for these nodes enable IP connectivity to external systems as well as internal connectivity between nodes. During the initial set up of a node, the Junos Space super administrator configures node networking settings through the CLI interface. However, You can not use the CLI interface to change network settings.

To change network settings, navigate to Platform > Manage Fabric > Network Settings. Changing network settings allow you to move Junos Space fabric from one network location to another location without reinstallation.

Existing settings for both the management interface and device management interface (IP address, net mask and default gateway) for all nodes are displayed in a table. The settings for a node are displayed as a row in the table.

Nodes require restart to apply new network settings.

This topic includes the following topics:

- [Network Settings Configuration Guidelines on page 416](#)
- [Changing the VIP Interface in the Same Subnet on page 416](#)
- [Changing the Node Management IP in the Same Subnet on page 416](#)
- [Changing the Default Gateway on page 417](#)
- [Changing the Management IP to a Different Network on page 417](#)
- [Adding the Device Management IP Address on page 417](#)
- [Changing the Device Management IP Address in the Same Subnet on page 418](#)
- [Changing the Device Management IP Address to a Different Network on page 418](#)
- [Deleting a Device Management IP Address on page 418](#)
- [Changing the VIP Interface to a Different Network on page 419](#)
- [Changing the Node Management IP Address of All Nodes in the Fabric to the Same Subnet on page 419](#)
- [Changing the VIP interface of a Multi-Node Fabric to a Different Network on page 419](#)

Network Settings Configuration Guidelines

- The VIP interface and Node IP address should be in the same subnet.
- The node management IP address of the first two nodes in the fabric must be in the same subnet.
- When you modify the device management IP address, all the devices connected to that node should be updated with the new device management IP address.

Changing the VIP Interface in the Same Subnet

There is only one VIP for the entire fabric.

Changing the Node Management IP in the Same Subnet

To change the node management IP in the same subnet:

1. Click the pencil icon for the node on which you want to change the management IP.
The settings appear for you to modify
2. Change the management IP in the same subnet.

3. Click OK.
4. Click Modify.

The Shutdown/reboot confirmation dialog box appears.

Changing the Default Gateway

To change the default gateway:

1. Click the pencil icon for the node on which you want to change the default gateway.
The settings appear for you to modify
2. Change the default gateway.
3. Click OK.
4. Click Modify.

The Shutdown/reboot confirmation dialog box appears.

Changing the Management IP to a Different Network

To change the management IP to a different network:

1. Click the pencil icon for the node on which you want to change the management IP.
The settings appear for you to modify.
2. Change the management IP from a different network.
3. Change the VIP, subnet mask, and default gateway.
4. Click OK.
5. Click Modify.

The Shutdown/reboot confirmation dialog box appears.

Adding the Device Management IP Address

To add the device management IP address:

1. 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.
2. Click Add.
3. Add the VIP, subnet mask, and default gateway for the device management interface.
4. Click OK.
5. Click Modify.

The Shutdown/reboot confirmation dialog box appears.

Changing the Device Management IP Address in the Same Subnet

To change the device management IP address in the same subnet:

1. Click the pencil icon for the node on which you want to change the device management IP.

The settings appear for you to modify.

2. Change the device management IP to a new one in the same subnet.
3. Click OK.
4. Click Modify.

The Shutdown/reboot confirmation dialog box appears.

Changing the Device Management IP Address to a Different Network

To change the device management IP address to a different network:

1. Click the pencil icon for the node on which you want to change the device management IP.

The settings appear for you to modify.

2. Change the device management IP to a new in a different subnet.
3. Change the subnet mask and default gateway.
4. Click OK.
5. Click Modify.

The Shutdown/reboot confirmation dialog box appears.

Deleting a Device Management IP Address

To delete a device management IP address

1. 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.

2. Uncheck the Enable device management interface option.
3. Click OK.
4. Click Modify.

The Shutdown/reboot confirmation dialog box appears.

Changing the VIP Interface to a Different Network

The VIP interface and the node IP should be in the same subnet.

To change the VIP interface to a different network:

1. Change the VIP interface to a different network.
2. Change the node IP address.
3. Click OK.
4. Click Modify.

The Shutdown/reboot confirmation dialog box appears.

Changing the Node Management IP Address of All Nodes in the Fabric to the Same Subnet

To change the node management IP address and all nodes in the fabric to the same subnet:

1. 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.

2. Change the node management IP address to a new one in the same subnet.
3. Click OK.
4. Repeat Steps 1 through 3 for each node in the fabric.
5. Click Modify.

The Shutdown/reboot confirmation dialog box appears.

Changing the VIP interface of a Multi-Node Fabric to a Different Network

The node IP address and the VIP interface must be in the same subnet.

To change the VIP interface of a multi-node fabric to a different network:

1. Change the VIP interface to a new one in a different network.
2. Change the node IP address.
3. Click OK.
4. Repeat Steps 1 through 3 for each node in the fabric.
5. Click Modify.

The Shutdown/reboot confirmation dialog box appears.

Related Documentation

- [Shutting Down or Rebooting a Node From Junos Space on page 420](#)

Shutting Down or Rebooting a Node From Junos Space

From Junos Space, the super administrator can shut down or reboot fabric nodes (appliances or virtual machine hosts) when they are moved or their network settings reconfigured. You can shut down or reboot a fabric node using the **Platform > Administration > Manage Fabric > Shut Down Node** action. Optionally, you can enter a message to display to administrators logged in to an affected node.

To shut down or reboot a node in the fabric,

1. Select the node and either select from the right mouse-click menu or-from the Actions drawer the appropriate action, either **Shutdown Node** or **Reboot Node**.

The **Reboot Node/Shutdown Node** dialog box appears.

2. Select the appropriate action by clicking either the **Shutdown** or the **Reboot** option button.
3. (Optional) You can enter a message to be displayed to console users (for any administrator logged into the node using the CLI. The message appears on UNIX shell).

If you do not enter anything, console users will see either **Junos Space shutdown** or **Junos Space reboot** on the shell.

4. Click **Confirm**.

The shut down or reboot action occurs.

**Related
Documentation**

Deleting a Node

You can delete a node from the Junos Space fabric directly using **Platform > Administration > Manage Fabric > Fabric Monitoring > Delete Node**. You must remove the deleted node from the network and re-image it. Thereafter, you can add it to the fabric using **Platform > Administration > Manage Fabric > Add Fabric 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 there is another node that has the capacity to assume that role. You are prompted to enable that role on another candidate node before deleting that node. If you delete a high availability node, but there is not another node to transfer that role, high availability does not occur.

When you delete a fabric node, Junos Space does the following:

- Removes reference to that node host name and IP address from remaining nodes.
- Stops database replication on both the deleted node and the back up database node.
- The database backup copy in that node will not be available for the remaining cluster to restore from that copy
- Copies the database to the new database node.
- Shuts down all services that interact with other nodes.

You can delete only one node at a time. You must have Super Administrator or System Administrative role access privileges to delete a node.

To delete a node:

1. Select **Platform > Administration > Manage Fabric**.

Select the node that you want to delete, and select **Delete Node** from the Actions drawer.

You can also right-click the node and select **Delete Node** from the pop-up menu.

The Fabric Monitoring inventory page tabular view displays at a glance whether a node is configured for high availability. Look for Up in the Database and Load Balancer columns.

2. In the Warning dialog box, confirm that you want to delete the node by clicking **Continue**.
 - If a node you want to delete is not configured for high availability or a node is configured for high availability but there is no other node available to assume that role, the **Delete Node** dialog box appears displaying the node name and management IP address of only the node you want to delete.

- If a node is configured for high availability, the **Delete Node** dialog box notifies you of that fact and lists all candidate nodes that have the capacity to take over that role.
- 3. In the **Delete** dialog box, select the node you want to delete.
- 4. Click **Delete**.

Node deletion is scheduled as a job immediately after you click **Delete**. The Delete Node action is also audit logged. The **Delete Fabric Node Job Information** dialog box appears.
- 5. In the **Delete Fabric Node Job Information** dialog box, click the **Job ID** link.

Job Manager displays the **View Job Details** dialog box for you to verify and monitor delete node information, such as job type, job ID, percent complete, job state, scheduled start and end time, user name, and a brief job summary.
- 6. If a problem occurs in the delete node job, you can troubleshoot by viewing the job status in the **Platform > Audit Logs > View Audit Logs** inventory page.



NOTE: When you delete a node, a UDP communication exception occurs. This behavior is normal.



NOTE: When you delete a load balancer node, a VIP switch may occur and cause the Junos Space progress indicator to appear. This behavior is normal.

**Related
Documentation**

- [Fabric Management Overview on page 405](#)
- [Viewing Nodes in the Fabric on page 412](#)
- [Adding a Node to an Existing Fabric on page 409](#)

Understanding Overall System Condition and Fabric Load

You can view the overall Junos Space system condition and fabric load from the platform application dashboard or from the Administration workspace landing page.

System Condition

To calculate the overall system condition, Junos Space uses an algorithm based on cluster health and node-function health:

- Cluster health indicates the percentage of nodes in the fabric that are currently running.

For example, if only three nodes are reachable in a four-node fabric, cluster health is 75%.
- Load-balancer health indicates the percentage of nodes (enabled for load balancing) that are running the load balancing process.

For example, if two nodes are enabled for load balancing and the load-balancing process is running on only one node, the load-balancing health is 50%.

- Database health indicates the percentage of nodes (enabled for database requests) that are running the database process.

For example, if two nodes are enabled as database server and the database process is running on only one node, then database health is 50%.

- Application-logic health indicates the percentage of nodes (enabled for application logic (DML and business logic)) that are running the application-logic process.

For example, if three nodes are enabled for application logic and the application-logic process is running on only two nodes, then application-logic health is 67%.

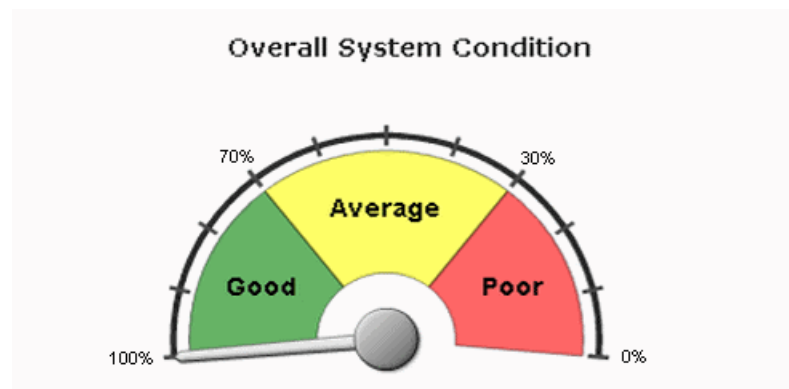
Junos Space retrieves data on the nodes and the node functions running, and then applies the following algorithm to determine the overall system condition:

$$\text{overall system condition} = \left[\frac{\text{number of nodes running}}{\text{number of nodes in fabric}} \right] * \left[\frac{\text{number of nodes running load balancing process}}{\text{number of nodes enabled for load balancing}} \right] * \left[\frac{\text{number of nodes running database server process}}{\text{number of nodes enabled as database server}} \right] * \left[\frac{\text{number of nodes running application logic process}}{\text{number of nodes enabled for application logic}} \right]$$

Using the preceding examples for cluster health and node-function health, the overall system condition is expressed as a percentage:

$$\text{overall system condition} = 75\% * 50\% * 50\% * 67\% = 12.5\%$$

The Overall System Condition dialog box indicates Poor (0–30%), Average (30–70%), or Good (70–100%), based on the value the algorithm returns.

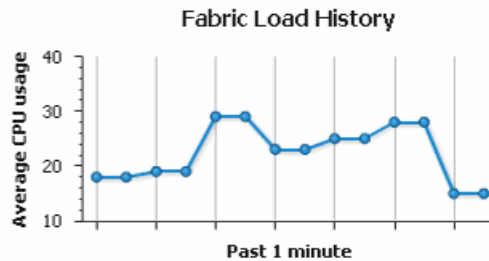


The overall system health indicates 0% (Poor) when any one of the following conditions is detected:

- No nodes in the fabric are running.
- No nodes enabled for load balancing are running the load balancing process.
- No nodes enabled for database requests are running the database process.
- No nodes enabled for application logic are running the application logic process.

Fabric Load

The Fabric Load chart displays the average CPU usage across all nodes that are running in the fabric.



Junos Space uses the following algorithm to determine the fabric load:

$$\text{fabric load} = [\text{total CPU usage for all nodes running}] / [\text{number of nodes running}]$$

For example, given a fabric with three nodes running and CPU usage of 80%, 30%, and 10%, respectively, the fabric load is 40%. The following example illustrates how the fabric load is calculated.

$$\begin{aligned} \text{fabric load} &= [80\% + 30\% + 10\%] / 3 \\ \text{fabric load} &= 120\% / 3 \\ \text{fabric load} &= 40\% \end{aligned}$$

To view the average CPU use at a specific data point, drag the mouse over the data point of interest.

To obtain details about the status of the fabric, click any data point in the graph. The Fabric Monitoring dialog box appears and shows detailed status for each node in the fabric. Status information includes CPU, disk, and memory usage and indicates up or down status for each node function enabled on the node.

- Related Documentation**
- [Fabric Management Overview on page 405](#)
 - [Junos Space User Interface Overview on page 11](#)

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 logical components of the nodes such as memory, availability, load, and so on, are available through the SNMP protocol. The threshold values for these components are defined by the system. You can also specify the values for certain parameters. Junos Space is informed whenever these threshold values are crossed and sends you a notification. Henceforth, this is referred to as self-monitoring.

To enable self monitoring:

1. Select **Platform > Administrator > Manage Fabric**. The Manage Fabric page appears.

2. Select the node you want to track and click **SNMP Start** from either the Actions drawer or from the right-click context menu.

Junos Space monitors the status of the selected node and notifies you whenever the threshold values are crossed.

To specify certain parameters for self-monitoring:

1. Select **Platform > Administrator > Manage Fabric**. The Manage Fabric page appears.
2. Select the node that you want to set threshold values for and click **SNMP Configuration** from either the Actions drawer or from the right-click context menu.
The SNMP Configuration dialog box appears.
3. Enter the external SNMP manager IP address in the **SNMP Manager IP** field.
4. Enter a value between 0 and 100 to specify the threshold value for disk usage in the **Disk Usage(%)** field. This is the maximum percentage of the /var directory that can be utilized by the node. The default value is 5%.
5. Enter the threshold value for system load average in the **System Load** field. This is the maximum percentage of CPU resource that can be utilized by the node. The default value is 4.
6. Click **Confirm** to save your settings and return to the Manage Fabric page.

To disable self-monitoring:

1. Select **Platform > Administrator > Manage Fabric**. The Manage Fabric page appears.
2. Select the node you want to stop tracking and click **SNMP Stop** from either the Actions drawer or from the right-click context menu.

Junos Space stops tracking the selected node.

Related Documentation

- [Understanding Overall System Condition and Fabric Load on page 422](#)
- [Fabric Management Overview on page 405](#)
- [Inventory Pages Overview on page 28](#)
- [Viewing Nodes in the Fabric on page 412](#)

Creating a System Snapshot

You can use the System Snapshot feature to create a snapshot of the system state and rollback the system to a predefined state. The snapshot includes all persistent data on the hard disk including data in the database, system and application configuration files, and application and Linux executables. The System Snapshot is a fabric-wide operation that maintains consistency across all nodes in the fabric.

Typically, you would use the System Snapshot feature for rolling back the system when it is in an unrecoverable error-state due to corruption of system files, interruption of critical processes, etc.. You can also roll back the system to an older release if the system exhibits undesirable behaviors after a software version upgrade.



TIP: We recommend using System Snapshot before performing significant actions (Add/Delete Node, Application Installation) and such actions that have the potential to precipitate the system into an undesirable state. You can delete the snapshot after you have ascertained that these actions were performed successfully.

System Snapshot is currently supported on a Junos Space fabric that consists of only Space VM or only Space Appliance. This feature is not supported on a hybrid fabric consisting of both Space VM and Space Appliance.

System Snapshot does not impact the performance of a Space VM. However, if you are using a Space Appliance, performance may be impacted by the number of write operations performed to the snapshot's logical volume.

The maximum size that a snapshot can occupy for a new 11.3 Space Platform is 300GB. The maximum size that a snapshot can occupy for a Space Platform migrated from releases prior to 11.3 is 43GB. On the Real Appliance, the snapshot will become invalid if it has been kept for a long time, because the snapshot volume disk space usage increases as write operations continue. Once the usage reaches the maximum size of snapshot volume, the snapshot will be disabled. Therefore, ensure that you clear enough hard disk space to accommodate the snapshot.

If you are upgrading Network Application Platform from releases prior to 11.3, perform the following steps before using the System Snapshot feature:

1. Connect the recovery USB/CD to Space Appliance, and reboot to set USB/CD as the first boot option.
2. Restart the box, and choose the **rescue-serial** mode while booting.
3. Follow the on-screen steps and choose **Skip** when asked whether you want to find an existing Space installation and mount to `mnt/sysimage`.
4. Once you are in the recovery shell, execute the following sequence of commands:
 - a. `lvm vgchange -ay jmpvgnocf`
 - b. `e2fsck -f /dev/jmpvgnocf/lvroot`
 - c. `resize2fs -f /dev/jmpvgnocf/lvroot 900G`
 - d. `lvm lvreduce -L1024G /dev/jmpvgnocf/lvroot`
 - e. `resize2fs -f /dev/jmpvgnocf/lvroot`

After executing these commands, start creating the snapshot. The steps used to create a system snapshot for a Space VM and a Space Appliance are almost identical, but there are two additional preliminary steps for the Space VM:

If you are working with a Space VM:

- a. Select **Administration > Manage 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. From the navigation ribbon, select **Administration > Manage Fabric > System Snapshot**.

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 can store only one System Snapshot.

2. Click **Take Snapshot**.

The System Snapshot Confirmation dialog box appears.

3. Enter the name of the snapshot in the Snapshot Name box.
4. Enter the comments in the Comment box.
5. Click **Confirm**.

A new job is created and the job ID appears in the System Snapshot Job Information dialog box.

6. Click the job ID to view more information about the job created. This action directs you to the Job Management work space.

The time taken to complete the snapshot job for a VM is dependent on the number of nodes in the fabric, the disk size of the VM, the memory size of the VM, and the performance of the ESX server. The time taken to complete the snapshot job for a Space Appliance is dependent on the disk space used on the appliance.



NOTE: You may not be able to create a snapshot of the system state if any of the following conditions are true:

- Insufficient disk space on ESX servers.
- Mis-configuration on one of the ESX servers.
- One of the nodes is down.
- Hybrid fabric consisting of both Space VM and 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 428](#)
- [Restoring the System to a Snapshot on page 428](#)

Deleting a System Snapshot

To delete a System Snapshot:

1. From the navigation ribbon, select **Administration > Manage Fabric > System Snapshot**.
2. Click **Delete**.

The System Snapshot Deletion dialog box appears. A new job is created and the job ID appears in the System Snapshot Job Information dialog box.

3. Click the job ID to view more information about the job created. This action directs you to the Job Management work space.



NOTE: You may not be able to delete a snapshot of the system state if any of the following conditions are true:

- Mis-configuration on one of the ESX servers.
- Hybrid fabric consisting of both Space VM and Space Appliance.
- Snapshot does not exist.

Related Documentation

- [Creating a System Snapshot on page 425](#)
- [Restoring the System to a Snapshot on page 428](#)

Restoring the System to a Snapshot

The process to restore a system to a snapshot is differs depending on whether you are using a VM or an Appliance.

To restore a system snapshot when using a VM:

1. From the navigation ribbon, select **Administration > Manage Fabric > System Snapshot**.
2. Click **Restore**.
3. Click **OK**.
4. Login to the ESX servers and power on the VM after few minutes.



NOTE: If the Space GUI is not accessible on a VM, you can restore the fabric by shutting down every node in the fabric and logging into ESX servers where the VM is located.

To restore a System Snapshot when using an Appliance:

1. From the navigation ribbon, select **Administration > Manage Fabric > System Snapshot**.
2. Click **Restore**.

The System Restore Instruction for Appliance dialog box appears.

3. Follow the instructions on this dialog box.
4. Click **OK**.



NOTE: You may not be able to restore the system to a snapshot if one of the following conditions are true:

- One of the nodes is down.
- New nodes were added after a snapshot was created. A warning message that prompts you to delete the new nodes before restoring is shown.
- Some nodes were deleted after a snapshot was created. A warning message that prompts you to restore the nodes before restoring is shown.

**Related
Documentation**

- [Creating a System Snapshot on page 425](#)
- [Deleting a System Snapshot on page 428](#)

CHAPTER 37

Manage Databases

- [Database Backup and Restore Overview on page 431](#)
- [Backing Up the Database on page 433](#)
- [Restoring a Database in the User Interface on page 437](#)
- [Restoring a Database in Maintenance Mode on page 440](#)
- [Viewing Database Backup Files on page 442](#)
- [Deleting Database Backup Files on page 443](#)
- [Viewing Job Recurrence on page 444](#)

Database Backup and Restore Overview

The system administrator can perform Junos Space database backup, restore, and delete operations from the Platform > Administration > Manage Databases workspace. The administrator can initiate a database backup operation from either the Manage Databases > Backup Database task or from Junos Space Maintenance Mode. In both cases, the backup database operation occurs in Maintenance Mode.

The backup database operation can be performed both locally or remotely. SCP is the protocol used for transferring the backup to a remote host.

By default, Junos Space automatically backs up the database once a week. However, the administrator can schedule a backup to run at anytime and perform either local or remote backups. All jobs that completed prior to the time the backup operation starts are captured in the database backup file.

To perform database backup or restore operations, a Junos Space user must be assigned the system administrator role.

Restore the Junos Space database if any of the following conditions occur:

- Junos Space data is corrupted, and you need to replace it with uncorrupted data.
- The Junos Space software became corrupted, and you reinstalled the Junos Space software.
- You upgraded to a new version of Junos Space and need to populate the Junos Space database with existing data.

Backing up a Database

The system administrator can back up a Junos Space database from the Platform > Administration > Manage Databases > Backup Database task. During a backup, Junos Space 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. The administrator can perform a local or remote database backup. When the administrator performs a local backup, Junos Space 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. When the administrator performs a remote database backup, Junos Space backs all data and log files to a remote location on a network hosts or media.

For a remote backup, use only a Linux-based server. You must specify a remote host that is configured to run the Linux Secure Copy (SCP) command. You must also specify a valid user ID and password for the remote host. To ensure that you are using a valid directory, check the destination directory before you initiate a database backup to the remote system.

For more information about backing up a database, see [“Backing Up the Database” on page 433](#).

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 database to a previous state. The administrator can restore the database from the Junos Space user interface (Platform > Administration > Manage Databases workspace) (see [“Restoring a Database in the User Interface” on page 437](#)), or directly from the Maintenance Mode Actions dialog box (if Junos Space goes down and you cannot access the user interface) (see [“Restoring a Database in Maintenance Mode” on page 440](#)).

When a user initiates a restore database operation from the user interface, Junos Space prompts the user for the user name and password to enter maintenance mode. When the user is authenticated, Junos Space initiates the restore database operation and Junos Space remains in maintenance mode until the database is restored. When Junos Space is in maintenance mode, Junos Space is down on all nodes in the fabric and only the web proxy is running. During this time, all Junos Space users, except the maintenance mode administrator, are locked out of the Junos Space system. When the restore operation completes and the administrator exits maintenance mode, Junos Space is restarted on all nodes, and users can again access the system through the Junos Space user interface.

Related Documentation

- [Restoring a Database in the User Interface on page 437](#)
- [Restoring a Database in Maintenance Mode on page 440](#)
- [Backing Up the Database on page 433](#)
- [Maintenance Mode Overview on page 402](#)

Backing Up the Database

The system administrator can make a backup copy of the Junos Space database and, at a later time, use the backup file to restore the Junos Space database to a previous state. The database backup file contains configuration data for managed nodes, managed devices, deployed services, scheduled jobs, Junos Space users, and so forth.

The administrator can perform local and remote backup and restore operations. You perform a local backup to copy the backup file to the default directory `/var/cache/jboss/backup`. You perform a remote backup to copy the backup file to remote network hosts or media.

This topic includes the following tasks:

- [Backing Up the Database to a Local Directory on page 433](#)
- [Backing Up the Database to a Remote Host on page 434](#)

Backing Up the Database to a Local Directory

To back up the Junos Space database to a local directory:

1. Navigate to the **Platform > Administration > Manage Databases > Backup Database**.

The Backup Database dialog box appears. The default behavior is a backup occurring once weekly, which appears in the Schedule at a later time section, under Repeat.

2. In the Mode field, select **local** to back up the Junos Space database to the default directory `/var/cache/jboss/backup`.



NOTE: When you select the local mode option, the Username, Password, Confirm password, Machine IP, and Directory text boxes in the Backup Database dialog box are disabled.

3. Optional: In the Comment box, add a comment to describe or otherwise identify the backup operation.
4. Optional: Schedule the database backup to occur at a later time. Click **Schedule at a later time** to expand the schedule area of the Backup Database dialog box. Specify a back up database start date and time.



NOTE: The selected time in the scheduler corresponds to Junos Space server time but using the local time zone of the client computer.

5. Optional: Schedule database backup recurrence by clicking **Repeat** to reveal its controls.

- a. Specify the database backup recurrence by setting the interval and the increment.

Unit of Time	Increment
Minutes	1-59
Hours	12:00 AM - 11:45 PM
Days	1-6
Weeks	1-4
Weekdays	Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday
Weekends	Saturday, Sunday,
Monday/Wednesday/Friday	Monday, Wednesday, Friday
Tuesday/Thursday	Tuesday, Thursday
Fortnight (14 days)	1-26
Months	1-12, plus date of recurrence expressed as a date, and as one the first, second, third, fourth or last Monday-Sunday of the month.
Years	1-50, plus date of recurrence expressed as a date, and as one the first, second, third, fourth or last Monday-Sunday of the month.

Where 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 drop-down list box. If you do not specify a recurrence end, the database backup will reoccur endlessly until you cancel the job manually.

6. Click **Backup**.

The database is backed up. The **Order Information** dialog box appears.

7. Optional: Click the Job ID in the Order Information dialog box to view the database backup job details in the View Job Details dialog box.

8. Click **OK**.

The Junos Space database backup appears on the Manage Databases inventory page. See "[Viewing Scheduled Jobs](#)" on page 347.

Backing Up the Database to a Remote Host

The protocol used to transfer the database backup to a remote host is SCP, Secure Copy Protocol..

To back up the Junos Space database to a remote host:

1. Navigate to the **Platform > Administration > Manage Databases > Backup Database**.

The Backup Database dialog box appears.

2. In the Mode field, select **remote**.
3. Enter a username to access the remote host server.
4. Enter the corresponding password.
5. Reenter the password.
6. Enter the remote host server IP address.
7. Enter a directory path on the remote host server for the database backup file.



NOTE: The directory path must already exist on the remote host server.

8. Optional: Add a comment to describe or otherwise identify the backup operation.

9. Optional: Schedule the Junos Space database backup operation to occur at a later time. Click the down-arrow to expand the schedule area of the dialog box.

- Clear the **Schedule at a later time** check box (the default) to initiate the database backup when you click Backup.
- Select the **Schedule at a later time** check box to specify a later start date and time for the database backup.



NOTE: The selected time in the scheduler corresponds to Junos Space server time but using the local time zone of the client computer.

10. Optional: Schedule database backup recurrence by clicking the **Repeat** arrow.

The Repeat area expands.

a. Specify the database backup recurrence by setting the interval and the increment:

Unit of Time	Increment
Minutes	1-59
Hours	12:00 AM - 11:45 PM
Days	1-6
Weeks	1-4
Weekdays	Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday
Weekends	Saturday, Sunday,
Monday/Wednesday/Friday	Monday, Wednesday, Friday
Tuesday/Thursday	Tuesday, Thursday
Fortnight (14 days)	1-26
Months	1-12, plus date of recurrence expressed as a date, and as one the first, second, third, fourth or last Monday-Sunday of the month.
Years	1-50, plus date of recurrence expressed as a date, and as one the first, second, third, fourth or last Monday-Sunday of the month.

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 drow-down list box. If you do not specify a recurrence end, the database backup will reoccur endlessly until you cancel the job manually.

11. Click **Backup**. The database back up occurs.

The Order Information dialog box appears.

12. Optional: Click the Job ID in the Order Information dialog box to view job details for the database backup. The View Job Details dialog box appears.

13. Click **OK** to close the View Job Details dialog box.

When the backup operation finishes, the Junos Space database backup file appears in the Manage Databases inventory page.

Related Documentation

- [Restoring a Database in the User Interface on page 437](#)
- [Restoring a Database in Maintenance Mode on page 440](#)
- [Viewing Database Backup Files on page 442](#)
- [Deleting Database Backup Files on page 443](#)
- [Database Backup and Restore Overview on page 431](#)
- [Viewing Audit Logs on page 359](#)
- [Viewing Scheduled Jobs on page 347](#)

Restoring a Database in the User Interface

You can restore any archived Junos Space database to restore your Junos Space system to a previous state. When you initiate a restore database operation, Junos Space is shutdown on all nodes in the fabric and the system goes into maintenance mode, during which time only one maintenance mode administrator can log in to the system at a time. Once the restore database operation is complete, Junos Space is restarted and users can access the Junos Space user interface.

To restore a database, you must have System Administrator privileges and be a Maintenance Mode administrator.



NOTE: Before you restore a database, wait until all jobs currently running have completed.

To view information about the available database backup files before you select a database to restore, see [“Viewing Database Backup Files” on page 442](#).

Junos Space supports both local and remote backup and restore operations.

- [Restoring a Local Database on page 438](#)
- [Restoring a Database from a Remote Host on page 439](#)

Restoring a Local Database

To restore the Junos Space database to a previous state:

1. Navigate to the **Platform > Administration > Manage Databases**.

The Manage Databases inventory page appears displaying the previous database backups.

2. Select the database backup file you want to restore.

In the thumbnail view, slide the slider to the far right position. You see the database back up file detailed information for the selected database backup.

3. Open the Actions drawer and select **Restore Database**.

The Restore Database confirmation dialog box appears.



WARNING: You must log in to Junos Space Maintenance mode. Junos Space 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 during the restore database operation.

4. Click **Continue** in the Restore Database dialog box.

Junos Space prompts you enter a user name and password to enter maintenance mode.

5. Enter the maintenance mode user name and password.

6. Click **OK**.

Junos Space 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, and returns to normal operational mode.

The process of exiting maintenance mode and restarting Junos Space takes several minutes.

Restoring a Database from a Remote Host

To restore the Junos Space database to a previous state:

1. Navigate to the **Platform > Administration > Manage Databases**.

The Manage Databases inventory page appears displaying the previous database backups.

2. Select the database backup file you want to restore.
3. In thumbnail view, slide the slider to the far right to view the database backup detailed information. In tabular view the database backup detailed information appears in the table columns.
4. Open the Actions drawer and select **Restore Database**.

The Restore Database confirmation dialog box appears.



WARNING: You must log in to Junos Space Maintenance mode. Junos Space 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 during the restore database operation.

5. Click **Continue** in the Restore Database dialog box.

Junos Space prompts you enter a user name and password to log in to Maintenance mode.

6. Enter the maintenance mode user name and password.
7. Click **OK**.

Junos Space 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.

8. In the Restore Database Status dialog box, click **Return to Maintenance Menu**.

The Maintenance Mode Actions dialog box appears.

9. In the Maintenance Mode Actions dialog box, click **Log Out and Exit from Maintenance Mode**. This action exits maintenance mode, starts up Junos Space, and returns to normal operational mode.

The process of exiting maintenance mode and restarting Junos Space takes several minutes.

Related Documentation

- [Backing Up the Database on page 433](#)
- [Viewing Database Backup Files on page 442](#)
- [Deleting Database Backup Files on page 443](#)

- [Maintenance Mode Overview on page 402](#)
- [Restoring a Database in Maintenance Mode on page 440](#)

Restoring a Database in Maintenance Mode

In Junos Space, maintenance mode is a special mode that an administrator can use to restore the database when Junos Space is down on all nodes in the fabric and the Web proxy is running.

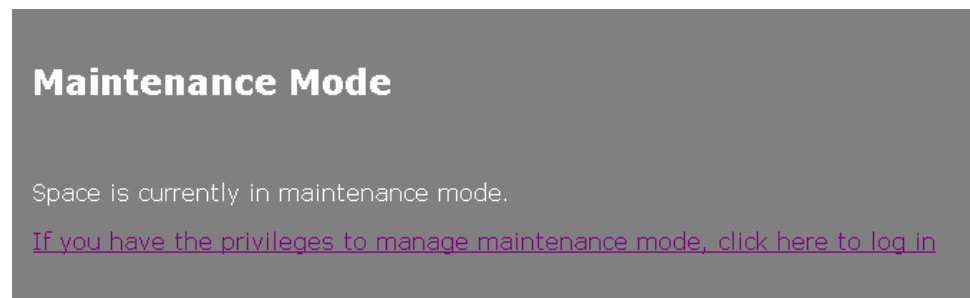
To restore a database in maintenance mode:

1. Connect to a Junos Space appliance in maintenance mode using the following URL, where *ip-address* is the Web access IP address for the appliance:

`https://ip-address/maintenance`

The Maintenance Mode dialog box appears.

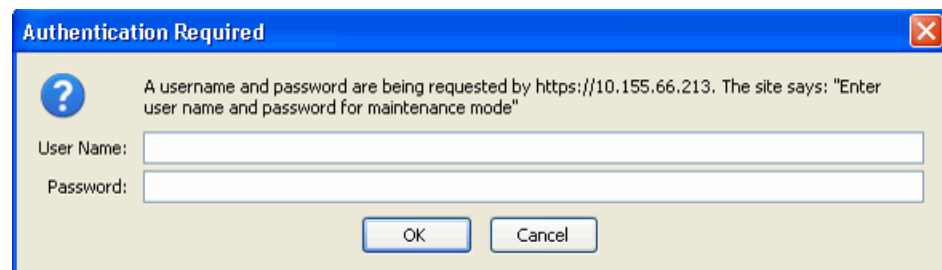
Figure 136: Maintenance Mode Dialog Box



2. Click the link to log in.

The Authentication Required dialog box appears.

Figure 137: Authentication Required Dialog Box



3. Enter the user name and password for maintenance mode access.
4. Click **OK**.

The Maintenance Mode Actions dialog box appears.

Figure 138: Maintenance Actions

- [Restore Database from Backup](#)
This action leads user to select a database backup file and overwrite the current database
- [Download Troubleshooting Data and Logs](#)
This action allows user to download Space logs for troubleshooting
- [Log Out and Remain in Maintenance Mode](#)
This action logs out the current user so that another administrator can login and manage in maintenance mode
- [Log Out and Exit from Maintenance Mode](#)
This action returns Space to normal operational mode

5. Click the link **Restore Database from Backup** in the Maintenance Mode Actions dialog box.

Junos Space displays the available database backup files, as shown in the following example.

Figure 139: Selection Box

Choose a backup database to restore

☒ db_1255398948.gz (test1) created at Mon Oct 12 18:55:49 2009

[Return to Maintenance Menu](#)

6. From the available database backup files, select a database backup file to overwrite the current database.
7. Click **Submit**.

The database is restored from the backup copy you selected.

Figure 140: Confirmation Message

Space database is being restored from a backup copy : db_1255650255.gz

Restore database success!

[Return to Maintenance Menu](#)

8. Click **Return to Maintenance Menu**.
The Maintenance Mode Actions dialog box appears.
9. Click **Log Out and Exit from Maintenance Mode**.
Junos Space returns to normal operational mode.

Related Documentation

- [Maintenance Mode Overview on page 402](#)
- [Database Backup and Restore Overview on page 431](#)

- [Backing Up the Database on page 433](#)
- [Restoring a Database in the User Interface on page 437](#)

Viewing Database Backup Files

The Manage Databases inventory page displays information about Junos Space database backups, including the date and time of the backup, the backup file name and location, and the IP address of the Junos Space appliance that was backed up. From the Manage Databases inventory page, the administrator can restore a database or delete a database backup.

- [Changing Views on page 442](#)
- [Viewing Database Details on page 442](#)
- [Manage Database Commands on page 443](#)

Changing Views

You can view database back information in thumbnail or tabular views. By default, Manage Database data displays in thumbnail view. In thumbnail view databases are represented by an icon has a database backup name and the date the back occurred. In tabular view, each database backup is represented by a row in the table,

To change views:

1. Navigate to the **Platform > Administration > Manage Databases**.
The Manage Databases inventory page appears.
2. Click a view indicator at the right of the Manage Databases page title bar.

Viewing Database Details

To view detailed database backup information:

- Double-click a database in either thumbnail or tabular views. The Database Backup Details page appears.
- In thumbnail view, move the zoom slider to the far right to display detailed information.

[Table 58 on page 442](#) defines the database backup detailed information.

Table 58: Fields in the Manage Databases Table

Field	Description
Name	The name of the database backup file. Junos Space automatically assigns a name to the backup file.
Backup Date	Date and time of the database backup.
Comment	Information a Junos Space user optionally provides in the Comments field of the Backup Database dialog box when scheduling database backup.

Table 58: Fields in the Manage Databases Table (*continued*)

Machine	IP address of the appliance on which the database backup was performed.
File Path	File path for the database backup.

Manage Database Commands

From the Manage Database inventory page, you can perform the following actions:

- Delete Database Backup—“[Deleting Database Backup Files](#)” on page 443
- Restore Database—“[Restoring a Database in the User Interface](#)” on page 437
- Tag It—“[Tagging an Object](#)” on page 495
- View Tags—“[Tagging an Object](#)” on page 495
- Clear All Selections—Clears all selections you made using the Select Page link. You can also clear all selections by clicking the Select None link.

Deleting Database Backup Files

The system administrator can delete archived database backup files that are no longer useful for restore operations.



NOTE: When you delete a database backup file from the Manage Databases inventory page, the backup file is permanently deleted from Junos Space and cannot be retrieved or restored.

To delete a Junos Space database backup file:

1. Navigate to the **Platform > Administration > Manage Databases**.

The Manage Databases inventory page appears.

2. From the Manage Databases inventory page (thumbnails or table view), select one or more database backup files that you want to delete.
3. Optional: View the database backup file detailed information before deleting the file. In thumbnail view the slider to the far right. In tabular view, detailed database backup file information appears as columns in the table.
4. From the Actions drawer, select **Delete Database Backup**. You can also right-click the database backup files you want to delete.

Junos Space deletes the selected Junos Space database backup files. The deleted backup files are no longer displayed in the inventory page and are deleted from the `/var/lib/mysql/backup` directory.

Related Documentation

- [Backing Up the Database on page 433](#)
- [Restoring a Database in the User Interface on page 437](#)

- [Restoring a Database in Maintenance Mode on page 440](#)
- [Viewing Database Backup Files on page 442](#)

Viewing Job Recurrence

You can view information about when a job recurs. For example, in Junos Space release 1.4, you can view the recurrence of a database backup job.

To view job recurrence information:

1. Navigate to **Platform > Administration > Manage Database**.

The Manage Database inventory 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**.

Related Documentation

- [Backing Up the Database on page 433](#)
- [Viewing Scheduled Jobs on page 347](#)
- [Viewing Audit Logs on page 359](#)

CHAPTER 38

Manage Licenses

- [Generating and Uploading the Junos Space License Key File on page 445](#)
- [Viewing Licenses on page 447](#)

Generating and Uploading the Junos Space License Key File

The Junos Space software provides a default, 60-day trial license. After 60 days, the use of the Junos Space software expires except for the Upload License command. The administrator must activate the software with the Juniper Networks license key to regain use of the Junos Space software. Within two weeks of the license expiration date, a license expiration warning appears when users log in to Junos Space and from the About Junos Space page.

Junos Space 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 product—appliances, connection points, connections, and applications. When you order Junos Space, Juniper Networks LMS sends an e-mail with an authorization code or serial number and instructions on how to obtain a license key.
2. Uploading the license key using the Junos Space Administration workspace user interface. The system administrator must upload a license key file in the Administration Manage Licenses user interface to license the Junos Space product and activate the configuration ordered.

This procedure includes the following topics:

1. [Generating the License Key File on page 445](#)
2. [Uploading the License Key File Contents on page 446](#)

Generating the License Key File

If you order Junos Space, Juniper Networks sends an e-mail with an authorization code that includes a resource guide describing how to obtain a license key.

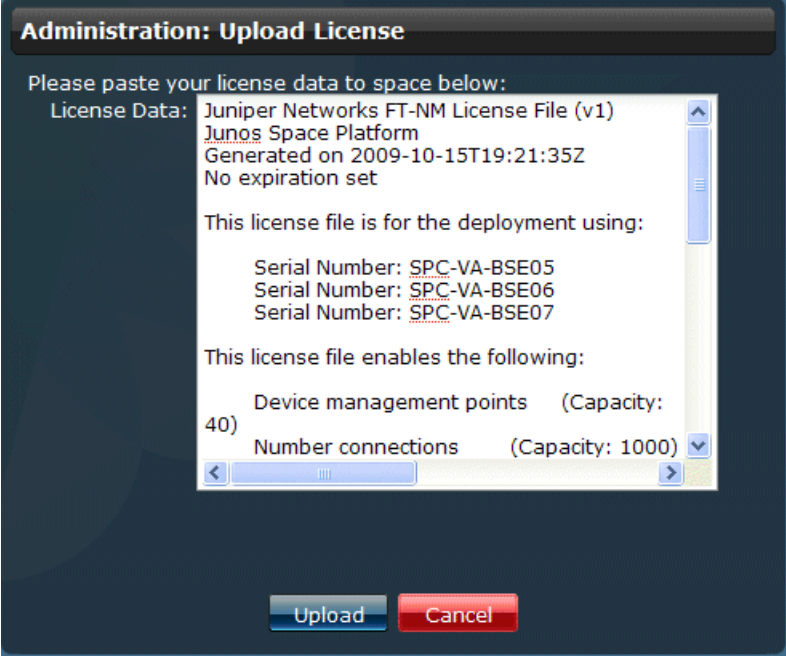
If you order a Junos Space virtual appliance, you also receive an e-mail with a serial number and instructions on how to go to the Juniper Networks license management system to apply that serial number.

Uploading the License Key File Contents

To upload the license key file, follow these steps:

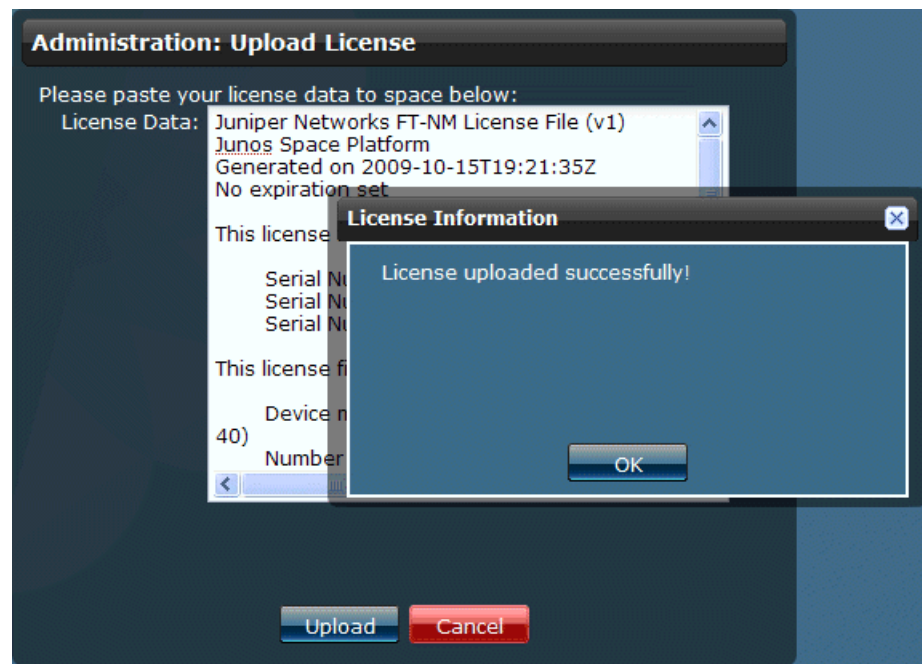
1. Open the Juniper Networks Authorization Codes e-mail you received and follow the directions.
2. Open the license key text file attached to the e-mail and copy all the contents.
3. In Junos Space Application Chooser, click the Network Application Platform application icon.
4. In the navigation ribbon, click the Administration workspace icon. The Administration dashboard appears.
5. In the navigation ribbon, click the Manage Licenses task icon. The Manage Licenses inventory page appears.
6. In the navigation ribbon, click the Upload License icon. The Upload License page appears.
7. Paste the contents of the license key text file in the License Data text field using the Web browser Edit > Paste command.

Figure 141: Administration: Upload Licence Dialog Box

The image shows a web-based dialog box titled "Administration: Upload License". It has a dark blue header bar with the title in white. Below the header, the text "Please paste your license data to space below:" is displayed. A text area labeled "License Data:" contains the following text: "Juniper Networks FT-NM License File (v1)", "Junos Space Platform", "Generated on 2009-10-15T19:21:35Z", and "No expiration set". Below this, the text "This license file is for the deployment using:" is followed by three lines of serial numbers: "Serial Number: SPC-VA-BSE05", "Serial Number: SPC-VA-BSE06", and "Serial Number: SPC-VA-BSE07". Further down, the text "This license file enables the following:" is followed by two items: "Device management points (Capacity: 40)" and "Number connections (Capacity: 1000)". At the bottom of the dialog, there are two buttons: "Upload" (blue) and "Cancel" (red).

8. Click **Upload**. The license key data is uploaded in Junos Space database. The license uploaded successfully message appears.

Figure 142: License Information Upload Success Message



9. Click **OK**. The license appears on the Manage Licenses inventory page.

Figure 143: Manage Licenses Inventory Page



Related Documentation

- [Viewing Licenses on page 447](#)

Viewing Licenses

The Manage Licenses inventory page displays the Junos Space license that the administrator has uploaded. For more information about obtaining and uploading the Junos Space licence, see [“Generating and Uploading the Junos Space License Key File” on page 445](#). You can view licenses in Junos Space as graphics or as tables. By default,

Junos Space displays thumbnail representations of licenses. Licenses might include Junos Space licenses as well as licenses for VAR applications that run on Junos Space.

- [Changing the View on page 448](#)
- [Viewing Manage License Details on page 449](#)

Changing the View

The Manage Licenses page displays the Junos Space trial license until you upload the one specifically generated for your software installation. By default the Manage License inventory page appears in thumbnail view. In thumbnail view the uploaded license is represented by an icon. In tabular view, the software image is represented by a row in the Manage Software table. In tabular view, the uploaded license appears by name.

To change the Manage Licenses inventory page view:

- Click a view indicator to the right of the Manage Software name in the page title bar to switch between thumbnail and tabular view.

Viewing Manage License Details

In thumbnail view You can view the Junos Space license by double-clicking the license on the Manage Licenses inventory page. The License File dialog box appears. If the license is trial, you see the number of days before the 60-day trial license expires. If the license is commercial, you see the license file.

Figure 144: License File



In Tabular view, you see the following license detailed information.

Table 59 on page 449 defines the license details.

Table 59: Manage Licenses Details

Field	Description
License Type	The Junos Space license can either be a trial license installed with the Junos Space software image or a commercial one that you upload into Junos Space.
SKU Model #	The Junos Space license stock keeping unit model number. If the license is trial, the SKU is trial-license . If commercial, the license SKU for example is <i>SPC-DEV-PTS_ADD-20</i> .
Total License Days	For a trial license, the total number of license days is 60 ; unlimited for a commercial license.

Table 59: Manage Licenses Details (*continued*)

Remaining Days	For a trial license, the remaining days is the count down of the number of days since when you installed Junos Space (for example 36) ; unlimited for a commercial license.
----------------	---

**Related
Documentation**

- [Generating and Uploading the Junos Space License Key File on page 445](#)
- [Inventory Pages Overview on page 28](#)
- [Viewing and Exporting Device License Inventory on page 91](#)

CHAPTER 39

Manage Applications

- [Application Management Overview on page 451](#)
- [Managing Junos Space Applications on page 452](#)
- [Modifying Application Settings on page 454](#)
- [Configuring Network Application Platform Application Settings on page 456](#)
- [Configuring Network Activate Application Settings on page 457](#)
- [Adding a Junos Space Application on page 458](#)
- [Upgrading a Junos Space Application on page 460](#)
- [Junos Space Software Upgrade Overview on page 461](#)
- [Upgrading Junos Space Software on page 462](#)
- [Upgrading the Network Application Platform on page 463](#)
- [Uninstalling a Junos Space Application on page 467](#)

Application Management Overview

You can use the Manage Applications pages to manage the Junos Space Network Application Platform (platform) and all other separately packaged applications.

In these pages, you can perform the following tasks:

- Install new Junos Space application using the **Platform > Administration > Manage Applications > Add Application** task, see [“Adding a Junos Space Application” on page 458](#).
- Upgrade the Platform using the **Platform > Administration > Manage Applications > Upgrade Platform** action, see [“Upgrading the Network Application Platform” on page 463](#). The Platform provides the running environment for all Junos Space applications, so upgrading it causes operation interruption.
- Upgrade a Junos Space application while Junos Space is still running using the **Platform > Administration > Manage Applications > Upgrade Application** action, see [“Upgrading a Junos Space Application” on page 460](#).
- Uninstall a Junos Space application while Junos Space is still running using the **Platform > Administration > Manage Applications > Uninstall Application** action, see [“Uninstalling a Junos Space Application” on page 467](#).

- Modify the Platform application settings using the **Platform > Administration > Manage Applications > Modify Application Settings** action, see [“Modifying Application Settings” on page 454](#).
- Tag applications to categorize them for filtering and performing Manage Applications actions using the **Platform > Administration > Manage Applications > Tag It** action, see [“Tagging an Object” on page 495](#).
- View Tags that you have already created on a selected application using the **Platform > Administration > Manage Applications > View Tags** action, see [“Viewing Tags” on page 496](#).



NOTE: The Junos Space Upgrade image includes the platform, Service Now, and Service Insight. Other Junos Space applications are separately packaged in image files. The administrator must download application files from the Juniper Networks Web site to the local client file system. The administrator must upload an application file in Junos Space. Once uploaded, Junos Space installs or upgrades the application. When the application is installed, you can launch it from Application Chooser. When you upgrade Network Application Platform, all applications except Service Now are disabled. Upgrade all disabled applications to the current release. Users in an upgraded application's workspace are directed to Application Chooser.

Related Documentation

- [Managing Junos Space Applications on page 452](#)
- [Modifying Application Settings on page 454](#)
- [Uninstalling a Junos Space Application on page 467](#)
- [Upgrading a Junos Space Application on page 460](#)
- [Upgrading the Network Application Platform on page 463](#)
- [Tagging an Object on page 495](#)
- [Viewing Tags on page 496](#)

Managing Junos Space Applications

Manage Junos Space applications from the **Platform > Administration > Manage Applications** task. All applications that you have uploaded and installed appear in the **Manage Applications** inventory page. From the Manage Applications inventory page you, the super administrator or system administrator can manage Junos Space hot-pluggable applications, such as install, upgrade, and uninstall, while Junos Space is still running. You can also upgrade the Network Application Platform that provides the runtime environment for all Junos Space applications. Upgrading the Platform causes an interruption of Junos Space operation. The Platform upgrade takes place in Maintenance mode.

The administrator can also modify Platform application settings and tag applications to categorize and filter them to perform bulk actions on multiple applications at once.

To install or upgrade an application:

1. Download a new Junos Space application from the Juniper Networks software download site to the local client machine
 2. To add an application, upload that application into Junos Space using **Platform > Administration > Manage Applications > Add Application**. To upgrade an application, select **Platform > Administration > Manage Applications**. Select the application on the Manage Applications inventory page, then select **Upgrade Application**.
 3. Once uploaded, you can install or upgrade the application.
 4. Once you upgrade or install an application, it appears on the Manage Applications inventory page. The new or upgraded application appears in Application Chooser and the Application Switcher global action pop-up menu at the right in the Application Chooser title bar.
- [Changing The View on page 453](#)
 - [Viewing Detailed Application Information on page 453](#)
 - [Performing Manage Application Actions on page 454](#)

Changing The View

Installed Junos Space applications appear in two views: thumbnail and tabular. The default is thumbnail view. Use the view indicators at the top-left in the Manage Applications title bar.

In thumbnail view, applications appear as icons listed in descending order by application title. Each application has a title, description, version, and build. To see more detailed information about an application double-click it move the zoom slider at the top-right to the far right. The default zoom slider position is in the middle. Select an application to select it before performing an action.

In tabular view, applications appear in a table sorted by application title. Each application is a row in the Manage Applications table. Click a row in the table to select it before performing a command. Double-click a row to see detailed application information.

To change views:

- Click a view indicator at the right in the Manage Applications page title bar.

Viewing Detailed Application Information

[Table 60 on page 453](#) defines the information displayed for each application in the Manage Applications inventory page. In thumbnail view to see application details, double-click an application, click **Details**, or slide the slider to the far right. In tabular view, the detailed information appears in the columns.

Table 60: Application Information

Application Information	Description
Title	Name of the Junos Space application.

Table 60: Application Information (*continued*)

Application Information	Description
Version	The Junos Space application software version.
Release Type	The Junos Space application software version release level.
Build	The Junos Space application software build number.
Description (Thumbnail view)	A brief description of the Junos Space application

Performing Manage Application Actions

You can perform the following actions on applications from the Manage Applications Actions drawer. You must first select an application before you can perform an action on it from the Actions drawer. You can also right-click an application to perform these actions.

- Modify Application Settings—See [“Modifying Application Settings” on page 454](#).



NOTE: This action is available for the Platform only.

- Uninstall Application—See [“Uninstalling a Junos Space Application” on page 467](#).
- Upgrade Application—See [“Upgrading a Junos Space Application” on page 460](#).
- Upgrade Platform—See [“Upgrading the Network Application Platform” on page 463](#).



NOTE: This action is available for the Platform only.

- Tag It—See [“Tagging an Object” on page 495](#).
- View Tags—See [“Viewing Tags” on page 496](#).
- Untag It—See [“Untagging Objects” on page 497](#).

Modifying Application Settings

You, the Super Administrator or System Administrator, can modify Junos Space application settings.

To modify application settings:

1. Select **Platform > Administration > Manage Applications**.
The **Manage Applications** inventory page appears.
2. Select the application.
Select Network Application Platform to modify the Platform application settings.
3. Select **Modify Application Settings** from the Actions drawer.

The appropriate Modify Application Settings page appears.

4. Configure the following application settings depending on the application you are managing:
 - [Configuring Network Application Platform Application Settings on page 456](#)
 - [Configuring Network Activate Application Settings on page 457](#)
5. Click **Modify**.

**Related
Documentation**

- [Application Management Overview on page 451](#)
- [Managing Junos Space Applications on page 452](#)
- [Uninstalling a Junos Space Application on page 467](#)
- [Upgrading a Junos Space Application on page 460](#)
- [Creating a Tag on page 498](#)
- [Managing Tags on page 492](#)

Configuring Network Application Platform Application Settings

Table 61 on page 456 defines the application settings you can configure for the Network Application Platform. You must have Super Administrator or System Administrator privileges.

Table 61: Network Application Platform Application Settings

Category	Application Setting Name	Description
Devices	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 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 configuration changes in Space for a device are pushed, committed and synchronized during device discovery.
	Junos Space initiates connection to device	This check box is selected by default, so Junos Space initiates connection with managed devices. To have managed devices initiate connection with Junos Space, deselect this check box.
	Max auto resync waiting time secs	This text box specifies the time within which device configuration changes are synchronized to the database. 20 seconds is the default waiting time. You can specify any number of seconds. There is no specific range.
	Polling time period secs	This setting is for specifying the interval at which to poll the configuration of devices that do not support syslog. Junos Space polls and compares the configuration it has with that of the device(s) at the interval set here. If there is a difference, Space synchronizes its configuration. The default is 900 seconds.
	SSH port for device connection	This text field specifies the SSH port on the device. Junos Space uses this port to discover devices. The default value, 22 , is the standard SSH server port.

Table 61: Network Application Platform Application Settings (*continued*)

Category	Application Setting Name	Description
Users	Automatic logout of idle user sessions (min)	<p>This text box 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 to the logout page. This setting conserves server resources and protects the system from unauthorized access.</p> <p>The text box values are:</p> <ul style="list-style-type: none"> • 60 minutes is the default setting. An error message appears if you enter a value less than 0. • 120 minutes is the maximum setting. An error message appears if you enter a value more than 120 minutes. • 0 minutes turns the setting off.

Related Documentation

- [Modifying Application Settings on page 454](#)

Configuring Network Activate Application Settings

You can configure the Network Activate application settings from the Platform > Administration > Manage Applications inventory page. See [“Modifying Application Settings” on page 454](#)

You must have Super Administrator privileges to configure Network Activate application settings.

[Table 62 on page 457](#) defines the application settings you can configure for the Network Activate application settings.

Table 62: Network Activate Application Settings

Category	Application Setting Name	Description
Deployment	Deploy configuration to the device	Disable this setting to deploy configuration to Junos Space user interface only.
	Save configuration in XML format	This setting is disabled by default, to deploy the service order and view the configuration using JUNOS curly braces syntax.
	Use vlanmaps for flexible tagged services	Enable this setting if MX Series devices are configured for VLAN mapping.
Audit	Perform functional audit on control plane only	Enable this option to check only the control plane to ensure connectivity among endpoints and verify that UNIs are functioning correctly. Disable this setting to check the control plane and also the data plane to verify packet transmission between each valid pair of endpoints in the service.

Table 62: Network Activate Application Settings (*continued*)

Category	Application Setting Name	Description
Logging	Log Directory	Modify the default audit log repository directory. The default log directory is <code>/var/tmp/jboss</code> .

Related Documentation • [Modifying Application Settings on page 454](#)

Adding a Junos Space Application

The administrator can add a new Junos Space application while Junos Space is still running.



NOTE: Service Now and Service Insight are bundled with, installed, and upgraded with the Network Application Platform. You must add, or upgrade all other applications separately. Junos Space 11.2 supports only Junos Space release 11.2 hot-pluggable applications.

To upgrade Junos Space applications, see “[Upgrading a Junos Space Application](#)” on [page 460](#).

To add a Junos Space application:

1. Ensure that the Junos Space application you want to add is downloaded from the Juniper Software download site to the local client file system.

<https://www.juniper.net/support/products/space/#sw>

2. Select **Platform > Administration > Manage Applications > Add Application**.

The Add Application dialog box appears. If you have not uploaded any applications, the page is blank.

3. Upload the new application by performing one of the following:

- a. Click **Upload via HTTP**.

The Software File dialog box appears.

- i. Type the name of the application file or click **Browse** to navigate to where the new Junos Space application file is located on the local file system.

- ii. Click **Upload**.

- b. Click **Upload via SCP**.

The Upload Software via SCP dialog box appears. Add the Secure Copy credentials to upload the Junos Space application image from a remote server to Junos Space.

- i. Add your username.
- ii. Add your password.

- iii. Conform by adding your password again.
- iv. Add the host IP address.
- v. Add the local path name of the Junos Software application file.
- vi. Click **Upload**.

The new application is uploaded from the local file system into Junos Space and displayed by application name, filename, version, release level, and required Junos Space Platform version.

- 4. a. Wait until the job is completed.

The Add Application Job Information dialog box appears.

- b. In the Add Application Job Information dialog box, if you click the Job ID link, you see the Add Application job on the **Platform > Job Management > Manage Jobs** inventory page.
 - i. Ensure that the job is successful.
 - ii. Select **Administration > Manage Application > Add Application** to continue with the add application process.

The Add Application dialog box appears.

- c. In the **Add Application Job Information** dialog box, if you click **OK**, the Add Application dialog box appears.

- 5. In the **Add Application** dialog box, select the new uploaded application.

You see the new application file on the Add Application page.

- 6. Click **Install**.

Wait until the application fully deploys.

- 7. Without logging out of Junos Space, navigate to the Application Chooser.

- 8. Click the Application Switcher global icon at the top-right in the application banner.

The Application Switcher pop-up menu appears.

- 9. Click **Select Application**.

Application Chooser appears with the new application icon.

- 10. Click the new application icon to view and begin using its workspaces and tasks.

Related Documentation

- [Application Management Overview on page 451](#)
- [Managing Junos Space Applications on page 452](#)
- [Upgrading a Junos Space Application on page 460](#)
- [Upgrading the Network Application Platform on page 463](#)
- [Modifying Application Settings on page 454](#)

- [Uninstalling a Junos Space Application on page 467](#)
- [Upgrading a Junos Space Application on page 460](#)
- [Tagging an Object on page 495](#)
- [Viewing Tags on page 496](#)

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. Use **Platform > Administration > Once the application is upgraded successfully, you can launch it from Application Chooser.**

To install a new Junos Space application, use the **Platform > Administration > Manage Applications > Add Application** action, see [“Adding a Junos Space Application” on page 458](#).

To upgrade an existing Junos Space application:

1. Ensure that the application to which you want to upgrade is downloaded from the Juniper Software download site to the local client file system.
<https://www.juniper.net/support/products/space/#sw>
2. Navigate to **Platforms > Administration > Manage Applications**. The Manage Applications inventory page appears.
3. Right-click the application that you want to upgrade and select **Upgrade Application**. You can also select the application and select **Upgrade Application** from the Actions drawer.

The Upgrade Application dialog box appears displaying all previously uploaded versions of that application.

4. Do one of the following:
 - If the software file for the application to which you want to upgrade is listed in the Upgrade Application dialog box, select it and click **Upgrade**.
The application upgrade process begins. Go to the next step.
 - If the application to which you want to upgrade is not listed in the Upgrade Application dialog box, click **Upload**. The Software File dialog box appears.
 - a. Click **Browse** and navigate to where the software file to which you want to upgrade is located on the local file system.
 - b. Click **Upload**.
The software file is uploaded into Junos Space. 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 > Manage Applications** to continue with the add application process.

The Upgrade Application dialog box appears.

- e. Select the software file to which you want to upgrade, and click **Upgrade**. The application upgrade process begins.
5. Navigate to the Application Chooser and launch the application you upgraded.

**Related
Documentation**

- [Application Management Overview on page 451](#)
- [Managing Junos Space Applications on page 452](#)
- [Adding a Junos Space Application on page 458](#)
- [Upgrading the Network Application Platform on page 463](#)
- [Modifying Application Settings on page 454](#)
- [Uninstalling a Junos Space Application on page 467](#)
- [Tagging an Object on page 495](#)
- [Viewing Tags on page 496](#)

Junos Space Software Upgrade Overview

To upgrade software for the Junos Space Virtual Appliance, you upload the Junos Space image file to your existing fabric and perform the software upgrade in the Junos Space user interface. When you perform an upgrade, all appliances (nodes) in the fabric are upgraded with the new software.

To ensure a successful upgrade of your Junos Space appliances, complete the following tasks.

- Back up all your Junos Space data files before you begin the upgrade process.
- Download the Junos Space software image from the Juniper Networks software download Web site.
- Complete the steps to upgrade your current Junos Space software to the latest software version.



NOTE: To perform a Junos Space upgrade, you must have super administrator or system administrator access privileges.

- Validate that the software is successfully installed by logging in to the user interface.

To view the version of the installed Junos Space software, select the Help icon in the user interface banner and click **About**.

- Upload the License Key that was sent to you when you purchased the Junos Space software upgrade.

**Related
Documentation**

- [Upgrading Junos Space Software on page 462](#)

Upgrading Junos Space Software

To upgrade software for the Junos Space Virtual Appliance, you download the Junos Space Upgrade image file from the Juniper Networks software download site onto the local client file system. You upload the Junos Space image file to your local file system using the Upgrade Platform action in the Manage Applications workspace. When you perform an upgrade, all appliances (nodes) in the fabric are upgraded with the new software.



CAUTION: Junos space supports upgrades from the last two versions. Junos Space 11.4 supports upgrading from 11.2 or 11.3. Previous version upgrades may require a two-step upgrade. Example: 11.1 to 11.2 to 11.4.

-
- [Junos Space 11.4 Release Highlights on page 462](#)
 - [Before You Begin on page 463](#)
 - [Upgrading Junos Space Release 11.2 or 11.3 to Release 11.4 on page 463](#)

Junos Space 11.4 Release Highlights

The Junos Space Upgrade Release 11.4 includes:

Junos Space Release 11.4 Contents

- Network Application Platform Release 11.4 The platform provides the operating environment for Junos Space, therefore upgrade using the Platform > Administration > Manage Application Upgrade Platform action.
- Service Now Release 11.4
- Service Insight Release 11.4

Available Hot-Pluggable Applications

The following applications are hot-pluggable in Junos Space. Hot-pluggable applications mean that adding removing, and upgrading occurs while Junos Space is still running, and without service interruption. A hot-pluggable application is packaged separately and has an separate image file for installing and upgrading.

- Ethernet Design
- Network Activate
- QoS Design
- Virtual Control Release

Before You Begin

Before you upgrade the Junos Space Software, ensure that you are aware of the following:

- Upgrading to Junos Space release 11.4 clears existing user preferences set using the User Preference global action icon at the right in the title bar of Application Chooser.
- We recommend that you:
 - Back up the Junos Space database before you begin the upgrade process. See also [“Application Management Overview” on page 451](#).
 - Clear the Web browser cache before logging in to the upgraded Junos Space software.
- You must log in as the default super administrator or system administrator to upgrade Junos Space.

Upgrading Junos Space Release 11.2 or 11.3 to Release 11.4

The Platform provides the running environment for all Junos Space applications, so upgrading it causes operation interruption.



NOTE: When upgrading Junos Space from release 11.2 or 11.3 to 11.4, the Network Application Platform and Service Now and Service Insight applications are upgraded only. Other Junos Space release 11.2 or 11.3 applications are disabled. You must upgrade release 11.2 or 11.3 disabled applications to release 11.4 (see [“Upgrading a Junos Space Application” on page 460](#)) or uninstall them (see [“Uninstalling a Junos Space Application” on page 467](#)). Do not add disabled Junos Space applications using **Platform > Administration > Manage Applications > Add Application**.

To upgrade Junos Space from release 11.2 or 11.3 to release 11.4, see [“Upgrading the Network Application Platform” on page 463](#).

Related Documentation

- [Application Management Overview on page 451](#)
- [Managing Junos Space Applications on page 452](#)

Upgrading the Network Application Platform

The Network Application Platform (Platform) provides the running environment for all Junos Space applications, so upgrading causes operation interruption. The Upgrade Network Application Platform action allows the administrator to upgrade the Network

Application Platform independently from one version to another without installing other Junos Space applications.



NOTE: Junos Space Network Application Platform supports upgrades from the last two versions. Platform 11.3 supports upgrading from 11.2 or 11.1. Previous version upgrades may require a two-step upgrade. Example: 1.4 to 11.1 to 11.3.



NOTE: During an upgrade of Junos Space release 2.0, or 11.1 to release 11.2 on a multi-node fabric, the install status is shown in the installation process.

To upgrade the Junos Space Platform:

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

2. Select **Platform > Administration > Manage Applications**.

The Manage Applications inventory page appears.

3. Right-click the **Network Application Platform** application to select it.

4. Select **Upgrade Platform** in the pop-up menu.

You can also select the platform and select **Upgrade Platform** from the Actions drawer. The **Upgrade Application** page appears displaying all previously uploaded versions of the Platform.

5. Do one of the following:

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

The application upgrade process begins. (Go to 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 page appears.

Upload the new application by performing one of the following:

- a. Click **Upload via HTTP**.

The Software File dialog box appears.

- i. Type the name of the application file or click **Browse** to navigate to where the new Junos Space application file is located on the local file system.

- ii. Click **Upload**

- b. Click **Upload via SCP**.

The Upload Software via SCP dialog box appears. You must add the following Secure Copy remote machine credentials.

- i. Add your username.
- ii. Add your password.
- iii. Conform by adding your password again.
- iv. Add the host IP address.
- v. Add the local path name of the Junos Software application file.
- vi. Click **Upload**.

The new application is uploaded from the local file system into Junos Space and displayed by application name, filename, version, release level, and required Junos Space Platform version

When the process 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 **Platform > Job Management > Manage Jobs** inventory page.
 - i. Ensure that the job is successful.
 - ii. Select **Administration > Manage Applications** to continue with the add application process.

The Manage Applications inventory page appears.

- b. Right-click the **Network Application Platform** application and select **Upgrade Platform**.
- c. Click **OK**.

The Upgrade Platform dialog box appears. You see the application file that was uploaded.

- d. Select the application file to which you want to upgrade, and click **Upgrade**. The application upgrade process begins.
6. You enter **Maintenance** mode. Junos Space 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 **OK**.

Junos Space displays a status dialog box during the platform upgrade process.

9. When the platform upgrade completes, click the **Return to Maintenance Menu** link.

The Maintenance Mode Actions dialog box appears.

10. Click the **Log Out and Exit from Maintenance Mode** link.

The installation progress dialog box appears.



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

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: Juniper Networks recommends that you clear the Web browser cache before logging in to the upgraded software.



NOTE: Juniper recommends that you perform a functional audit on all deployed services after upgrading.

You can now log in to begin using the upgraded Junos Space software.

**Related
Documentation**

- [Application Management Overview on page 451](#)
- [Managing Junos Space Applications on page 452](#)
- [Modifying Application Settings on page 454](#)
- [Uninstalling a Junos Space Application on page 467](#)
- [Upgrading a Junos Space Application on page 460](#)
- [Tagging an Object on page 495](#)
- [Viewing Tags on page 496](#)

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 Manage Applications inventory page.

To uninstall a Junos Space application:

1. Select **Platform > Administration > Manage Applications**.

The Manage Applications inventory page appears.

2. Right-click the application you want to uninstall and select **Uninstall Application**. You can also select **Uninstall Application** from the Actions drawer.

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.

Related Documentation

- [Application Management Overview on page 451](#)
- [Managing Junos Space Applications on page 452](#)
- [Modifying Application Settings on page 454](#)
- [Upgrading a Junos Space Application on page 460](#)
- [Upgrading the Network Application Platform on page 463](#)
- [Tagging an Object on page 495](#)
- [Viewing Tags on page 496](#)

CHAPTER 40

System Troubleshooting

- [System Status Log File Overview on page 469](#)
- [Customizing Node System Status Log Checking on page 471](#)
- [Customizing Node Log Files To Download on page 472](#)
- [Downloading the Troubleshooting Log File from the UI on page 472](#)
- [Downloading the Troubleshooting Log File In Maintenance Mode on page 474](#)
- [Downloading Troubleshooting System Log Files Using the CLI on page 475](#)

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 469](#).

The system administrator can customize the information that is collected in the system log file. See [“Customizing Node System Status Log Checking” on page 471](#).

The system administrator can download the latest log files for each fabric node when logged into an appliance. See [“Downloading System Log Files For an Appliance” on page 470](#).

In each operating mode, the system administrator can customize the default log files that are download from an appliance. See [“Customizing Node Log Files To Download” on page 472](#).

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 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: 1.1.1.1Filesystem    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 471](#).

Downloading System Log Files For an Appliance

The system administrator can download the latest log files for each fabric node when logged into an appliance. The system status log file and all other third party log files are collected and compressed in a troubleshooting file.

[Table 63 on page 470](#) lists the files included in the **troubleshoot** file.

Table 63: Log Files included in the troubleshoot File

Description	Location
System status log file	<code>/var/logSystemStatusLog</code>
Jboss log files	<code>/var/log/jboss/*</code>
Service Provisioning data files	<code>/var/tmp/jboss/debug/*</code>
MYSQL error log	<code>/var/log/mysqld.log</code>
Log files for Apache, NMA, Webproxy	<code>/var/log/httpd/*</code>
Watchdog log file	<code>/var/log/watchdog/*</code>
Linux system messages	<code>/var/log/messages/*</code>

The system administrator can download log files in each operation mode as follow:

- Server Mode (See [“Downloading the Troubleshooting Log File from the UI” on page 472](#).)
- Maintenance Mode (See [“Downloading the Troubleshooting Log File In Maintenance Mode” on page 474](#).)
- CLI mode (See [“Downloading Troubleshooting System Log Files Using the CLI” on page 475](#).)

Customizing Log Files To Download

The system administrator can also customize the log files to be downloaded for specific fabric nodes. For more information, see [“Customizing Node Log Files To Download” on page 472](#).

Related Documentation

- [Maintenance Mode Overview on page 402](#)
- [Customizing Node System Status Log Checking on page 471](#)
- [Customizing Node Log Files To Download on page 472](#)

- [Downloading the Troubleshooting Log File from the UI on page 472](#)
- [Downloading the Troubleshooting Log File In Maintenance Mode on page 474](#)
- [Downloading Troubleshooting System Log Files Using the CLI on page 475](#)

Customizing Node System Status Log Checking

The system administrator can customize the system checking for a fabric node so that the necessary information is written to `/var/log/SystemStatusLog`. The administrator must modify the fabric node Perl script in `/usr/nma/bin/writeLogCronJob`.

To customize system status checking for an appliance, modify the `writeSystemStatusLogFile` sub-function in `writeLogCronJob` as shown:

```
sub writeSystemStatusLogFile{
    my $err = 0;
    my $logfile = $_[0];
    $err = system("date >> $logfile");
    $err = system("df /var >> $logfile");
    $err = system("top -n 1 -b | grep Cpu >> $logfile");
    $err = system("top -n 1 -b | grep Mem: >> $logfile");
    $err = system("top -n 1 -b | grep Swap: >> $logfile");

    ***<Add additional system command here that you want to print out in the
    SystemStatusLog file>***

    if ($err == 0 ) {          print "write log to $logfile successfully\n";
    } else {                  print "cannot write log to $logfile\n";
    }
    return $err;
}
```

Related Documentation

- [Maintenance Mode Overview on page 402](#)
- [System Status Log File Overview on page 469](#)
- [Customizing Node Log Files To Download on page 472](#)
- [Downloading the Troubleshooting Log File from the UI on page 472](#)
- [Downloading the Troubleshooting Log File In Maintenance Mode on page 474](#)
- [Downloading Troubleshooting System Log Files Using the CLI on page 475](#)

Customizing Node Log Files To Download

The system administrator can customize the log files that are downloaded for each fabric node by modifying the Perl script in `/var/www/cgi-bin/getLogFiles`.

To customize the log files that are downloaded for each fabric node, modify the `getLogFiles` Perl script zip command as shown:

```
...
system("zip -r $logFileName /var/log/jboss/* /var/tmp/jboss/debug/
/var/log/mysqld.log /var/log/httpd/* /var/log/watchdog /var/log/messages
/var/log/SystemStatusLog > /dev/null");
...
```

Related Documentation

- [Maintenance Mode Overview on page 402](#)
- [System Status Log File Overview on page 469](#)
- [Customizing Node System Status Log Checking on page 471](#)
- [Downloading the Troubleshooting Log File from the UI on page 472](#)
- [Downloading the Troubleshooting Log File In Maintenance Mode on page 474](#)
- [Downloading Troubleshooting System Log Files Using the CLI on page 475](#)

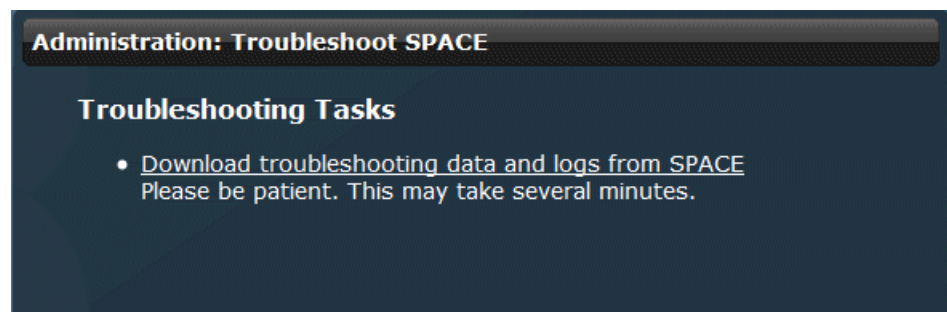
Downloading the Troubleshooting Log File from the UI

From the Administration workspace, the system administrator can download a troubleshooting file `troubleshoot_yyyy-mm-dd_hh-mm-ss.zip` that contains useful information for managing and monitoring the nodes in the system. The troubleshoot zip file includes the server Coordinated Universal Time (UTC) date and time. For example, `troubleshoot_2010-04-01_11-25-12.zip`.

To retrieve troubleshooting data and log files, follow these steps:

1. From the navigation ribbon, select the Administration workspace icon.
2. From the navigation ribbon, select the **Troubleshoot SPACE** task.

The Troubleshoot SPACE page appears.



3. Click the **Download troubleshooting data and logs from SPACE** link to access the **troubleshoot_yyyy-mm-dd_hh-mm-ss.zip** file in your browser.
 - If you are using Mozilla Firefox: In the Opening troubleshoot zip dialog box, select **Save file** and click **OK** to save the zip file to your computer using the Firefox Downloads dialog box.
 - If you are using Internet Explorer: From the File Download screen, select **Save** and select a directory on your computer where you want to save the **troubleshoot_yyyy-mm-dd_hh-mm-ss.zip** file.
4. When you contact the Juniper Technical Assistance Center, describe the problem you encountered and provide the JTAC representative with the **troubleshoot.zip** file.

[Table 64 on page 473](#) lists the files included in the **troubleshoot_yyyy-mm-dd_hh-mm-ss.zip** file.

Table 64: Data and Log Files in troubleshoot.zip File

Description	Location
Jboss log files	/var/log/jboss/*
Service Provisioning data files	/var/tmp/jboss/debug/*
MYSQL error log	/var/log/mysqld.log
Log files for Apache, NMA, Webproxy	/var/log/httpd/*
Watchdog log file	/var/log/watchdog/*
Linux system messages	/var/log/messages/*
CPU/RAM/Disk statistics (during past 24 hours)	Not applicable

Related Documentation

- [Maintenance Mode Overview on page 402](#)
- [System Status Log File Overview on page 469](#)
- [Customizing Node System Status Log Checking on page 471](#)
- [Customizing Node Log Files To Download on page 472](#)
- [Downloading the Troubleshooting Log File In Maintenance Mode on page 474](#)
- [Downloading Troubleshooting System Log Files Using the CLI on page 475](#)

Downloading the Troubleshooting Log File In Maintenance Mode

Maintenance Mode is a special mode that an administrator can use to perform system recovery or debugging tasks while all nodes in the fabric are shutdown and the web proxy is running.

The administrator can download the **troubleshoot_yyyy-mm-dd_hh-mm-ss.zip** file from Maintenance Mode. The troubleshoot zip file includes the server Coordinated Universal Time (UTC) date and time. For example, **troubleshoot_2010-04-01_11-25-12.zip**.

To download the troubleshooting log file in maintenance mode, follow these steps:

1. Connect to an appliance in maintenance mode by using the appliance URL.

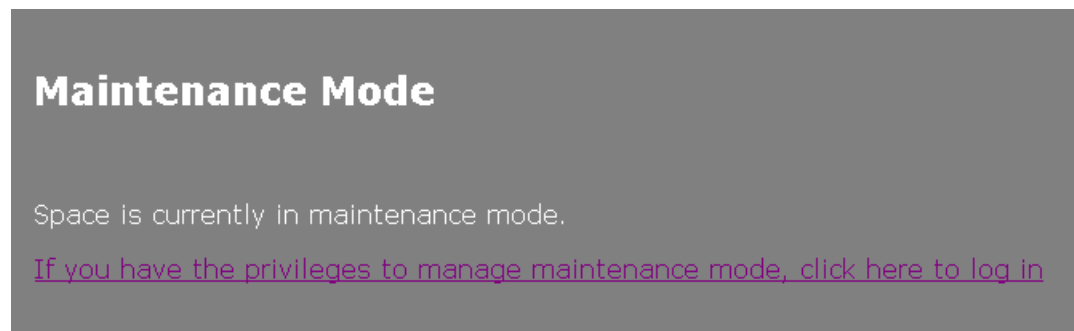
For example:

`https://<ipaddress>/maintenance`

Where *ipaddress* is the address of the Juniper Networks appliance.

The Maintenance Mode page appears.

Figure 145: Maintenance Mode Page



2. Click the **click here to log in** link. The login dialog box appears.
3. Log in to maintenance mode using the authorized login name and password.
4. Click OK. The Maintenance Mode Actions menu appears.
5. Click **Download Troubleshooting Data and Logs**. The file download dialog box appears.
6. Click Save to download the **troubleshoot_yyyy-mm-dd_hh-mm-ss.zip** file to the connected computer.
7. Click **Log Out and Exit from Maintenance Mode**.

Related Documentation

- [Maintenance Mode Overview on page 402](#)
- [System Status Log File Overview on page 469](#)
- [Customizing Node System Status Log Checking on page 471](#)
- [Customizing Node Log Files To Download on page 472](#)

- [Downloading the Troubleshooting Log File from the UI on page 472](#)
- [Downloading Troubleshooting System Log Files Using the CLI on page 475](#)

Downloading Troubleshooting System Log Files Using the CLI

If Junos Space is operating, the administrator can log into an appliance console and download system status logs for each fabric node using the CLI Network Settings Utility > SecureCoPy (SCP) command. If the system is not operating, the Administrator can download system status logs using the CLI USB command.

The Network Settings Utility, for both commands, collects all system log files in the `/var/log` subdirectory and creates a `*TAR` file to download. For more information on the log files that are written, see “[System Status Log File Overview](#)” on page 469.

This procedure includes the following tasks:

- [Downloading a System Log File Using a USB Device on page 475](#)
- [Downloading System Log File Using SCP on page 476](#)

Downloading a System Log File Using a USB Device

Using the Networks Settings Utility Retrieve Logs > USB command, the administrator can download system status logs to a connected USB device if the network is down.

1. Using a console utility, such as SSH or Telnet, connect to the appliance. The Junos Space Settings Menu appears.

Junos Space Settings Menu

```
1> Change Password
2> Set Routing
3> Set DNS Servers
4> Change Time Options
5> Retrieve Logs
6> Security
7> (Debug) run shell
```

```
Q> Quit
R> Redraw Menu
```

Choice [1-7,QR]:

2. Type option **5> Retrieve Logs**. The Retrieve Logs submenu appears.

Choice [1-7,QR]: 5

```
1> Save to USB
2> Send via SCP
```

```
M> Return to Main Menu
R> Redraw Menu
```

Choice [1-2,MR]:

3. Select 1> **Save to USB**. The USB device must be connected to an appliance.
4. Indicate whether you want to continue. Enter **y** for yes; **n** to abort.
5. The Save to USB process downloads the log files from all cluster members and combines them into a **.tar** file. Once the file is created, the process copies the file onto a USB device. You see the following:

Copying 20090827-1511-logs.tar to USB drive

Downloading System Log File Using SCP

Using the Networks Settings Utility Retrieve Logs > SCP command, the administrator can download system status logs to a specific location.

To download system status logs using SCP, follow these steps:

1. Using a console utility, such as SSH or Telnet, connect to an appliance. The Junos Space Settings Menu appears.

Junos Space Settings Menu

```
1> Change Password
2> Set Routing
3> Set DNS Servers
4> Change Time Options
5> Retrieve Logs
6> Security
7> (Debug) run shell
```

```
Q> Quit
R> Redraw Menu
```

Choice [1-7,QR]:

2. Type option 5> **Retrieve Logs**. The Retrieve Logs submenu appears.

Choice [1-7,QR]: 5

```
1> Save to USB
2> Send via SCP
```

```
M> Return to Main Menu
R> Redraw Menu
```

Choice [1-2,MR]:

3. Select 2> **Send via SCP**. The process retrieves the log files on all cluster members and combines them into a **.TAR** file.
4. Indicate whether you want to continue. Enter **y** for yes; **n** to abort.
5. Specify the SCP server IP address to which to transfer the file.

6. Enter the remote SCP user. For example, root
7. Enter the remote SCP file location. For example, **/root/tmplogs**. You see the following:

```

Remote scp IP: 123.123.123.123
Remote scp user: root
Remote scp path: /root/tmplogs
Is this correct? [y/n]
The authenticity of host '123.123.123.123 (123.123.123.123)' 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 '123.123.123.123' (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.
123.123.123.123 password:
20090827-1517-logs.tar
100% 18MB 17.6MB/s 00:01

```

8. Indicate whether the SCP server information is correct. Enter **y** for yes; **n** if incorrect.
9. Indicate whether you want to continue. Enter **y** for yes; **n** for no.

Related Documentation

- [Maintenance Mode Overview on page 402](#)
- [System Status Log File Overview on page 469](#)
- [Customizing Node System Status Log Checking on page 471](#)
- [Customizing Node Log Files To Download on page 472](#)
- [Downloading the Troubleshooting Log File from the UI on page 472](#)
- [Downloading the Troubleshooting Log File In Maintenance Mode on page 474](#)

CHAPTER 41

Authentication Servers

- [Managing Remote Authentication Servers on page 479](#)

Managing Remote Authentication Servers

- [Remote Authentication Overview on page 479](#)
- [Understanding Junos Space Authentication Modes on page 480](#)
- [Configuring Remote Authentication Method Workflows on page 481](#)
- [Managing Remote Authentication Servers on page 483](#)
- [Creating a Remote Authentication Server on page 484](#)
- [Modifying Authentication Settings on page 486](#)
- [Junos Space Log In Behavior with Remote Authentication Enabled on page 486](#)

Remote Authentication Overview

Junos Space, by default, authenticates users to log in locally when you configure their accounts using **Platform > Users > Manage Users > Create User**.

Using the **Platform > Administration > Manage Auth Servers** workspace, you can authenticate users to log in exclusively from a centralized location using one or more RADIUS remote authentication servers. You can also authenticate users to log in to Junos Space using both local and remote authentication.

Users stored on RADIUS server contain no Junos Space role or authorization information, therefore you must create local dummy users corresponding to the RADIUS users, and configure them with Junos Space roles using **Platform > Users > Manage Roles > Create Role**. See [“Creating Users” on page 381](#) and [“Creating a User-Defined Role” on page 395](#).

You can configure the order in which Junos Space connects to remote authentication servers by preference. Junos Space authenticates using the first reachable remote authentication server on the list.

You must install or upgrade to Junos Space 11.2 or later to use remote authentication.

Junos Space supports RADIUS authentication methods: PAP and CHAP

You must have Super Administrator, System Administrator privileges to configure remote authentication server settings, authentication modes, and user passwords and settings.

Regular Junos Space users will not be able to configure their password if you maintain them solely by a remote authentication server.

You may choose to allow some privileged users to set a local password so they can still log onto the system if the remote authentication server is unreachable.

**Related
Documentation**

- [Configuring Remote Authentication Method Workflows on page 481](#)
- [Understanding Junos Space Authentication Modes on page 480](#)
- [Managing Remote Authentication Servers on page 483](#)
- [Creating a Remote Authentication Server on page 484](#)
- [Modifying Authentication Settings on page 486](#)
- [Junos Space Log In Behavior with Remote Authentication Enabled on page 486](#)

Understanding Junos Space Authentication Modes

Junos Space provides three authentication modes: local , remote, and remote-local. The default authentication mode is local. You configure local authentication from **Platform > Users >Manage Users > Create Users**. You configure remote and remote-local authentication from **Platform > Administration > Remote Auth Servers**.



NOTE: You configure local authorization from **Platform > Users >Manage Users > Create Roles**. See “[Understanding How to Configure Users to Manage Objects in Junos Space](#)” on page 372, “[Creating Users](#)” on page 381, and “[Creating a User-Defined Role](#)” on page 395. The current Junos Space release does not support remote authorization.

The following sections describe the authentication modes:

- [Local Authentication on page 480](#)
- [Remote Authentication on page 480](#)
- [Remote-Local Authentication on page 481](#)

Local Authentication

To configure local Junos Space authentication, navigate to **Platform > Users >Manage Users > Create Users**. To configure Junos Space authentication, see “[Creating Users](#)” on page 381.

Remote Authentication

User authentication information is stored on one or more remote authorization servers only. Authorization info, however, must be configured and stored in Junos Space. To configure Junos Space remote authentication, see “[Configuring Remote Authentication Method Workflows](#)” on page 481. User authentication and authorization information are stored locally in Junos Space.

Remote-Local Authentication

Existing and temporary user authentication and authorization information is stored in Junos Space. New user authentication information and password changes are maintained on the remote authentication server. You must configure new user authorization information which is stored in Junos Space. To configure Junos Space remote-local authentication, see [“Configuring Remote Authentication Method Workflows” on page 481](#).

Related Documentation

- [Remote Authentication Overview on page 479](#)
- [Configuring Remote Authentication Method Workflows on page 481](#)
- [Managing Remote Authentication Servers on page 483](#)
- [Creating a Remote Authentication Server on page 484](#)
- [Modifying Authentication Settings on page 486](#)
- [Junos Space Log In Behavior with Remote Authentication Enabled on page 486](#)

Configuring Remote Authentication Method Workflows



WARNING: To avoid a BEAST TLS 1.0 attack, whenever you log in to Junos Space in a browser tab or window, make sure that 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.

This topic describes the workflow necessary to configure Junos Space: local, remote, and remote-local authentication methods:

- [Configuring Local Authentication on page 481](#)
- [Configuring Remote Only Authentication on page 482](#)
- [Configuring Local-Remote Authentication on page 482](#)

Configuring Local Authentication

1. Log in to Junos Space.
2. Create users and select existing user roles from **Platform > Users > Manage Users > Create Users**.

See [“Understanding How to Configure Users to Manage Objects in Junos Space” on page 372](#), and [“Creating Users” on page 381](#).

3. Create user-defined roles if necessary from **Platform > Users > Manage Roles > Create Roles**.

See [“Creating a User-Defined Role” on page 395](#).

Configuring Remote Only Authentication

1. If users have Junos Space accounts, enter their usernames and passwords on one or more of your remote authentication servers. Also enter the default Junos Space username **super** and **password** if you want to use it.
2. Log in to Junos Space.
3. Navigate to **Platform > Administration > Create Auth Server** and configure the preferences for one or more remote authentication servers. See [“Creating a Remote Authentication Server” on page 484](#).

Configuring Local-Remote Authentication

1. If users exist in Junos Space, keep and manage them. You can manage Junos Space users from **Platform > Administration > Manage Users**.
2. If you need to add more Junos Space users, see [“Creating Users” on page 381](#).
3. Configure an remote authentication server, see [“Creating a Remote Authentication Server” on page 484](#).

Related Documentation

- [Remote Authentication Overview on page 479](#)
- [Understanding Junos Space Authentication Modes on page 480](#)
- [Managing Remote Authentication Servers on page 483](#)
- [Creating a Remote Authentication Server on page 484](#)
- [Modifying Authentication Settings on page 486](#)
- [Junos Space Log In Behavior with Remote Authentication Enabled on page 486](#)

Managing Remote Authentication Servers

The **Platform > Administration > Manage Auth Server** page allows you to configure remote authentication settings to allow users to log in to Junos Space from a remote authentication server. The **Manage Auth Server** page includes two areas: **Mode Settings** and **Remote Authentication Servers** table.

From the **Auth Mode Settings** area, you can select and save the Junos Space 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. Navigate to **Platform > Administration > Manage > Remote Auth Servers**.

2. In the **Mode Settings** area, select the authentication method you want to use.

By default, Junos Space is in local authentication mode and the controls for the **Remote Authentication Server** table are disabled. If you select the Use **Remote Authentication** check box, the **Remote Authentication Only** and **Remote-Local Authentication** options are enabled.

3. Click **Save** to store the remote authentication mode setting you select.
4. In the **Authentication Servers** table Add a new remote authentication server by clicking Add (+). See [“Creating a Remote Authentication Server” on page 484](#).
5. Modify an authentication server by doubling clicking that server row in the table. See [“Modifying Authentication Settings” on page 486](#).
6. Delete an authentication server by selecting that row and clicking Delete (X) to remove an authentication server.
7. Click a row and select the arrows to move the server up and down the list. Up arrow will be grayed out if at the top of the list; down arrow will be grayed out if at the bottom of the list.

Sorting for columns are disabled, since there is an explicit sort order as determined by the arrows.

8. On selection of the server, click **Test Connection** to display a transient result of last connection test.
9. Confirm that you want to test the server connection.

After testing, the Status dialog box appears displaying the test results: success or failure.

10. Click OK.

If the connection results fails, ensure the server settings are correct.

- Related Documentation**
- [Remote Authentication Overview on page 479](#)
 - [Configuring Remote Authentication Method Workflows on page 481](#)
 - [Understanding Junos Space Authentication Modes on page 480](#)
 - [Creating a Remote Authentication Server on page 484](#)
 - [Modifying Authentication Settings on page 486](#)
 - [Junos Space Log In Behavior with Remote Authentication Enabled on page 486](#)

Creating a Remote Authentication Server

To run Junos Space remote authentication, you must create one or more remote authentication servers and configure the server settings.

To create a remote authentication server:

1. Navigate to **Platform > Administration > Manage > Remote Auth Servers**.
2. In the Mode Settings area, select the authentication method you want to use.

In local authentication mode, the controls for the Remote Authentication Server table are enabled so you can add authentication servers first and only switch to non-local authentication mode when you are ready later. If you select the Use **Remote Authentication** check box, the **Remote Authentication Only** and **Remote-Local Authentication** options are enabled. Mousing over the help icon, displays a description of the available authentication modes.

3. Click **Save** to store the remote authentication mode setting you select.
4. In the Authentication Servers table Add a new remote authentication server by clicking Add (+).

The Create Auth Server dialog box appears.

5. Enter the required settings to connect Junos Space to the remote authentication server. See table [Table 65 on page 484](#).

Table 65: Remote Authentication Server Settings

Setting	Description
Protocol	<p>The supported authentication protocols:</p> <ul style="list-style-type: none"> • PAP—Password Authentication Protocol. This default protocol provides a two-way handshake during the initiation of the connection with the remote authentication server and Junos Space. 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 responds with the password and the challenge.
IP Address	The IP address of the remote authentication server. The format is 1.0.0.1 to 223.255.255.254, excluding 127.x.x.x.

Table 65: Remote Authentication Server Settings (*continued*)

Setting	Description
Port Number	The remote authentication server assigned UDP port number. The default is 1812 . RADIUS has been officially assigned UDP port 1812 for RADIUS Authentication.
Shared Secret	The text string that serves as a password between the RADIUS server, proxy, and client.
Number of Tries	The number of retries that a device can attempt to contact a RADIUS authentication server. The default tries is 3 .
Max Retry Timeout MSecs	The interval in milliseconds Junos Space waits for a reply from a remote authentication server. The default value is 6000 . The retry timeout improves server access on busy networks where overall response times may vary widely from network to network.

6. In the Create Auth Server dialog box, click **OK**.

The remote authentication server appears as a row at the bottom of the table.

7. In the Manage Auth Servers page, click **Test Connection** to verify the Junos Space 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 479](#)
- [Understanding Junos Space Authentication Modes on page 480](#)
- [Configuring Remote Authentication Method Workflows on page 481](#)
- [Modifying Authentication Settings on page 486](#)
- [Junos Space Log In Behavior with Remote Authentication Enabled on page 486](#)

Modifying Authentication Settings

The Manage Authentication Servers page allows you to change Junos Space authentication mode and remote authentication server connection settings.

To modify remote authentication settings:

1. In the Mode Settings area, change to the authentication method you want to use.

By default, Junos Space is in local authentication mode and the controls for the **Remote Authentication Server** table are disabled. If you select the Use **Remote Authentication** check box, the **Remote Authentication Only** and **Remote-Local Authentication** options are enabled. Mousing over the help icon, displays a description of the available authentication modes.

2. Click **Save** to store the remote authentication mode setting you select.
3. In the Authentication Servers table click the server edit icon that you want to modify. See [“Creating a Remote Authentication Server” on page 484](#).

The Modify Authentication Server dialog box appears.

4. Change the remote authentication server settings you want to change.

For a description of the available remote authentication server, see [“Creating a Remote Authentication Server” on page 484](#).

5. In the Create Auth Server dialog box, click **OK**.

The modified remote authentication server settings are saved in the database.

6. On the Manage Auth Servers page, click **Test Connection** to verify the Junos Space 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 479](#)
- [Configuring Remote Authentication Method Workflows on page 481](#)
- [Understanding Junos Space Authentication Modes on page 480](#)
- [Creating a Remote Authentication Server on page 484](#)
- [Managing Remote Authentication Servers on page 483](#)
- [Junos Space Log In Behavior with Remote Authentication Enabled on page 486](#)

Junos Space Log In Behavior with Remote Authentication Enabled

This topic describes Junos Space log in behavior with remote authentication only or remote-local authentication enabled.

Login Behavior with Remote Authentication Only Enabled



WARNING: To avoid a BEAST TLS 1.0 attack, whenever you log in to Junos Space 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.

- The user logs in with the correct credentials:
 - As long as the user's password is on the remote server, login is successful.
 - If the first remote authentication server is present, log in success or failure solely depends on the password stored there, as no other servers are consulted. If the first authentication server is not reachable, the second server is connected in the order specified. If no authentication server is reachable, Junos Space tries the local password in the Junos Space 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 is denied.



NOTE: Authentication servers, for security purposes, will not distinguish between these two cases. Therefore, Junos Space must always treat these type of logins as an authentication failure. Once Junos Space receives a response from an authentication server, the only options are immediate success or failure. No other servers are contacted.

- If no authentication servers are reachable, Junos Space tries the local password. If the local password does not exist, or if the credentials do not match, logging into Junos Space fails.
- The user attempts to log in but the remote server is down—See the previous two log in behaviors for details. Notify the Junos Space administrator when a remote authentication server is down.
- The user attempt to login when the remote authentication server has the correct credentials, but there is no equivalent user in Junos Space. The user can not log in to Junos Space because there is no role information.
- The user attempts to login when the remote authentication server is configured for Challenge/Response:

- If the remote authentication server indicates a challenge is required, it provides the challenge question. Junos Space displays the challenge question to the user on the Juniper login page, and waits for the user's response.
- If the challenge question is answered correctly, it is possible that the authentication server may request additional challenges.
- If the challenge question is answered incorrectly, it is possible that the authentication server may re-challenge the user with the same challenge, use a different challenge, or fail the login attempt completely. It's up to the authentication server configuration.
- If the final challenge is answered correctly, the user logs in successfully.

Log In Behavior with Remote-Local Authentication Enabled



WARNING: To avoid a BEAST TLS 1.0 attack,, whenever you log in to Junos Space 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.

- The user logs in with the correct credentials— Junos Space checks the remote authentication servers first. If authentication fails or if a server is unreachable, Junos Space tries to authenticate locally. If there is a Junos Space local password and the credentials match, the user logs in successfully.
- The user logs in with incorrect credentials— Junos Space checks the remote authentication servers first. If authentication fails or if a server is unreachable, Junos Space tries to authenticate locally. If there is a Junos Space local password and the credentials match, the user logs in successfully.
- The user attempts to login but the remote server is down— Authentication occurs using only the local password. If the password exists and there is a match, the user logs in successfully. If the password does not exist and there is no match, the user does not log in successfully.
- The user attempts to login when the remote authentication server has the correct credentials, but there is no equivalent user in Junos Space. The user can not log in.
- The user attempts to login when the remote authentication server is configured for Challenge/Response:
 - If the remote authentication server indicates a challenge is required, it provides the challenge question. Junos Space displays the challenge question to the user on the Junos Space login page, and waits for the user's response.
 - If the user answers challenge question correctly, it is possible that the authentication server may request additional challenges.
 - If the user answers challenge question correctly, it is possible that the authentication server may re-challenge the user with the same challenge, use a different challenge, or fail the login attempt completely. It's up to the authentication server configuration.
 - If the user answers challenge question correctly, log in is successful.

**Related
Documentation**

- [Remote Authentication Overview on page 479](#)
- [Logging In to Junos Space on page 3](#)
- [Configuring Remote Authentication Method Workflows on page 481](#)
- [Understanding Junos Space Authentication Modes on page 480](#)
- [Creating a Remote Authentication Server on page 484](#)
- [Modifying Authentication Settings on page 486](#)

CHAPTER 42

Managing Tags

- [Overview on page 491](#)
- [Managing Tags on page 492](#)
- [Creating Tags on page 498](#)

Overview

- [Managing Tags Overview on page 491](#)

Managing Tags Overview

Use Manage Tags to view tag information, and create, share, rename, or delete them.

There are three roles relevant to tags:

- To access Manage Tags and perform the above-mentioned tasks, you must have the System Administrator role. You can create public and private tags. You can also create hierarchies of tags.
- To share user-defined tags by publishing them so that others can use them, you must have the Tag Administrator role.
- Any Junos Space user can tag, view, apply, and untag objects.

Tag names should not start with space, can not contain a comma, double quote, parentheses, and can not exceed 255 characters.

To use Tags:

1. Create a private or shared tag using the **Platform > Administration > Manage Tags > Create Tag** user interface. See [“Creating a Tag” on page 498](#).
2. Tag an object on an inventory page. For example you can tag an object on the **Platform > Manage Devices** inventory page. Once you tag an object, you can view or untag existing tags. See [“Tagging an Object” on page 495](#) and [“Untagging Objects” on page 497](#).
3. (Optional) Create hierarchical tags and manage them in the Tag Hierarchy pane in the Tag view on an inventory landing page for taggable objects (such as devices).
4. Manage tags using the **Platform > Administration > Manage tags** inventory page. You can share, rename, or delete tags. See [“Viewing Tags” on page 496](#), [“Renaming Tags” on page 494](#), [“Deleting Tags” on page 495](#)

- Related Documentation**
- [Tagging an Object on page 495](#)
 - [Viewing Tags on page 496](#)
 - [Untagging Objects on page 497](#)
 - [Filtering Inventory Using Tags on page 497](#)

Managing Tags

- [Managing Tags on page 492](#)
- [Sharing a Tag on page 493](#)
- [Renaming Tags on page 494](#)
- [Deleting Tags on page 495](#)
- [Tagging an Object on page 495](#)
- [Viewing Tags on page 496](#)
- [Untagging Objects on page 497](#)
- [Filtering Inventory Using Tags on page 497](#)

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. The inventory page allows you to manage and manipulate personal tags you created. You must be the System Administrator role to manage tags.

The View Tags page is blank unless there are some public tags or private tags you created. Tags are only visible to you unless you have the Tag Administrator share them and make them public to all users. Tags created by other users are private and only visible to them unless the Tag Administrator shares them; making them public.

Manage all tags applied to inventory objects from the **Platform > Administration > Manage Tags View Tags** inventory page. You can share, rename or delete tags. The **View Tags** page is blank until you create one or more tags using the **Platform > Administration > Create Tag** task.

Viewing Tags On the View Tags Inventory Page

To view tags on the **View Tags** inventory page:

- All tags created appear on the **View Tags** inventory page in tabular view listed alphabetically by tag name.

You can filter inventory objects by a tag name (see [“Filtering Inventory Using Tags” on page 497](#)).

Viewing Tag Information

Tag data includes the tag name, access type, and the number of objects tagged by a particular tag. See [Table 66 on page 493](#).

Table 66: Tag Information

Tag Data	Description
Name	Unique tag name. Tag names cannot start with a space or be longer than 256 characters.
Access Type	Tags can either be public (shared) or private (visible only to the creator).
Tagged Object Count	The number of objects in all workspace inventory pages by the tag.

You can sort and hide columns. For more information about manipulating tables in tabular view, see [“Inventory Pages Overview” on page 28](#).

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.

You can also select the **Page** link to select all tags at once. To deselect all tags, you can also click the None link.

2. Select a command from the Actions drawer or right-click pop-up menu.

You can share (see [“Sharing a Tag” on page 493](#)), rename (see [“Renaming Tags” on page 494](#)), delete (see [“Deleting Tags” on page 495](#)), or deselect all selected tags.

Related Documentation

- [Managing Tags Overview on page 491](#)
- [Tagging an Object on page 495](#)
- [Viewing Tags on page 496](#)
- [Untagging Objects on page 497](#)
- [Creating a Tag on page 498](#)

Sharing a Tag

User-defined tags are always created as private tags initially. When you feel that your tag has public value, sharing a tag makes it public for all users to use it to tag objects on a workspace inventory page. To share a tag, you must have Tag Administrator privileges.

To share a tag

1. Select **Platform > Administration > Manage Tags View Tags** inventory page:
2. Select one or more private tags on the **View Tags** inventory page.

3. Select **Share Tag** from the Actions drawer or right-click to select **Share Tag** from the pop-up menu.

The **Share Tag** status box appears to indicate whether the tag sharing is successful.

You can also share a tag when you create one (see [“Creating a Tag” on page 498](#)).

4. Click **OK**.

The tag **Access Type** changes on the **View Tags** inventory table from **private** to **public**.

Related Documentation

- [Managing Tags Overview on page 491](#)
- [Managing Tags on page 492](#)
- [Renaming Tags on page 494](#)
- [Deleting Tags on page 495](#)
- [Creating a Tag on page 498](#)

Renaming Tags

The Rename Tag command provides you flexibility to reorganize or re-categorize managed objects according to your changing needs.

To rename a tag:

1. Navigate to the **Platform > Administration > Manage Tags** inventory page.

The **View Tags** page appears.

2. In the **View Tags** table, select the tag you want to rename.

3. Select **Rename Tag** from the Actions drawer.

The **Rename Tag** dialog box appears.

4. Type a tag name in the **New Name** text field.

A tag name should not start with a space, cannot contain a comma, double quote, parentheses, or exceed 255 characters

5. Click **Rename**.

The old tag is renamed and saved in the database. You see the renamed tag in the **View Tags** table.

When you navigate to the manage inventory page from which you created the tag, you will see the renamed tag name in the Actions > **View Tags** dialog box and in the search list.

Related Documentation

- [Managing Tags Overview on page 491](#)
- [Managing Tags on page 492](#)
- [Sharing a Tag on page 493](#)
- [Deleting Tags on page 495](#)

- [Creating a Tag on page 498](#)
- [Filtering Inventory Using Tags on page 497.](#)

Deleting Tags

Use the Delete Tags action to remove managed object tags you no longer need.

To delete a tag:

1. Navigate to the **Platform > Administration > Manage Tags** inventory page.
The **View Tags** page appears.
2. In the **View Tags** table, select one or more tags you want to delete.
3. Select **Delete Tag** from the Actions drawer. You can also right-click the selected inventory object(s) and select **Delete Tags** from the pop-up menu.

The **Delete Tags** dialog box appears to confirm that you want to delete the tag.

4. Click **Delete**.

The tag is removed from the database and no longer appears in the View Tags table.

Related Documentation

- [Managing Tags Overview on page 491](#)
- [Managing Tags on page 492](#)
- [Sharing a Tag on page 493](#)
- [Renaming Tags on page 494](#)
- [Creating a Tag on page 498](#)

Tagging an Object

You can create user-defined tags in an application workspace inventory page to easily categorize and organize managed objects. Subsequently, you can view and use these tags to easily search for multiple objects to view status or perform a bulk action on them without having to select each individually.

To tag an object:

1. Navigate to an application workspace manage inventory page. For example, select **Platform > Devices > Manage Devices**.
2. Select the inventory object(s) you want to tag.
3. Select **Tag It** from the Actions drawer.

The **Apply Tag** dialog box appears.

4. Select or type the tag name in the text box.

If you have existing tags, start to type a tag name in the name field. Existing tags appear in the selection box.

5. Click **Apply Tag**. This action tags the object and stores the tag in the database.

**Related
Documentation**

- [Managing Tags Overview on page 491](#)
- [Managing Tags on page 492](#)
- [Viewing Tags on page 496](#)
- [Untagging Objects on page 497](#)
- [Filtering Inventory Using Tags on page 497](#)
- [Creating a Tag on page 498](#)

Viewing Tags

The View Tags action from application workspace inventory pages allows you to see all of the tags that you have assigned a managed object on your network. You must first tag a managed object to see its tags.

Use tags to label and categorize objects in your network, such as subnets, devices, services, users, customers, and so forth so you can filter, monitor, or perform batch actions on them without having to select each object separately.

Tags created by you are private and only visible to you unless you have the Tag Administrator share them to the public domain, making them public. Tags created by other users are only visible to them unless the Tag Administrator shares them, then you can view them.

To view tags on an inventory object:

1. Navigate to a workspace inventory page.
2. Select only one inventory object for which you want to view tags.
3. Select **View Tags** from the Actions drawer. You can also right-click an object and select **View Tags** from the pop-up menu.

The **View Tags** dialog box appears with a tag list displaying all tags applied to the selected object.

4. Click **OK**.

**Related
Documentation**

- [Managing Tags on page 492](#)
- [Tagging an Object on page 495](#)
- [Untagging Objects on page 497](#)

Untagging Objects

You can untag or remove a tag from an object on a workspace inventory page. You can only select one object at a time to untag.

To untag an object:

1. Navigate to a workspace inventory page. For example, select **Platform > Devices > Manage Devices**.
2. Select one object on the workspace inventory page at a time.
3. Select **Untag** in the Actions drawer or right-click an object and select **Untag** from the pop-up menu.

The **Untag the Object** dialog box appears.

4. Select the tag that you want to remove and
5. Click **Untag**.

Related Documentation

- [Managing Tags Overview on page 491](#)
- [Managing Tags on page 492](#)
- [Tagging an Object on page 495](#)
- [Viewing Tags on page 496](#)
- [Creating a Tag on page 498](#)

Filtering Inventory Using Tags

You can use tags to filter objects on a workspace inventory page. Filtering allows you to view only the objects that you want categorized by the tag name.

To filter using a tag:

1. On the workspace inventory page, click the magnifying glass in the search field at the top-right of the page. You can also type the first letter of the tag name.

The list appears with the object names on the top and the tag names on the bottom. If you clicked a letter in the search field, only the tag names starting with that letter appear.

2. Click a tag name in the list.

Only the inventory objects with that tag name appear. You see **Filtered By the tag** name at the top-left of the page.

3. Click the red **X** to unfilter the inventory page.

Related Documentation

- [Managing Tags Overview on page 491](#)
- [Managing Tags on page 492](#)
- [Tagging an Object on page 495](#)

- [Viewing Tags on page 496](#)
- [Untagging Objects on page 497](#)
- [Creating a Tag on page 498](#)

Creating Tags

- [Creating a Tag on page 498](#)

Creating a Tag

To create a tag:

1. Select **Platform** > **Administration** > **Manage Tags** > **Create User** task.
The **Create Tags** dialog box appears.
2. If necessary select the **Share Tag** option.
When you share a tag, all users can use that tag. Only the Tag Administrator can publish tags to the public domain.
3. Type a tag name in the text box.
A tag name should not start with a space, cannot contain a comma, double quote, parentheses, or exceed 255 characters
4. Click **Create**.
The tag appears in the **View tags** inventory page. If the tag is shared it is public; if not it is private.

Related Documentation

- [Managing Tags Overview on page 491](#)
- [Managing Tags on page 492](#)
- [Sharing a Tag on page 493](#)
- [Renaming Tags on page 494](#)
- [Deleting Tags on page 495](#)

Managing Permission Labels

- [Managing Permission Labels Overview on page 499](#)
- [Working With Permission Labels on page 501](#)

Managing Permission Labels Overview

Permission Labels are the tool by which you can enforce object-level access control; for example, you can restrict a user with the role of Device Manager to a subset of devices that you choose. Working with permission labels is therefore an extension to user management.

Permission Labeling enables you to define users' access to objects in—or elements of—Junos Space. These objects can be users, roles, or devices. Prior to the release of Junos Space 11.3, access was associated solely with roles. It was the role that defined the elements a user could access; for example, a Device Admin could access the Devices workspace, and work with all the devices there. Using Permission Labels enables you to restrict a user's access to subordinate parts of the elements associated with his or her role.

You can now confer the Device Admin role on a user, and then assign a permission label to that user to restrict him or her to managing only devices with the same label, as opposed to all the devices in Junos Space.

Similarly, you can attach a permission label to the users in a particular location (for example, San Francisco), and assign the same label to a user administrator. Provided all the users in other locations are also labeled—but differently—that user administrator's activities are confined to managing users in San Francisco.

The same principle applies to roles. You can attach a label to the roles for managing other applications, such as Service Now or Network Activate, and then assign the same label to appropriately qualified users.

Working with permission labels is a three step process, involving the creation of a label, assigning that label to a user, and attaching that label to an object. You can choose not to use permission labels at all. However, once you decide to implement them, they have an effect on all users and objects, in that labeling an object immediately restricts it to viewing by users with the same label. Only users with the appropriate roles can manipulate objects in Junos Space, and without the appropriate distribution of permission labels *in addition*, even users with the appropriate roles cannot see labelled objects.

These are the possible combinations:

- If you do not assign a label to a user, that user can see all the unlabeled objects necessary to perform the tasks associated with his or her role.
- If you assign a label to a user, but do not attach the same label to any objects, the effect is the same as above.
- If you do not attach a label to an object, all users with the appropriate role can see that object.
- If you attach a label to an object, only users to whom the same label has been assigned, and who have the appropriate role can see and access that object.

Examples of labelling discrepancies:

- You attach a label to some of your devices, but you forget to assign that label to any users. Result: only users with the Permission Label Manager role can see those devices.
- You attach a "UK" label to all your devices, but you assign the device manager user who is supposed to manage them the "London" label. Result: the device manager cannot even see the devices.
- You attach the "Bengaluru" permission label to some of your devices. You assign the same label to the person who is supposed to manage *only* those devices, not the devices in Chennai. You forget to label the Chennai devices. Result: the device manager in Bengaluru can see all the devices, but *only* he or she can see the Bengaluru devices.

Both objects and users can have multiple permission labels that can be assigned and attached or removed at any time. • but a user who is both a Permission Label Manager + Device Admin will only be able to execute operations on Devices)



NOTE: • If a system is upgraded from a previous release to 11.3, all elements will be global by default (no permission labels applied), and users will not have any permission labels pre-assigned to them. The Super Admin will be able to execute all the new Permission Label tasks.

Because assigning permission labels amounts to controlling access, it requires a special role, Permission Label Administrator. Any user who can perform this task can see all the labels for all the objects appropriate to his or her other roles. In other words, to label configuration files, you also need to have the Configuration File Manager role. To the Permission Label Administrator role belong three tasks:

- Design permission label—Create and delete permission labels.
- Assign permission label—Assign permission labels to users
- Attach permission label—Attach permission labels to objects

Instructions for performing these three tasks are in [“Working With Permission Labels” on page 501](#). You might wish to separate these tasks because you might not want a user to create an object such as a device, label it, and then ensure only he or she has access to that object.

Operations with permission labels generate Audit Log entries, showing not only the usual level of detail with the task performed, etc., but also information about the person who performed the task:

- Login ID
- First name
- Last name
- Email address
- Assigned role

**Related
Documentation**

- [Working With Permission Labels on page 501](#)
- [Role-Based Access Control Overview on page 371](#)
- [Understanding How to Configure Users to Manage Objects in Junos Space on page 372](#)
- [Predefined Administrator Roles on page 373](#)

Working With Permission Labels

From an efficiency perspective, it works best to create all your permission labels at once. Therefore, before you begin, it is best to map out what you intend to do, so that you can correctly match up permission labels with objects and users. For a discussion of the consequences of mistmatching them, see [“Managing Permission Labels Overview” on page 499](#).

Once you have created your permission labels, you assign them to users and attach them to objects. The sequence in which you assign and attach does not matter.

These instructions assume you have prepared your mapping, and that the users to whom you will assign permission labels already have the appropriate roles (see [“Understanding How to Configure Users to Manage Objects in Junos Space” on page 372](#)).

Both objects and users can have multiple permission labels that can be assigned and attached or removed at any time.

1. [Creating Permission Labels on page 501](#)
2. [Assigning Permission Labels to Users on page 502](#)
3. [Attaching Permission Labels to Objects on page 503](#)

Creating Permission Labels

Note that you can only create, delete, or rename permission labels if your role includes the Design Permission Label task (see [“Role-Based Access Control Overview” on page 371](#)).

To create a permission label:

1. From within the Administration workspace, navigate to Manage Permission Labels > Create Permission Label.

The Create Permission Label dialog box appears.

2. In the Label Name box, enter an alphanumeric name. Spaces are acceptable, if not desirable.

The tag appears, listed on the Manage Permission Labels page.

You can rename or delete a permission label by selecting the label on the Manage Permission Labels page and selecting those commands from the Actions drawer.



NOTE: Every instance of a label is renamed. Users assigned the old label now automatically have the new, renamed label.

Assigning Permission Labels to Users

Note that you can only assign permission labels to users or remove them from users if your role includes the Assign Permission Label task (see [“Role-Based Access Control Overview” on page 371](#)).

To assign a permission label to a user:

1. From within the Administration workspace, navigate to Manage Permission Labels.

The Manage Permission Labels page appears.

2. Select the permission label you want to assign and select **Assign Permission Labels to Users** from the Actions drawer.

The Assign Permission Labels to Users page appears.

3. Select the appropriate user(s). To page through the table, use the controls on the status bar at the bottom of the table. This also shows the total number of pages of records, the current page being displayed, and the number of items per page, which can be adjusted.

The following information appears for each user: login IDs, their last and first names, and the permission labels already assigned to them.

4. Click **Assign**.

The Manage Permission Labels page reappears, displaying the label name with the Assigned Users Count adjusted to reflect the number of users assigned to the label.

You can un-assign or remove a permission label from a user by selecting the label on the Manage Permission Labels page and selecting **Remove permission label from user** from the Actions drawer. Only one label at a time can be removed, although you can remove it from multiple users at the same time.

Attaching Permission Labels to Objects

In the context of permission labels, objects can be users, devices, and roles.

Note that you can only assign permission labels to objects or remove them from objects if your role includes the Attach Permission Label task (see [“Role-Based Access Control Overview” on page 371](#)).

To attach a permission label to an object:

1. From within the Administration workspace, navigate to Manage Permission Labels.

The Manage Permission Labels page appears.

2. Select the permission label you want to assign, and select **Attach Permission Labels to Objects** from either the Actions drawer.

The **Manage Permission Label and Objects** page appears. On the left, it displays a list of object types to which permission labels have already been attached. On the right, it displays a list of the actual objects of the type highlighted on the left, to which labels have already been attached. If no labels have yet been attached, these lists are empty.

3. If necessary, to select the type of object to which the label is to be attached, click the plus icon to add a managed object type. This saves you having to search through all the objects managed by Junos Space.

There are three types of object to which you can attach a label:

- Users—User Object—Managed object type for admin user
- Roles—Role Object—Managed object type for RBAC (Role-based access control) Role, which actually means any role
- Devices—Device-Object—Managed object type for device objects.

The **Add More Object Types** dialog box appears, displaying the names of the objects not yet in the table and their descriptions.

4. Select one or more object types and click **OK**.

The **Manage Permission Label and Objects** page reappears, now displaying the type(s) of object you selected in the last step.

5. To choose the particular object to which a label is to be attached, select it from the **Device Object** or **Role Object** or **User Object** list if it is already displayed, otherwise click the plus icon.

The **Add More Objects** dialog box appears. At the top of the dialog box appears the name of the label with which you are currently working. Below is a table showing the names of the individual objects in the category you selected, their descriptions, and the labels already attached to them.

6. Select the appropriate object(s). To page through the table, use the controls on the status bar at the bottom of the table. This also shows the total number of pages of

records, the current page being displayed, and the number of items per page, which can be adjusted.

7. Click **OK**.

The **Manage Permission Label and Objects** page reappears, now displaying the type of object plus the individual objects you selected in the last step.

You can unattach or remove a permission label from an object by selecting the label on the Manage Permission Labels page and selecting **Remove permission label from object** from the Actions drawer. Only one label at a time can be removed, although you can remove it from multiple objects at the same time.

**Related
Documentation**

- [Managing Permission Labels Overview on page 499](#)
- [Role-Based Access Control Overview on page 371](#)
- [Understanding How to Configure Users to Manage Objects in Junos Space on page 372](#)

CHAPTER 44

Managing DMI Schemas

- [Managing DMI Schemas Overview on page 506](#)
- [Updating a DMI Schema on page 508](#)
- [Creating a tgz File for Updating a DMI Schema on page 511](#)
- [Setting a Default DMI Schema on page 513](#)
- [Troubleshooting DMI Schema Management on page 514](#)

Managing DMI Schemas Overview

To manage multiple DMI schemas (device management interface schemas) for Junos-based device families and device types, use the DMI schema management workspace.

Each device type is described by a unique data model (DM) that contains all the configuration data for it. The DMI schema lists all the possible fields and attributes for a type of device. The newer schemas describe the new features coming out with recent device releases. It is important that you load into Junos Space all your device schemas, otherwise only a default schema will be applied when you try to edit a device configuration using the device configuration edit action in the Devices workspace (see [“Editing Device Configuration Overview” on page 68](#)). If Junos Space has exactly the right DMI schema for each of your devices, you can access all of the configuration options specific to each device.

The DMI Schema Management workspace enables you to add or update schemas for all Junos Space devices. It also lets you know when you do not have the schema for a device. On the Manage DMI Schemas page, in the tabular view, when it says under the column DMI Schema "Need Import" it means the JunOS schema for that device OS is not bundled with Space and you need to download it from the Juniper Schema Repository.

An important aspect of schema management is setting a default DMI schema for each device family. When you create a device template, the template needs a default schema for the device family (see [“Selecting the Device Family and Naming a Device Template Definition” on page 169](#)). Conversely, in order to access all the configuration options for a particular device via the Edit Device Configuration action in the Devices workspace, you need to have the DMI schema specific to that device.

The schema management facility enables you to connect with Juniper’s SVN Repository so that you can download new schemas as necessary.



NOTE: Ensure that you only download device schemas pertaining to the devices that are currently managed from Junos Space. As and when more devices are added, you can download the device schemas that are relevant to the newly added devices.

A schema is delivered in the form of a .tgz file, an archive containing multiple files reflecting the configuration hierarchy for the selected device family, platform and OS version. You can even create your own tgz file (see [“Creating a tgz File for Updating a DMI Schema” on page 511](#)).

A typical goal in the DMI Management workspace—**Manage DMI Schemas**—is to enable a device to be managed in JUNOS Space.

For each DMI schema currently installed, the **Manage DMI Schemas** inventory landing page displays:

- Name
- Device Family
- OS Version
- Device Series
- State—default or otherwise

You can view the schemas in tabular form or as thumbnails. In tabular view, you can sort the schemas by clicking on their column headings.

You can select one or more schemas and perform the following actions on them using the Actions drawer or the right mouse-click menu:

- Set default schemas

Do this to return a custom configuration of a DMI schema to the default.

- Tag and untag schemas
- View schema tags, with
 - Tag Name
 - Access Type

To add or update a DMI schema, see [“Updating a DMI Schema” on page 508](#).

**Related
Documentation**

- [Updating a DMI Schema on page 508](#)
- [Setting a Default DMI Schema on page 513](#)
- [Creating a tgz File for Updating a DMI Schema on page 511](#)
- [Troubleshooting DMI Schema Management on page 514](#)
- [Device Discovery Overview on page 39](#)
- [Add Deployed Devices Wizard Overview on page 51](#)

Updating a DMI Schema

To add or update a DMI schema, you must have the .tgz archive containing it on the machine running the Junos Space GUI. There are several ways of acquiring such files. You can:

- Create your own file (see [“Creating a tgz File for Updating a DMI Schema” on page 511](#)).
- Download a file from Juniper’s SVN Repository. This topic contains the instructions for doing this.
- Get a file from Juniper support staff.

From the **Schema Update** page, Junos Space is able to identify which schemas you already have installed, and based on the discovered devices, also suggests new schemas. You can, however, pick other available schemas and download them as well, or instead.

On the **Schema Update** page, you can either:

- Install a DMI schema on Junos Space using a file you already have on the machine running the Junos Space GUI.

Or:

- Get a DMI schema from Juniper and update Junos Space, which involves the following sub-tasks:
 - Configure a connection to the SVN Repository.
 - Connect to the SVN Repository and install DMI schemas on Junos Space.

To install a DMI schema update on Junos Space:

From the Network Application Platform, navigate to **Administration > Manage DMI Schemas > Update Schema**.

The **Update Schema** page appears.

If you already have the tgz file on your system:

1. Select the **Archive (tgz)** option button.
2. Click **Browse**.

The **File Upload** dialog appears.

3. Navigate to the .tgz file and select it. Click **Open**.

The **Schema Update** page reappears, displaying the .tgz filename in the **Browse** field.

4. Click **Upload**.

Do not move away from the **Schema Update** page while the .tgz file is uploading to Junos Space. Note that the process can take some time, depending on how many schemas are in the file.

5. Select the desired schema and click **Install**.

The **Manage DMI Schemas** inventory landing page reappears, displaying the newly installed schema.

If you need to download the file from the SVN Repository, and you have not yet configured the connection to the repository:

1. Have the following to hand:

- URL : <https://xml.juniper.net/dmi/repository/trunk>
- Username: userName
- Password: userPasswd

2. Select the **SVN Repository** option button.

3. Click **Configure**.

The **SVN Access Configuration** dialog box appears.

4. Enter the SVN URL, the username and the password in the appropriate text fields. Click **Test Connection**.



NOTE: Do not include leading or trailing spaces when copying/pasting or when typing in the SVN URL. If you do, the URL is not parsed correctly and the connection does not succeed.

A message appears to tell you whether the connection was established successfully or not.

5. Whether or not connection was successful, click **OK**.

The **SVN Access Configuration** dialog box reappears.

6. Either:

- If the connection failed, click **Cancel**, find the correct credentials, and repeat the above steps.
- If the connection was successful, click **Save**.

The **Schema Update** page reappears, displaying the SVN Repository URL.

If you need to install the file from the SVN Repository, and you have already configured the connection to the repository:

1. Select the SVN Repository option button.
2. Ensure the repository's URL appears in the URL field. If the field is blank, you must configure the connection. See step 3 above.

3. Click **Connect**.

The content of the repository with DMI schema releases appears in table form under **Available Updates** on the **Schema Update** page. The already installed versions are preselected.

Junos Space detects and marks any missing schemas with a red arrow symbol. Missing schemas are the OS versions on devices that Junos Space discovers in your network, but which have not been installed on Junos Space.

You can sort by clicking on the column headings: Device Family, Release, Date. To change the display, click the arrow that appears when you click a column heading. To determine whether sorting should be ascending or descending, click the arrow that appears when you click a column heading.

4. (Optional) To display the recommended schemas only, select the **Show recommended schemas** check box.

Select the desired schemas.



NOTE: You need at least one schema for each device family in your network. See [“Setting a Default DMI Schema” on page 513](#).

Click **Install**.

A message appears, asking you to wait. After installation, the **Manage DMI Schemas** page reappears, displaying the new schema(s).

**Related
Documentation**

- [Managing DMI Schemas Overview on page 506](#)
- [Setting a Default DMI Schema on page 513](#)
- [Troubleshooting DMI Schema Management on page 514](#)
- [Creating a tgz File for Updating a DMI Schema on page 511](#)

Creating a tgz File for Updating a DMI Schema

This topic describes how to create a tgz file containing a DMI schema for any Junos-supported device.

Use the .tgz file to update a DMI schema on Junos Space (see “Updating a DMI Schema” on page 508).

This topic contains instructions for creating a .tgz file on Linux or on Microsoft Windows.

Linux

Create a .tgz file containing a DMI schema on Linux as follows:

Before you begin, either install the Svn(Subversion) Client on Linux for Ubuntu:

```
> sudo bash
```

```
> apt-get install subversion
```

Or:

For other versions, consult:

http://wiki.greenstone.org/wiki/index.php/Install_SVN_on_Linux

The tgz must comply with the given format .

All the files must be extracted to a folder structured as follows:

```
dmi/deviceFamily/releases/osVersion/....
```

Examples For the whole Junos family

```
svn --username=userName --password=userPasswd co
http://xml.juniper.net/dmi/repository/trunk/junos/ dmi/junos/
tar czvf juniper-schema-repo-test.tgz dmi
```

For selected OS versions

```
svn --username=userName --password=userPasswd co
http://xml.juniper.net/dmi/repository/trunk/junos/releases/10.2R1.7/
dmi/junos/releases/10.2R1.7/
tar czvf juniper-schema-repo-test.tgz dmi
```

```
svn --username=userName --password=userPasswd co
http://xml.juniper.net/dmi/repository/trunk/junos/releases/10.4R2.3/
dmi/junos/releases/10.4R2.3/
tar czvf juniper-schema-repo-test.tgz dmi
```

```
svn --username=userName --password=userPasswd co
http://xml.juniper.net/dmi/repository/trunk/junos-es/releases/10.4R2.3/
dmi/junos-es/releases/10.4R2.3/
tar czvf juniper-schema-repo-test.tgz dmi
```

Windows

Create a .tgz file containing a DMI schema on Windows as follows:

1. Install the Subversion (SVN) Client on Windows using the following instructions:

<http://tortoisesvn.tigris.org/>

2. Install 7zip to generate a .tgz on Windows using the following instructions:

<http://www.7-zip.org/>

3. Check out the files from SVN using the Subversion client:

Set the SVN URL to <http://xml.juniper.net/dmi/repository/trunk>. Right-click and select **Checkout**.

4. Make the following settings:

URL of repository

<http://xml.juniper.net/dmi/repository/trunk/junos/releases/10.4R2.6>

Checkout directory

C:\dnld1\dmi\junos/releases/10.4R2.6

Checkout Depth

Immediate children, including folders

Leave the **Omit externals** check box empty.

Select **HEAD revision**. Click **OK**.

5. Create the tar file using 7-zip:

In 7-zip, right-click the DMI folder and select from the menu **Add To Archive**.

Select **Tar Format 2.5**.

6. Create gzip using 7-zip:

In 7-zip, right click the DMI .tar file and select from the menu **Add to Archive**.

Select **Zip Format**.

Related Documentation

- [Managing DMI Schemas Overview on page 506](#)
- [Setting a Default DMI Schema on page 513](#)
- [Updating a DMI Schema on page 508](#)
- [Troubleshooting DMI Schema Management on page 514](#)

Setting a Default DMI Schema

Set a default DMI schema for each device family to enable Junos Space to apply an appropriate schema to a device family. In a clean install situation, Junos Space automatically matches DMI schemas to device families, but in all other situations, you should set a default DMI schema for each device family.

When creating a device template definition, the system will use a default DMI schema for the device family unless you select a schema. See [“Selecting the Device Family and Naming a Device Template Definition” on page 169](#).

The configuration edit action in the Devices workspace always checks for an exact match between device and DMI schema. If it does not find a match, it will use the default schema (see [“Editing Device Configuration Overview” on page 68](#)).

To set a default DMI schema,

1. Navigate to **Network Application Platform > Administration > Manage DMI Schemas**.

The **Manage DMI Schemas** page appears, in the tabular view displaying the data in a table with the following columns:

- Device Family
- OS Version
- Device Series
- State—Whether default or not. An empty cell in this column means that the DMI schema in that row is not the default.

In the thumbnail view, this information is presented on each thumbnail.

2. In the tabular view, select the row that contains the appropriate combination of device family, OS version, and device series, and mouse over the Actions drawer to select **Set Default Schema**.

In the thumbnail view, select the appropriate thumbnail and perform the same action.

The **Set Default DMI Schema** dialog box opens, displaying the DMI schema name, device family, and OS version.

3. Click **Set Default**.

If any other schema was previously the default, in the tabular view, its cell in the **State** column empties, and the word “Default” appears in the State column for the selected schema. In the thumbnail view, the default status is indicated by an orange star on the icon for a DMI schema, and the word “Default” below the OS version.

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 506](#)
- [Updating a DMI Schema on page 508](#)

- [Selecting the Device Family and Naming a Device Template Definition on page 169](#)
- [Creating a tgz File for Updating a DMI Schema on page 511](#)
- [Troubleshooting DMI Schema Management on page 514](#)

Troubleshooting DMI Schema Management

This topic describes common problems associated with DMI schema management and provides solutions where possible. The following are issues that might be encountered:

- No schemas in new installation of Junos Space
- Schema tree not displayed

No schemas in new installation of Junos Space

When the Junos Space server first comes up, all the schemas for all the discovered devices should be pre-installed. Navigate to **Network Application Platform > Administration > Manage 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 **Manage DMI Schemas** page is empty, installation was unsuccessful.

There is no workaround for this problem.

Schema tree not displayed

Typically, if a schema is defective, its schema tree will not be displayed.

Verify that a particular schema has been parsed successfully: navigate to **Network Application Platform > Device Templates > Manage Definitions > Create Definition**. Select the schema in question and click **Next**.

The schema tree or hierarchy of configuration options should be displayed on the left. All nodes should be navigable, that is, it should be possible to drill down into the hierarchy to reach all the options.

If the topmost node (**Configuration**) cannot be opened to reveal the hierarchy, the schema was corrupted during porting (grep for SchemaMgr ERROR in server.log).



NOTE: One defective schema will not affect the other DMI schemas, which will still be available for use.

The solution to this problem is to replace one or more existing DMI schemas on the Junos Space server.

There are two ways of doing this:

- Using a script supplied by Juniper support. This requires restarting jboss.
- Using your own tgz file. This does not require restarting jboss.

For instructions, see [“Creating a tgz File for Updating a DMI Schema” on page 511](#).

**Related
Documentation**

- [Managing DMI Schemas Overview on page 506](#)
- [Updating a DMI Schema on page 508](#)
- [Creating a tgz File for Updating a DMI Schema on page 511](#)
- [Setting a Default DMI Schema on page 513](#)

PART 11

Index

- [Index on page 519](#)

Index

Symbols

#, comments in configuration statements.....	xxix
(), in syntax descriptions.....	xxix
< >, in syntax descriptions.....	xxix
[], in configuration statements.....	xxix
{ }, in configuration statements.....	xxix
(pipe), in syntax descriptions.....	xxix

A

access control	
object level.....	499
actions drawer, inventory page.....	33
active user history graph.....	23
Add deployed devices	
overview.....	51
add devices	
overview.....	99
adding deployed devices.....	52
adding devices.....	101
adding Junos Space application.....	458
Admin	
configuring OpenNMS.....	305
administrators	
CLI.....	401
maintenance mode.....	402
overview.....	401
user interface See user administration	
Advanced tab	
filling in.....	185
alarms	
viewing, acknowledging,	
unacknowledging.....	294
application	
adding.....	458
Platform, adding.....	463
uninstalling.....	467
upgrading.....	460
Application Chooser.....	13
icon.....	12
overview.....	9
starting.....	12

application dashboard.....	13
applications	
managing.....	451
settings, modifying.....	454
auto resync device.....	454
automatic logout of idle user sessions	
(mins).....	454
maximum auto resync waiting time	
(secs).....	454
switching between.....	9
assets	
tracking and searching for.....	289
audit log	
UTC to local timestamp, converting.....	363
audit logs	
archive file, naming conventions.....	364
archiving and purging.....	364
archiving to local server.....	365
archiving to remote server.....	366
default directory.....	357
exporting.....	367
overview.....	357
table view.....	359
user privileges.....	359
viewing	
most active users in last 24 hours.....	363
statistics.....	361
audit logs table	
description.....	360
job ID.....	360
task results.....	360
timestamp.....	360
audit trails	
exporting.....	367
authentication modes	
local.....	480
remote.....	480
remote-local.....	480
authentication server	
creating.....	484
modifying.....	486
auto resync device application setting.....	454
automatic logout of idle user sessions (mins)	
application setting.....	454
automatic resynchronization	
disabling.....	97

B

backup and restore See database	
---------------------------------	--

braces, in configuration statements.....	xxix
brackets	
angle, in syntax descriptions.....	xxix
square, in configuration statements.....	xxix

C

change request	
adding, editing or deleting a.....	75
change requests	
overview of.....	74
viewing.....	74
changing user passwords.....	4, 389
charts	
viewing.....	305
Checksum verification.....	235
checksum verification	
deleting results	277
procedure.....	253
verification result page controls	
description.....	277
Verify Checksum of Scripts on Device(s) dialog	
box.....	254
viewing results	277
CLI administrator	
changing password.....	401
name.....	401
tasks.....	401
comments, in configuration statements.....	xxix
commit script.....	225
conditions for deleting a fabric node.....	421
configuration file	
editing.....	334
configuration file editing	
, selecting perspective.....	69
configuration file inventory	
viewing.....	327
configuration file management	
overview.....	326
user privileges in.....	337
configuration files	
backing up.....	328
comparing.....	332
deleting.....	330
exporting.....	336
restoring.....	331
tagging, viewing, and untagging.....	337
untagging, tagging, and viewing.....	337
viewing, tagging, and untagging.....	337
configuration hierarchy.....	164

configuration options	
, editing.....	70
finding.....	174
configuration pages	
creating.....	170
configuring application setting.....	457
configuring application settings.....	456
connection profiles	
creating.....	113
managing.....	116
overview.....	111
connection status, for managed devices.....	66
conventions	
text and syntax.....	xxviii
creating a template definition.....	164
creating configuration pages.....	170
CSV files, managing	
overview.....	187
curly braces, in configuration statements.....	xxix
customer support.....	xxx
contacting JTAC.....	xxx

D

dashboard.....	13
statistics, viewing.....	23
database	
backup and restore, overview.....	431
device configuration data.....	40
device inventory data.....	40
database backup	
default directory.....	433
deleting files.....	443
local.....	433
overview.....	432
recurrence info, viewing.....	353, 444
recurring job.....	433
remote host.....	434
viewing files.....	442
database restore	
local.....	437, 438
overview.....	432
remote host.....	439
default gateway, changing.....	415
default values	
for configuration options, specifying.....	194
defining entered content.....	179
defining the operator's view.....	167

definition		device instances	
exporting a.....	201	deploying.....	108
importing a.....	200	device inventory	
definition states		data.....	40
template.....	215	exporting.....	62, 87
definitions, importing		overview.....	62
overview.....	162	device management	
Deleting a Device Image	243	overview.....	57
deleting scripts		device management IP	
from devices.....	256	adding.....	415
from Junos Space.....	251	deleting.....	415
deleting template definitions.....	199	device template	
deleting user.....	389	creating.....	206
deployed devices		overview.....	206
managing.....	54	device templates	
Deploying a Device Image	238	deleting.....	211
deploying scripts.....	252	deploying.....	209
deployment directory structure.....	252	inventory viewing.....	212
dialog box.....	253	modifying.....	210
Description tab		overview.....	158, 203
filling in the.....	178	statistics viewing.....	212
device		workflow.....	159
troubleshooting.....	94	devices	
viewing configuration information.....	94	auto-resynchronization, understanding.....	96
device configuration		changing resync time delay.....	97
editing.....	68	connecting to managed devices.....	122
device configuration changes		connecting to unmanaged devices.....	123
finalizing.....	72	connection status icons.....	64
device configuration data.....	40	deleting from Junos Space.....	79
device connection status.....	66	disabling auto-resync.....	97
device discovery		discovering.....	40
authentication.....	39	discovery, overview.....	39
Device Management Interface (DMI).....	39	exporting	
inventory and configuration data.....	40	license inventory.....	91
overview.....	39	logical inventory	40
specifying a probe method.....	43	management, overview.....	57
specifying credentials.....	45	physical interfaces, viewing.....	78
specifying device targets.....	41	physical inventory	40
viewing detailed reports.....	46	removing provisioning services before deleting	
viewing status.....	46	from Junos Space.....	80
device family		resynchronizing managed devices.....	80
selecting and naming a template		SSH connection.....	121
definition.....	169	viewing	
Device image deployment		connection status.....	63
in-service software upgrade.....	238	hardware inventory.....	63
Device Images		interfaces.....	63
Overview.....	223	IP address.....	63
device images and scripts overview.....	219	license inventory.....	63, 91
		operating system version.....	63

platform.....	63	monitoring node status	
statistics, by connection status.....	59	application logic.....	412
statistics, by Junos OS release.....	60	database.....	412
statistics, by platform.....	59	load balancer.....	412
disabling users.....	385	node functions	
discovery See device discovery		availability.....	409
DMI Schema		multinode.....	407
management overview.....	506	single node.....	406
DMI schema		node name.....	413
troubleshooting.....	514	node serial number.....	414
updating a.....	508	node threshold limit.....	407
DMI schemas		overview.....	405, 409
adding.....	511, 513	self monitoring.....	424
documentation		system health.....	422
comments on.....	xxix	fabric load history graph.....	23
downloading troubleshooting system log files		fabric node	
using CLI.....	475	deleting.....	421
E		filling in the Advanced tab.....	185
enabling scripts.....	255	filling in the description tab.....	178
configuration example for a commit		filling in the validation tab.....	181
script.....	255	font conventions.....	xxviii
configuration example for an event script.....	255	G	
configuration example for an op script.....	255	general tab	
dialog box.....	256	filling.....	176
enabling users.....	385	getting started assistants, using.....	5
error messages		See also help, accessing	
composing.....	184	global action icons.....	12
SSH session.....	123	Application Chooser.....	12
event script.....	225	Help.....	12
events		Log Out.....	12
viewing, querying, acknowledging.....	291	My Jobs.....	12
executing scripts.....	257	User Preferences.....	12
Execute Script on Device(s) dialog box.....	258	H	
exporting a		hardware inventory	
definition.....	201	viewing.....	75
exporting scripts.....	278	Help icon.....	12
F		help, accessing.....	6, 12
fabric		See also getting started assistants, using	
adding a node.....	409, 411	hiding table columns, inventory page, tabular	
connection status.....	413	view.....	32
CPU resource.....	413	I	
device connection IP address.....	413	icons	
disk space.....	414	Application Chooser.....	12
load history.....	424	help.....	12
management IP address.....	413	job status.....	347
memory resource.....	414	log out.....	12

my jobs.....	12
user preferences.....	12
image	
deploying a device.....	238
importing a	
definition.....	200
importing a script	
dialog box.....	248
overview.....	247
procedure.....	248
importing definitions	
overview.....	162
inventory page.....	14
actions drawer.....	33
EOL data.....	84
objects, tagging.....	495
overview.....	28
paging controls.....	34
right-mouse menu.....	33
search and filter field.....	33
sorting data in tabular view.....	32
table columns, hiding.....	32
tabular view.....	14, 31
tabular view, parts of.....	29
thumbnail view.....	14, 31
thumbnail view, parts of.....	29
zoom slider.....	32
ISSU.....	238
J	
job information pie chart.....	25
job status icons.....	347
jobs.....	347
canceling.....	352
management overview.....	341
types.....	341
viewing	
scheduled jobs.....	347
your jobs.....	345
viewing statistics	
by execution time.....	352
by state.....	351
by type.....	351
Junos OS release See devices categorized by	
Junos Space	
device discovery.....	40
user account, creating.....	381
Junos Space license, managing.....	447

Junos Space software	
base application.....	462
hot-pluggable applications.....	462
network application platform, upgrading.....	463
upgrade highlights.....	462
upgrade scenarios.....	462
upgrading , before you begin.....	463

L

license	
60-day trial.....	445
generating.....	445
Junos Space, managing.....	447
key file	
generating.....	445
uploading.....	446
license inventory	
device	
viewing.....	63
exporting.....	91
viewing.....	91
local authentication	
configuration workflow.....	481
local authentication mode.....	480
local password	
for remote authentication, clearing.....	390
Log Out icon.....	12
logging in to Junos Space with remote	
authentication configured.....	486
logging in, to Junos Space.....	3
See also logging out, from Junos Space	
logging out from Junos Space.....	12
logging out, from Junos Space.....	6
See also logging in, from Junos Space	
login behavior	
remote authentication.....	486
remote-local authentication.....	488
login credentials for manage devices	
changing.....	82

M

maintenance mode	
actions menu.....	403
administrator name.....	402
administrator password.....	402
administrator tasks.....	402
connecting to Junos Space appliance.....	404
lock time out.....	403
log in screen.....	402

overview.....	402
system locking.....	403
user administration.....	403
manage applications overview.....	451
Manage Applications workspace	
application, adding.....	458
application, uninstalling.....	467
application, upgrading.....	460
Platform, upgrading.....	463
Manage Scripts page	
fields description	226
management	
configuration file	
user privileges in.....	337
performance.....	284
management IP	
changing in same subnet.....	415
changing to different subnet.....	415
multinode	
changing in same subnet.....	415
managing applications.....	452
managing Junos Space license.....	447
managing template definitions.....	162
manuals	
comments on.....	xxix
maximum auto resync waiting time (secs)	
application setting.....	454
MD5 Validation Results	
Viewing	
Deleting.....	236
Modifying Device Image Details.....	244
modifying template definition.....	197
modifying users.....	387
My Jobs feature.....	345
My Jobs icon.....	12

N

Network Application Platform, overview.....	18
network settings	
configuration guidelines.....	415
configuring.....	415
node	
adding to fabric.....	409, 411
definition.....	405
deleting.....	421
threshold limit for devices.....	407

node functions	
application logic.....	407
database.....	407
load balancer.....	407
node lists for performance management	
viewing	287
nodes	
resyncing	288
searching for.....	288
notification	
status	
configuring OpenNMS.....	311
notifications	
configuring.....	317
destination paths, configuring.....	319
event notifications, configuring.....	317
path outages, configuring.....	320
viewing and searching for.....	297

O

object level access control.....	499
object tagging	
untagging.....	497
viewing.....	496
object, inventory	
applied tags, managing	492
filtering using tags.....	497
tag, creating	498
tags, managing.....	491
op script.....	225
OpenNMS	
configuring.....	305, 311
viewing charts.....	305
operations copying.....	264
operations creating.....	259
operations deleting.....	265
operations modifying.....	262
operations overview.....	229
operations running.....	263
operations viewing.....	279
operator's view	
defining.....	167
options	
configuration, finding.....	174
outages	
viewing and tracking.....	290
overall system condition gauge.....	23

- overview
 - definitions, importing.....162
 - importing definitions.....162
- P**
 - paging controls, inventory page.....34
 - parentheses, in syntax descriptions.....xxix
 - password, user, changing.....12
 - performance management
 - Admin, configuring OpenNMS.....305
 - notification status.....311
 - alarms, viewing and acknowledging.....294
 - assets, tracking and searching for.....289
 - event viewing, querying, acknowledging.....291
 - notifications, configuring.....317
 - notifications, viewing and searching for.....297
 - resyncing nodes.....288
 - searching for nodes.....288
 - thresholds, managing.....313
 - viewing and tracking outages.....290
 - viewing charts.....305
 - viewing node lists.....287
 - Permission Labels
 - assigning to users.....502
 - attaching to objects.....503
 - creating.....501
 - deleting.....501
 - managing.....499
 - removing from objects.....503
 - removing from users.....502
 - renaming.....501
 - physical interfaces
 - viewing.....78
 - Platform
 - active user history graph.....23
 - dashboard statistics, viewing.....23
 - fabric load history graph.....23
 - overall system health.....23
 - overview.....18
 - See also Platform dashboard overview
 - statistics page overview.....19
 - predefined role, managing.....393
 - modifying.....394
 - publishing template definition.....196
- R**
 - RADIUS authentication methods supported.....479
 - rebooting nodes.....420
 - recurring database backup.....433
 - remote authentication
 - configuration workflow.....482
 - configuration workflows.....481
 - configuring servers.....483
 - Junos Space login behavior.....486
 - local password, clearing.....390
 - method, selecting.....483
 - overview.....479
 - password, setting.....382
 - server settings, modifying.....486
 - server, creating.....484
 - remote authentication mode.....480
 - remote host
 - database backup.....434, 442
 - database restore.....439
 - remote-local authentication
 - configuration workflow.....482
 - remote-local authentication mode.....480
 - reports
 - node, database, statistics, domain, SNMP, KSC
 - overview.....286
 - restoring a database
 - overview.....432
 - restoring databases in maintenance mode.....440
 - Resynchronize with Network command.....62
 - resynchronizing See devices
 - right-mouse menu, inventory page.....33
 - role
 - predefined, managing.....393, 394
 - user-defined, deleting.....397
 - user-defined, managing.....393, 394, 395, 397
 - role-based administration.....371
 - authentication.....371
 - enforcement by workspace.....371
 - overview.....371
 - RBAC enforcement.....371
 - RBAC enforcement, limitations.....372
 - See also user administration
 - roles See user administration
 - predefined.....373
 - Rules in device template definitions
 - working with.....188
 - Rules, using
 - overview.....186
- S**
 - scheduled job statistics
 - viewing.....350

schema		states	
updating a DMI.....	508	template definition.....	215
schema management		statistics	
troubleshooting DMI	514	audit logs.....	361
schemas		dashboard, viewing.....	23
adding DMI.....	511, 513	devices.....	58
script details		jobs.....	351
Script Details dialog box.....	276	users.....	391
Script Details Dialog Box Controls		workspace, overview.....	26
Description.....	276	statistics page	
script modification.....	248	overview.....	19
Edit Script dialog box.....	249	status	
script types		notification	
modifying.....	249	configuring OpenNMS.....	311
script versions		super administrator.....	372
comparing.....	250	privileges.....	372
scripts		<i>See also</i> user administration	
overview.....	225	support, technical <i>See</i> technical support	
search and filter field, inventory page.....	33	switching applications.....	9
Secure Console		icon.....	12
connecting to devices.....	121	syntax conventions.....	xxviii
overview.....	121	system	
terminal control characters.....	126	connecting to appliance in maintenance	
user privileges.....	121	mode.....	404
Secure Copy (SCP) command		database restore.....	402
database backup.....	432	debugging.....	402
software upgrade		shutdown.....	402
in-service.....	238	system health statistics, viewing.....	23
software, Junos Space, upgrading.....	461, 462	system locking <i>See</i> maintenance mode	
sorting data, inventory page, tabular view.....	32	system status log file.....	469
SOS adapter		checking, customize.....	471
deleting.....	140	downloading.....	470
SOS software adapter		downloading using SCP.....	476
overview.....	133	downloading using USB device.....	475
SOS software adapter for managing non-DMI		files to download, customize.....	472
security devices		system status log file overview.....	469
installing.....	134		
specifying default values for configuration		T	
options.....	194	table columns, hiding in inventory page tabular	
specifying device-specific data in template		view.....	32
definitions.....	190	tabular view, inventory page.....	14, 31
SRX device clusters		tagging managed objects.....	495
configuring.....	126	tags	
SSH session		creating.....	495, 498
connecting to managed devices.....	122	deleting.....	495
connecting to unmanaged devices.....	123	inventory objects, filtering.....	497
error messages.....	123	managing.....	491, 492
overview.....	121	renaming.....	494
Staging a Device Image	234	sharing.....	493

- untagging.....497
 - viewing.....496
 - technical support
 - contacting JTAC.....xxx
 - template definition
 - cloning.....198
 - creating.....164
 - modifying.....197
 - naming and selecting the device family.....169
 - publishing.....196
 - unpublishing.....196
 - template definition states.....215
 - template definitions
 - deleting.....199
 - managing.....162
 - specifying device-specific data in.....190
 - workflow.....163
 - terminal control characters
 - for Secure Console.....126
 - thresholds
 - creating, modifying, and deleting.....313
 - thumbnail view, inventory page.....14, 31
 - Topology discovery
 - device targets, managing.....149
 - device targets, specifying.....48
 - discovering.....148
 - overview.....145
 - SNMP probes, managing.....151
 - SNMP probes, specifying.....49
 - troubleshoot zip file
 - contents470, 472
 - download from Junos Space Platform UI.....472
 - download in maintenance mode.....474
 - troubleshooting
 - device.....94
- U**
- uninstalling Junos Space application.....467
 - unpublishing template definition.....196
 - untagging inventory objects.....497
 - upgrade
 - in-service software238
 - upgrading Junos Space application.....460
 - upgrading Junos Space Platform.....463
 - upgrading Junos Space software.....461, 462
 - Uploading a Device Image233
 - user account
 - creating in Junos Space.....381
 - user administration.....371
 - default super administrator.....372
 - role assignment, understanding.....372
 - roles
 - definition.....372
 - predefined.....372, 373
 - task group.....373
 - viewing statistics.....391
 - viewing user account information.....386
 - See also* role-based administration
 - user interface
 - banner.....12
 - global action icons.....12
 - parts of.....12
 - User interface
 - navigating.....16
 - user interface, Junos Space, overview.....11
 - user password, changing.....12
 - User Preferences icon.....12
 - user privileges.....215
 - configuration file management.....337
 - user-defined role, creating.....395, 397
 - user-defined role, deleting.....397
 - user-defined role, managing.....393, 394
 - creating.....394
 - deleting.....394
 - overview.....394
 - users
 - disabling.....385
 - enabling.....385
- V**
- validation tab
 - filling in the.....181
 - view script details.....275
 - viewing device template definition statistics.....212
 - viewing device template inventory.....212
 - VIP interface
 - changing in same subnet.....415
 - changing to a different subnet.....415
 - multinode
 - changing in same subnet.....415
- W**
- workspace
 - Administration.....405
 - administrator access.....371
 - Audit Logs.....357
 - Devices.....57

DMI Schema Management.....	506
enforcement.....	371
Jobs.....	341
Users.....	371
workspace statistics.....	14
workspace statistics, overview.....	26
wwadapter	
installing.....	141
overview.....	140
 Z	
zoom slider, inventory page.....	32