

# Network Configuration Manager Online Help

VMware Smart Assurance 10.1.1

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2023 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

- 1 VMware Smart Assurance Network Configuration Manager Online User Guide 18**
- 2 Welcome to Network Configuration Manager 19**
  - Introducing Network Configuration Manager 19
  - Who Should use this Guide? 20
  - Logging into Network Configuration Manager 20
  - Setting RSA PINs 22
  - RSA Token Tools 23
  - RSA Token Usage 25
  - Logging Out 26
  - Disconnecting/Reconnecting 27
  - Inactivity Time out 27
  - Changing Your Password 27
  - Changing Token Pins 29
- 3 Introducing the User Interface 32**
  - The Dashboard 32
  - The Launch Window Overview 33
  - The Networks Navigation Tree 35
  - The Automation Library Navigation Tree 37
  - Using Contextual Launch 38
- 4 Accessing Help and Additional Documents 40**
  - Accessing the Online User Guide 40
  - Accessing Documents in the Reference Library 41
  - Using Keystroke Shortcuts 42
  - The Application icons 43
- 5 END USERS - Getting Started 45**
  - Getting Started - End User Overview 45
  - Getting Started - End Users Tasks 46
  - Working Within a Network 46
    - The Networks Navigation View 46
  - Working with Favorites 47
    - Favorites Overview 47
    - Editing Favorites Names 50
    - Deleting Favorites from the List 50

- Working with Devices (Devices View) 52
  - Options on the Device View Tool Bar 52
  - Devices Window Overview 54
  - Displaying Column Headings in the Devices View 57
  - Sorting Columns by Priority 59
  - Viewing the Device State Columns 59
  - Exporting the Devices View 60
  - Using Find in the Devices Window 60
  - Find Devices by Name 62
  - Find Devices by Config tab 62
  - Find Devices by Hardware 63
  - Accessing Editors in the Devices View 65
  - Scheduling a Device 65
  - Working with Virtual Devices 66
  - Using the Birds-Eye View 69
  - Device States 70
  - Clearing Device Flags 72
  - The Devices Legend 72
  - Filtering Devices 73
  - Deleting a Device 76
  - Using Right-Click Options 78
    - Right-Click Menu Options Overview 78
    - Compliance Audit 81
    - Enforce Policy 83
    - Cut-Through 84
    - Editor 85
    - Edit Device 86
    - Pull (Immediately) 87
    - Using Quick Commands 88
    - Using Saved Commands 89
    - Test Credentials 91
    - Updating OS Images 91
    - Resyncing Devices 97
    - Wizards 99
    - Navigations 99
    - Compare Configs 100
    - Compare (Run/Start) Out-of-Sync Files 102
    - Properties 105
    - Device Properties 106
    - The General Tab 119
    - The Configuration Tab 123

- Operational Units 132
- The Communications Tab 133
- The Baseline Tab 142
- The Site Tab 145
- The Comments Tab 148
- The Attachments Tab 149
- Working with Global Device Search 152
  - Global Device Search Overview 152
  - Using the IP Address Tab (within Global Device Search) 153
  - Global Search from the Name Tab 157
  - Global Search from the Configuration Tab 157
  - Global Search from the Hardware Tab 159
- Working with Sites 161
  - Sites Overview 162
  - How Sites and Views Work 165
  - Sites Best Practices 168
  - Sites Hierarchy and Logical Connections 168
  - Editing the Site Hierarchy 170
  - Removing a Site Hierarchy level 171
  - Permissions and Site Security 172
  - Sites Filters 172
  - Attributes 173
  - Creating the Site Hierarchy 173
  - The General Tab - Editing Site Properties 176
  - The Sites Comments Tab 178
  - The Sites Attachments Tab 178
  - Right-click Features 179
  - Data Fields in Sites 180
  - Right-click Features - Diagram View 181
  - Assigning Devices to Sites 181
  - Editing Device Associations to Sites 183
  - Symbolic Device Links in Sites 184
  - Sites - Legends 185
  - Sites Property Tabs 186
    - The General Tab - Editing Site Properties 186
    - The Sites Comments Tab 188
    - The Sites Attachments Tab 188
    - Adding an Attachment 189
    - Editing an Attachment 190
    - Deleting an Attachment 190
- Working with Views 191

- Views Overview 191
- Creating Views 193
- Editing Views 198
- Deleting Views 199
- Working within a Workspace 200
  - Workspaces Overview 200
  - Workspace Tool Bar Options 201
  - The Workspace Window 203
  - Creating Workspaces 206
  - Editing Workspaces Folder names 207
  - Deleting Workspaces 208
  - Workspace Properties - Right-Click Options 209
    - Workspaces Properties Overview 209
    - The General Tab 210
    - Adding (Managing) Network Devices 211
    - Adding Virtual Devices 213
    - Assigning User and Groups Permissions 216
    - Setting Workspace Permissions 219
    - The Comments Tab 220
    - The Attachments Tab 221
  - Workspace Properties - Tabs 224
    - Properties - Jobs 224
    - General 225
    - Configuration 226
    - Operational 228
    - Comments Tab 228
    - Attachments 229
- Multi-Configuration File Support 230
  - Multi-Configuration Overview 230
  - Pull/Push Activities 232
  - Supported Operations 233
  - Device Configuration State 234
    - Device Configuration State (and Revisioning) 234
    - Rollback / Restore Device Configuration State 237
    - Device State History 237
- Working with Editors 237
  - Editors Overview 237
  - Accessing Editors 240
  - Using Reference Variables 240
  - Additional Reference Variables 242
  - Using IP Address Ranges 244

- Inserting Template Variables 246
- Inserting Reference Variables 246
- Updating Devices 248
- Using Find and Replace in Editors 249
- Scheduling Jobs in Editors 250
- Saving in Editors 253
- Previewing Changes in Editors 255
- The Config Editor 256
  - The Config Editor Window 256
  - Creating a Config 260
  - Editing a Config 262
- The Configlet Editor 263
  - The Configlet Editor Window 263
  - Creating a Configlet 266
  - Editing Configlets 267
  - Updating Devices Affected by a Configlet 267
- The Interface Editor 269
  - The Interface Editor Window 269
  - Creating Interface Configlets 274
  - Editing Interfaces 276
  - Interface Editor - Updating Devices 277
- The Command Editor 279
  - The Command Editor Window 279
  - Creating a Command 283
  - Editing a Command 284
  - Updating Devices Affected by Commands 284
- Scheduling Jobs 286
  - Using the Scheduler 286
  - Scheduling a Run Time 287
  - Using the Schedule Tab 289
  - Reviewing Job Tasks 292
  - Using the Task Tab 294
  - Reviewing Job/Status Summary 297
  - Using the Notification Tab to Send an Email 297
  - Viewing Data Fields 299
- Working with the Schedule Manager 299
  - Schedule Manager Overview 299
  - Recurring Series 303
  - Viewing a Scheduled Job Summary 304
  - General Tab 304
  - Task Tab 305

- The History Tab 307
- Additional Task 307
- Printing a copy of a Job 308
- Exporting a Job (copy) 308
- Filtering the Job Listing 309
- Quick Filter 311
- Executing a Job 312
- Canceling a job 312
- Copying a Job 312
- Editing a Job 314
- Viewing and/or Updating Data Fields 315
- Deleting a Job 315
- Changing the Job Status 315
- Jobs in the Hold Status 317
- Schedule Manager (Override) Update Credentials 317
- Job Details 317
- Reviewing Job/Status Summary 318
- Refreshing a Job List 318
- Working with the Data Field Manager 318
  - Introducing the Data Field Manager 318
  - Working in the Data Field Manager 319
  - Adding a Data Field 320
  - Editing a Data Field 322
  - Deleting a Data Field 323

## **6 SYSTEM ADMINISTRATORS - Getting Started 325**

- Getting Started - System Administrator Tasks 325
- Getting Started - System Administration Overview 326
- System Administration Best Practices 329
- System Administration Tasks and Procedures 329
- System Administration User Rights 330
- Working with Global Settings 331
  - Global Settings Overview 331
  - Global - Access 333
    - Access Overview 333
    - Global - Device Servers 333
    - Global - Devices 339
    - Global - File Servers 344
    - Global - Out-of-Band Servers 346
    - Global - NCM RSA Token Service 350
  - Global - Credentials Manager 354



Global - Credentials Manager Overview	354
Credentials Best Practices	355
Credential Settings Overview	356
Working with Credentials	358
Global Credential Settings	359
Privilege Password for Multi-Level Mode	362
Credential Types	364
Using Credentials Configuration	367
Unique Credentials	372
Global Shared Credentials Options	374
Adding Global Shared Credentials	375
Viewing Associations	384
Roll Credentials	385
Rolling Credentials - Privilege Passwords	387
Editing global Shared Credentials	389
Removing Shared Credentials	391
Prompt User	392
Global - Device Options	393
Device Naming Overview	393
Device Naming Update	394
Device Naming Scheme	396
Device State Options	397
Global - User Management	398
User Management Overview	399
Working with System Users or Groups	400
Working with Permissions	408
Working with Authentication Servers	424
Global - Maintenance Windows	433
Global - Adding a Maintenance Window	433
Global - Editing a Maintenance Window	435
Networks- Removing a Maintenance Window	435
Global - Device Classes	436
Device Class Management Overview	436
Device Class Management Best Practices	438
Specifying Device Class Protocol	438
Working with Diagnostics	439
Managing the Supported Devices Class List	441
Generic Device Selection - Device Classes	444
Using the Diagnostic Tool	446
Diagnostic Tool Overview	446
Setting Up (Creating) Diagnostic Commands	447

- Cutting, Pasting, Copying and Inserting Diagnostic Commands 449
- Global - RSA Token Viewer 451
  - RSA Tokens Overview 451
  - Global - Global RSA Token Viewer 451
- Working with Network Settings 452
  - Network Settings Overview 452
  - Creating Networks 454
  - Setting Network Permissions 455
  - Editing Networks 458
  - Removing Networks 459
  - Managing Network Access Permissions 460
  - Setting Workspace Permissions for Each User and Group 463
  - Network - Access 464
    - Network - Out-of-Band Servers 464
    - Network - Device Servers 470
  - Networks - Credentials Manager 472
    - Credential Manager Overview 472
    - Credentials Best Practices 474
    - Setting Network Level Credentials 474
    - Viewing Network Credentials Associations 475
    - Rolling Credentials 476
    - Adding Network Shared Credentials 478
    - Copying Network Shared Credentials 484
    - Editing Network Credentials 486
    - Removing Network Credentials 487
    - Using Network Credentials Configuration 488
    - Auto Discovery 493
  - Networks - Maintenance Windows 520
  - Networks - Device Classes 525
  - Networks - Devices 529
  - Networks - Address Pools 533
  - Networks - NAT Configuration 545
  - Network - RSA Token Viewer 549
- Working with Networks 550
  - Networks Overview 550
  - Working with Networks 551
  - Creating a New Network 553
  - Update Data Fields 554
  - About Network Properties 555
  - The General Tab 556
  - The Baseline Tab 557

- The Comments Tab 560
- The Attachments Tab 561
- Adding an Attachment 562
- Deleting an Attachment 563
- Scheduling Network Level Config and Hardware Spec Pull Jobs 564
- Single Device Auto Discovery 566
- Scheduling Run Times 569
- Sending Email Notifications 571
- Working with Devices (Devices View) 572
  - Devices Window Overview 572
  - Options on the Device View Tool Bar 574
  - Displaying Column Headings in the Devices View 577
  - Printing the Devices View 578
  - Filtering Devices 579
  - Exporting the Devices View 582
  - Using Find in the Devices Window 583
  - Accessing Editors in the Devices View 584
  - Device States 584
  - Clearing Device Flags 586
  - Working with Virtual Devices 587
  - The Devices Legend 589
  - Deleting a Device 589
  - Using the Birds-Eye View 591
  - Using Right-Click Options 592
    - Right-Click Menu Options Overview 592
    - Compliance Audit 595
    - Enforce Policy 597
    - Cut-Through 598
    - Editor 600
    - Pull (Immediately) 601
    - Using Quick Commands 602
    - Using Saved Commands 604
    - Updating OS Images 605
    - Resyncing Devices 611
    - Comparing Run/Start in Devices 613
    - Wizards 613
  - Device Properties 614
    - Device Properties Tabs 614
    - The History Tab 616
    - The Audit Trails Tab 625
    - The Job Tab 626

- The General Tab 627
  - The General Tab Overview 627
  - Resync Device Configurations 630
- The Configuration Tab 631
  - Configuration Tab Overview 631
  - Config Files 632
  - Hardware 638
  - The Interfaces Tab 638
  - Other 640
- Operational Units 640
  - Operational Units Tab Overview 641
- The Communications Tab 641
  - Communication Tab Overview 641
  - Editing In-Band Communications 642
  - Managing Device Communications 644
  - Managing and Viewing Privilege Password Levels 645
  - Updating Credentials 646
- The Baseline Tab 650
  - Baseline Tab Overview 650
  - Adding Baseline Revision Comments 651
  - Rolling back to Baseline 651
  - Setting the Current Revision to Baseline 652
  - Comparing Device Revision Configs 652
- The Site Tab 653
  - Site Tab Overview 653
  - Adding Site Information 654
- The Comments Tab 656
  - Comments Tab Overview 656
- The Attachments Tab 657
  - Attachments Tab Overview 657
  - Editing an Attachment 658
  - Deleting an Attachment 658
- Working with Sites 659
  - Sites Overview 660
  - How Sites and Views Work 663
  - Sites Best Practices 666
  - Sites Hierarchy and Logical Connections 666
  - Editing the Site Hierarchy 668
  - Removing a Site Hierarchy level 669
  - Permissions and Site Security 670
  - Sites Filters 670

- Attributes 671
- Creating the Site Hierarchy 671
- The General Tab - Editing Site Properties 674
- Right-click Features 676
- Data Fields in Sites 677
- Right-click Features - Diagram View 678
- Assigning Devices to Sites 678
- Editing Device Associations to Sites 680
- Symbolic Device Links in Sites 681
- Sites - Legends 682
- Sites Property Tabs 683
  - The General Tab - Editing Site Properties 683
  - The Sites Comments Tab 685
  - The Sites Attachments Tab 685
    - Adding an Attachment 686
    - Editing an Attachment 687
    - Deleting an Attachment 687
- Working with Views 688
  - Views Overview 688
  - Creating Views 690
  - Editing Views 695
  - Deleting Views 696
- Working with Tools 697
  - Network Configuration Manager Tools Overview 697
- Working with the Schedule Manager 698
  - Schedule Manager Overview 698
  - Recurring Series 702
  - Viewing a Scheduled Job Summary 703
  - General Tab 703
  - Task Tab 704
  - Additional Task 706
  - Printing a copy of a Job 707
  - Exporting a Job (copy) 707
  - Filtering the Job Listing 708
  - Quick Filter 710
  - Executing a Job 711
  - Canceling a job 711
  - Copying a Job 711
  - Editing a Job 713
  - Deleting a Job 714
  - Changing the Job Status 714

- Jobs in the Hold Status 715
- Schedule Manager (Override) Update Credentials 715
- Job Details 716
- Reviewing Job/Status Summary 716
- Refreshing a Job List 717
- Displaying Columns in the Schedule Manager 717
- Scheduling Jobs 717
  - Using the Scheduler 717
  - Scheduling a Run Time 718
  - Using the Schedule Tab 721
  - Reviewing Job Tasks 724
  - Using the Task Tab 726
  - Reviewing Job/Status Summary 729
  - Using the Notification Tab to Send an Email 729
- Working with the Event Manager 731
  - Event Manager Overview 731
  - All Events Log 733
  - System Events Log 735
  - Security Events Log 737
  - Device Events Log 739
  - Printing Event Logs 741
  - Exporting Event Logs 741
  - Filtering the Event Manager Data 742
- Using the Command Line Interface (Bulk Import) 745
  - Using the Command Line Interface 745
  - Setting the Number of Devices 749
  - Importing Credentials 750
  - Importing Users 753
  - Importing Groups 754
  - Importing Sites 755
  - Exporting Credentials 757
  - Auto Discovery 758
  - Importing Devices 759
  - Using the Extract Config script 763
- Working with the DNS Wizard 764
  - Wizard Overview 764
  - The DNS Wizard Overview 765
- RSA 766
  - About RSA 766

## **7 NETWORK ADMINISTRATORS - Getting Started 768**

- Getting Started - Network Administrator Tasks 768
- Working with Networks 769
  - Networks Overview 769
  - Working with Networks 770
  - Creating a New Network 772
  - Update Data Fields 773
  - Network Right-Click Options 774
  - About Network Properties 774
  - The General Tab 776
  - The Baseline Tab 777
  - The Comments Tab 780
  - The Attachments Tab 781
  - Adding an Attachment 781
  - Editing an Attachment 782
  - Deleting an Attachment 783
  - Scheduling Network Level Config and Hardware Spec Pull Jobs 784
  - Single Device Auto Discovery 786
  - Scheduling Run Times 789
  - Sending Email Notifications 791
- Working with Network Settings 792
  - Network Settings Overview 792
  - Creating Networks 794
  - Setting Network Permissions 795
  - Editing Networks 798
  - Removing Networks 799
  - Managing Network Access Permissions 800
  - Setting Workspace Permissions for Each User and Group 803
  - Network - Access 804
    - Network - Out-of-Band Servers 804
    - Network - Device Servers 810
  - Networks - Credentials Manager 812
    - Credential Manager Overview 812
    - Credentials Best Practices 814
    - Setting Network Level Credentials 814
    - Viewing Network Credentials Associations 815
    - Rolling Credentials 816
    - Adding Network Shared Credentials 818
    - Copying Network Shared Credentials 824
    - Editing Network Credentials 826
    - Removing Network Credentials 827
    - Using Network Credentials Configuration 828

- Auto Discovery Manager 833
- Networks - Maintenance Windows - Done 860
- Networks - Device Classes 865
- Networks - Devices 869
- Networks - Address Pools 873
- Networks - NAT Configuration 885
- Working with Change Audit 889
  - Working with Change Audit 889
  - Search Results - Save 889
  - Search Results - Compare 891
- Automation Library 893
  - Working in the Automation Library 893
  - Automation Library - Tool bar 895
  - Using Search in Library Manager 896
  - Attributed Model 898
    - Introducing the Attributed Model (AM) 898
    - Introducing the Data Model 898
    - Object Types 899
    - Model Object Types 903
    - Metadata Information 910
  - Library Manager - System 913
    - Working with System in the Automation Library 913
    - New Option 914
    - Import Option 917
    - Refresh Option 919
  - Library Manager - Samples 919
    - Introducing Test Samples 919
    - Working with Network Configuration Manager Samples 931
    - Copying Samples 933
    - Customizing Sample Tests 934
    - Right-Click Samples Options 934
    - Working with a RegEx Compliance Test 935
    - Working with a Standard 961
    - Working with a Policy 965
    - Working with an Attributed Test 989
    - Working with Queries 996
    - Working with Templates 1010
    - Working with Saved Commands 1024
    - Working with a Data File 1035
    - Working with Compliance Audit 1039
  - Working with Template Merging 1041



Template Merging	1041
Working with OS Image Inventory Manager	1045
OS Image Inventory Manager Overview	1045
Adding OS (Image) Inventory	1046
Copying OS (Image) Inventory	1049
Editing OS (Image) Inventory	1051
Printing OS (Image) Inventory	1052
Deleting OS Image Inventory from the List	1053
Exporting Inventory Information from the OS Inventory Listing	1054
Filtering the OS Inventory List	1055
Displaying Columns in the OS Image Inventory	1056
Managing Credentials	1058
Credential Manager Overview	1058
Credentials Best Practices	1059
Setting Network Level Credentials	1060
Viewing Network Credentials Associations	1061
Rolling Credentials	1062
Adding Network Shared Credentials	1063
Copying Network Shared Credentials	1070
Editing Network Credentials	1072
Remove Network Credentials	1073
Using Network Credentials Configuration	1074
Working with Update Credentials	1079
Update Credentials Overview	1079

## **8** Glossary - Terms and Definitions 1081

# VMware Smart Assurance Network Configuration Manager Online User Guide

1

## Quick Access Links:

To access the information, click each links.

[Accessing Documents in the Reference Library](#) - takes you to the Reference Library.

[Getting Started - System Administration Overview](#) - takes you quickly to System Admin tasks.

[Getting Started - Network Administrator Tasks](#) - links you to Network Admin tasks.

[Getting Started - End User Overview](#) - gets the new end user started.

[Support](#) - outlines how to contact Customer Support.

[Copyright Information](#) - contains the copyright information.

# Welcome to Network Configuration Manager

# 2

This chapter includes the following topics:

- Introducing Network Configuration Manager
- Who Should use this Guide?
- Logging into Network Configuration Manager
- Setting RSA PINs
- RSA Token Tools
- RSA Token Usage
- Logging Out
- Disconnecting/Reconnecting
- Inactivity Time out
- Changing Your Password
- Changing Token Pins

## Introducing Network Configuration Manager

### What is Network Configuration Manager?

- An automated compliance, change and configuration management solution that delivers industry-recognized best practices
- A collaborative network infrastructure design, controlled change processes, network device, and service configuration transparency, and compliance with corporate and regulatory requirements—to enable you to ensure the security, availability, and operational efficiency of your network
- An automated support for all facets of the network infrastructure lifecycle, seamlessly integrating critical design, change, and compliance management requirements

## With Network Configuration Manager you can:

### Design

- Design new virtual networks based on existing designs with Network Configuration Manager's exclusive Virtual Design Workspace
- Collaborate securely in real time -- thanks to complete role-based security
- Employ intelligent automation to create large-scale designs--error free, in a fraction of the time
- Audit designs before deployment for compliance with corporate policy and government regulatory standards

### Change

- Realize significant improvements in the availability and constancy of services
- Use "Golden Configs" to create templates for new device deployments
- Virtually eliminate standard change errors
- Address standard and non-standard changes, and leverage all team members to complete routine and complex tasks with ITIL-compliant change processes and workflow approvals
- Adapt the configuration tool to your processes with integrations to popular workflow, trouble ticketing, and help desk solutions

### Ensure Compliance

- Design, enforce and report on adherence to complex policies
- Enforce policies over the entire domain--or just one network, site or subnet
- Demonstrate on-demand compliance, and its change/control process
- Report on historical compliance of the managed infrastructures using the configurations and policies in place on the date selected

## Who Should use this Guide?

This guide is created to address the tasks and procedures for the following users:

- [Getting Started - End Users Tasks](#)
- [Getting Started - System Administrator Tasks](#)
- [Getting Started - Network Administrator Tasks](#)

Click the appropriate link to begin working with Network Configuration Manager.

## Logging into Network Configuration Manager

Prior to logging into Network Configuration Manager, ensure that you are an authorized application user. An authorized user must be listed on the TACACS+ Security Server, or be a registered user in the application's Native Registry. Each time you log into Network Configuration Manager your User ID and Password are authenticated and validated against the TACACS+ Server, or the Network Configuration Manager Native Registry. Network Configuration Manager maintains an audit of all logins, as well as an authorized user list.

Access to secured networks is filtered by network-level authentication security.

To log into the application,

- 1 Open a web browser.
- 2 In the browser address field, enter the **application server URL**. Check with your System Administrator for the exact address.

For example: **http://ServerNameorIpAddress/XXXXXXXX/**

- 3 If presented with a login selection screen, click the **Launch VMware Smart Assurance Network Configuration Manager** link.
- 4 At the login screen, enter a valid **User ID** and **Password**.

---

**Note** If enabled, you can have the system remember your login using a check box that is visible on the login screen. Check with your System Administrator to verify that this feature is enabled. To have the application remember your login password, click within the **Remember Login** check box (if it is visible on the login window). This signifies that the **next time** you launch the Network Configuration Manager Application, your User ID and Password is remembered and will be retrieved by the system, and you will be automatically logged on.

---

- 5 Click **Ok**.

Once Network Configuration Manager opens, you can close the open browser window. To log off or exit the application correctly, see [Logging Out](#).

---

**Important** When the application is not active for a specified time, you will have to login again using your password. A message displays, and you must enter your password to keep working within the application.

---

**Note:** The Network Configuration Manager user interface has been enhanced by including a link to launch the EMC M&R user interface. This enhancement is available in the NCM Welcome screen and the Dashboard screen. During installation, if the EMC M&R IP address is provided, then the EMC M&R URL in the NCM user interface and welcome/splash screen is updated automatically.

## RSA Tokens

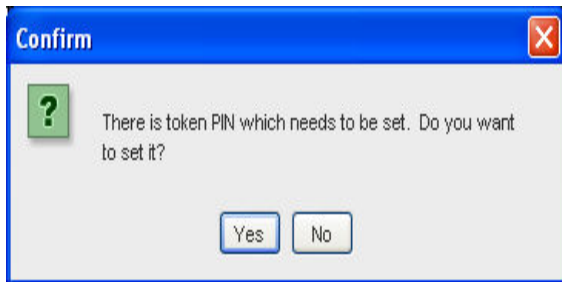
The first time you login, if your System Administrator has set up Network Configuration Manager to use **RSA Token Credentials**, and you have been assigned new RSA Tokens, you are prompted to set your RSA Token PINs. See [Setting RSA PINs](#) for the steps needed to complete this task.

## Setting RSA PINs

If your System Administrator has set up Network Configuration Manager to use RSA Token Credentials, you are prompted to set your RSA Token PINs when you login for the first time (after you are assigned new RSA Tokens).

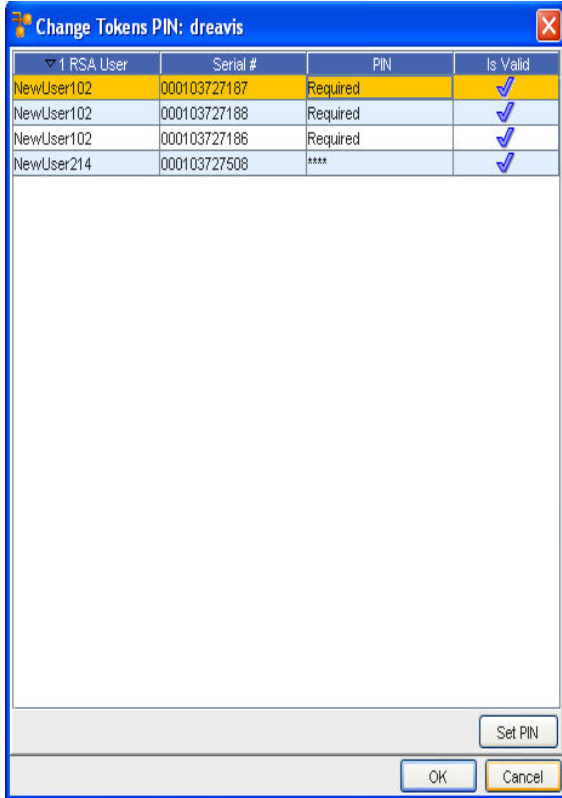
- 1 When prompted to set your RSA Token PINs, click Yes.

Figure 2-1. Confirm token pin dialog box



- 2 From the list of RSA tokens, select a RSA token. RSA tokens that have not had the PIN set, show as Required under the PIN column.
- 3 At the bottom of the Manage RSA Tokens pane, select Set PIN. The Set PIN window (for the user you selected) now opens.

Figure 2-2. Change token pin dialog box



- 4 At the Set PIN screen, enter a valid PIN in the New PIN box.
- 5 Enter the PIN again in the Confirm PIN box.
- 6 Click Ok.

## RSA Token Tools

### RSA Token Tools

There are multiple RSA Token Tools available in Network Configuration Manager for diagnostics, testing, and bulk tasks.

### RSA Authentication Manager Tools

RSA Authentication Manager Activity Monitors such as the real time Authentication Activity Monitor web page. This can be used to monitor authentication attempts to the RSA Authentication Manager.

## Network Configuration Manager RSA Token Service Tool

The Network Configuration Manager RSA Token Service Tool is available in the [Product\_Home]/tools directory on the Network Configuration Manager RSA Token Server to perform various tasks. To run the Network Configuration Manager RSA Token Service Tool, run the NCMRSATokenService.exe application installed on the token server.

### Usage:

```
NCMRSATokenService [-i | -p | -u | -h | -deleteAllKnownTokens | -importTokens directoryPath | -deleteToken]
```

**i:** install as a windows service

**p:** run as a windows process

**u:** uninstall as a windows service

**h:** this help

**importTokens <dir>:** importTokens from dir

**deleteAllKnownTokens:** delete all known tokens

**deleteToken <tokenSerialNumber>:** delete specific token

Network Configuration Manager RSA Token Server Instrumentation Data Web Page

The Network Configuration Manager RSA Token Server Instrumentation Data Web Page provides information on current usage and available statistics for soft tokens on the Network Configuration Manager RSA Token Server.

To access the Network Configuration Manager RSA Token Server Instrumentation Data Web Page, navigate to one the following addresses.

- If your Network Configuration Manager RSA Token Server is setup using http, use the following address: `http://<VCTokenServerIPAddress>:18001`, where <VCTokenServerIPAddress> is the IP Address of your Network Configuration Manager RSA Token Server.
- If your Network Configuration Manager RSA Token Server is setup using https, use the following address: `https://<VCTokenServerIPAddress>:18001`, where <VCTokenServerIPAddress> is the IP Address of your Network Configuration Manager RSA Token Server.

## Network Configuration Manager RSA Token Service Client Tool

The Network Configuration Manager RSA Token Service Client Tool is available in the [Product\_Home]/tools directory on Network Configuration Manager Device Server. This tool communicates with the token server to get information.

### Usage:

```
<NCMRSATokenTester> [-getpasscode <tokenSerialNumber> [pin]]-getinstrdata[-performancetestgetcode <numThreads> <callsPerthread> <rsatokenfile>]
```



- **getinstrdata:** Returns instrumentation data as a token server web page in plain text format on the command line.
- **performancetestgetcode:** Used to test performance of token code generation on multiple threads. Token serial numbers have to be provided in XML formatted token file.
- **getpasscode:** Returns the pass-code and token code of the supplied serial number. A pin is optional based on the token setup.

## RSA Token Usage

### RSA Token Restrictions

- The RSA API limits the number of tokens supported on the Network Configuration Manager RSA Token Server to a maximum of 1000.
- One token can be assigned to only one Network Configuration Manager credential or Network Configuration Manager user.

### Network Configuration Manager RSA Specific Errors

The following errors can occur during communication with token server.

- No tokens known by tokenserver
- Unknown tokens supplied
- Pin supplied for pinless token
- Pinfule token has no pin
- No tokens supplied
- RSA API error
- Unknown rsa token server error
- SSL error
- Error in calling token server endpoint
- Token server returned NULL selected token
- Unknown Exception thrown

### Network Configuration Manager Log and Result Messages

Log files with recorded errors or result messages, are available on the Token Server and Device Server. These log files can be used to analyze token code usage and generation issues.

RSA related failures are also recorded in the Network Configuration Manager scheduler results.

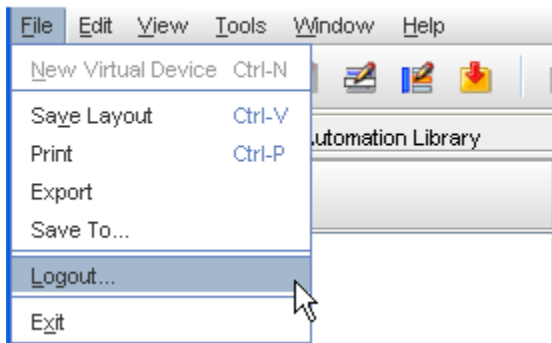
## Logging Out

There are two options for exiting Network Configuration Manager:

- **Logout** - Allows you to exit the application as the registered user, and re-opens the Login window making it ready for the next user to login.
- **Exit** - Allows you to completely exit the application.

To Log out as the registered user,

- 1 You can log out of the application at any time by selecting **File from the menu bar, then selecting Logout** . The Confirm window asking "Are you sure you want to logout of VMware Smart Assurance Network Configuration Manager?" opens.



- 2 At the Confirmation message, click **Yes**.

---

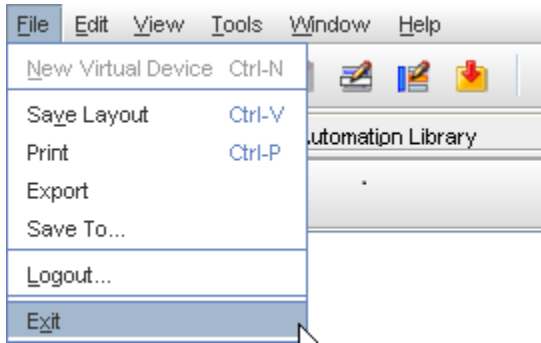
**Important** If you have made modifications to a Network, when you select Logout, the **Save View Properties** window opens, and allows you to select any views you want to save in the application. Click within the **check box** of any view displayed, and then click **Ok** to save that view. When presented with a number of check boxes (and views to save) you can click the **Select All** button to quickly save all views, then click **Ok**. To deselect any previously selected views, click the **Deselect All** button, make your new selections, and then click **Ok**.

---

You have now logged out of the application as a registered user. The login screen is active and ready for the next registered user to login to the application.

To Exit the application,

- 1 You can exit the application at any time by first selecting **File** from the menu bar, and then selecting **Exit**.



- 2 The Confirm window asking, "Are you sure you want to exit VMware Smart Assurance Network Configuration Manager?" opens. Click **Yes**.

You have now exited completely from the application.

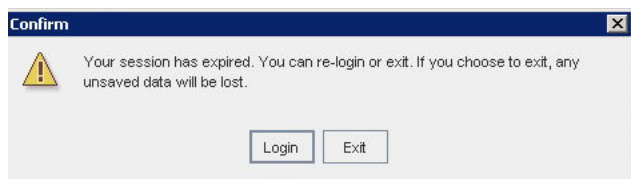
## Disconnecting/Reconnecting

When working within the Network Configuration Manager user interface, you can temporarily disconnect (undoc) your laptop, and then reconnect (doc) your laptop at any given time.

You can then continue working with the Network Configuration Manager user interface where you left off, before you disconnected (or undocked).

## Inactivity Time out

When your session of Network Configuration Manager has been inactive for a time, you now have two options to reactivate the session.



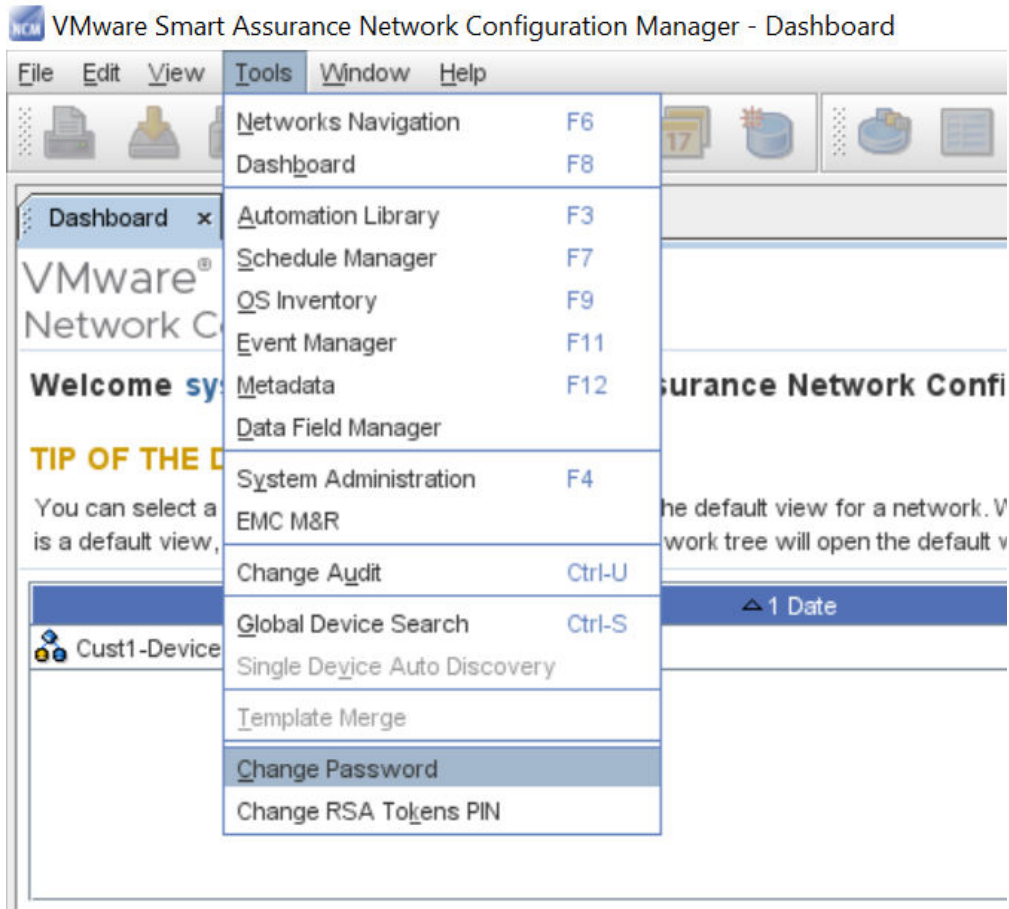
- A Confirm message displays offering you the option of logging in again, without leaving the last screen you were viewing, and continuing your tasks (clicking **Login**)
- To logout completely from the session and the application (clicking **Exit**)

## Changing Your Password

You can change your password anytime you are using the application.

**Important** Only passwords validated by the Native Registry can be changed using the following procedure. TACACS+ user passwords must be changed on the TACACS+ server, and RADIUS and LDAP user passwords must be changed on their respective servers.

- 1 On the menu bar, select **Tools**, and then select **Change Password**.



**Note** You can also select **Change Password** from the Launch Window's **Quick Access Links**.

The Change Password window opens.



- 2 In the Current Password field, enter the **password** that you are currently using to login.
- 3 In the New Password field, enter the **new password** you will use the next time you login. A password must consist of an alphanumeric combination.
- 4 In the Confirm Password Field, re-enter the **password** you entered in the New Password field.
- 5 Click **OK**. The Change Password window closes.

If the passwords in the New Password and Confirm Password fields do not match, you receive an error message indicating that your passwords do not match. In this case, repeat **steps 3 through 5**. Once your password is accepted, it is not necessary to logout of the application and log back in using the new password. The next time you logout or exit the application, your new password is active and must be used again for logging back in.

---

**Important** For added security it is recommended that you change your password periodically . For security, do not share your password with other users. If you feel your password has been compromised, **change your password immediately**.

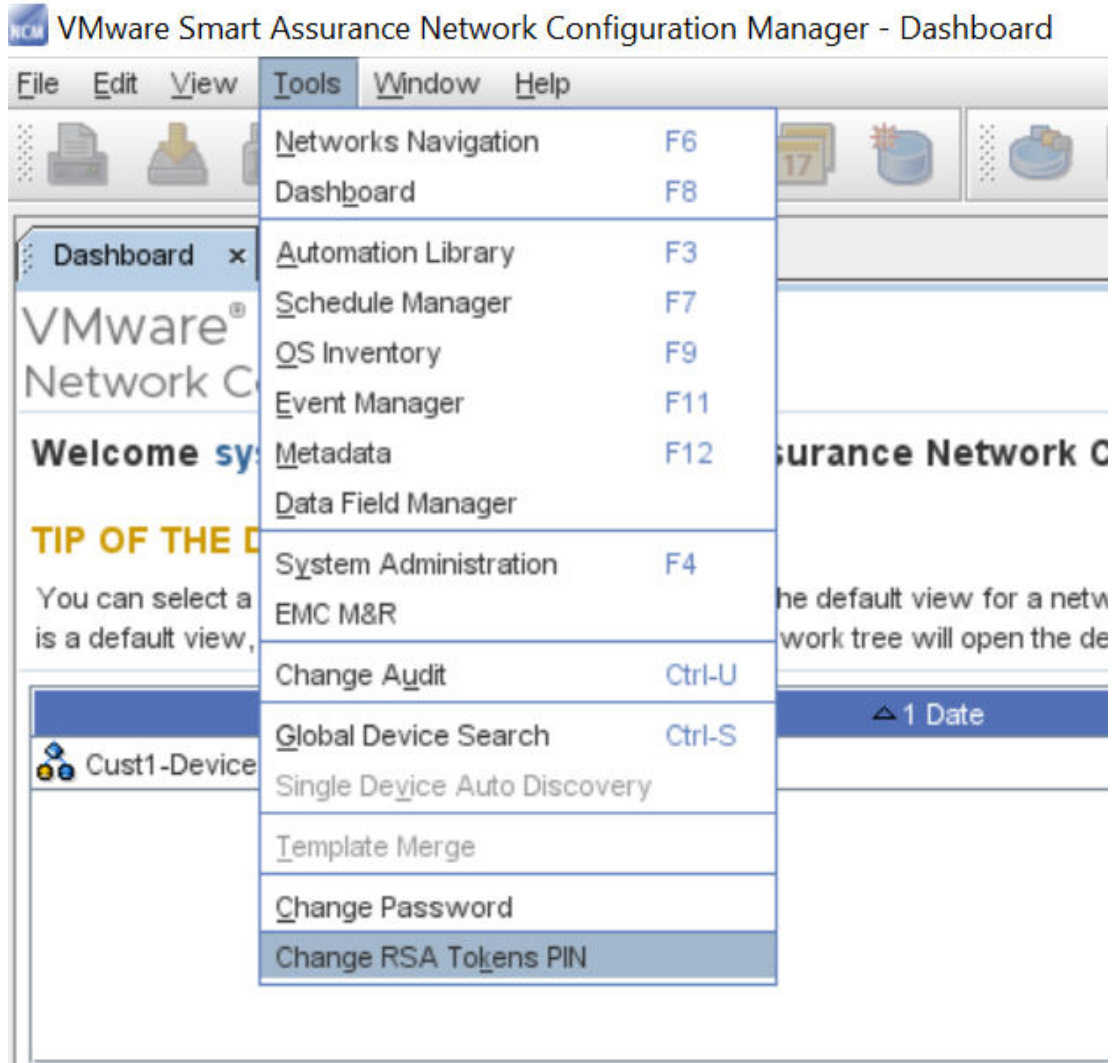
---

See: [Changing Token Pins](#)

## Changing Token Pins

If your System Administrator has setup Network Configuration Manager to use RSA Token Credentials, you will be prompted to set your RSA Token PINs when you login for the first time after you are assigned new RSA Tokens.

- 1 To open the Change Token PIN window from the navigation bar, select **Tools -> Change RSA Tokens PIN**.
- 2 From the list of RSA tokens, select an **RSA token** . RSA tokens that have not had the PIN set, show as Required under the PIN column.
- 3 At the bottom of the Manage RSA Tokens pane, select **Set PIN** . The Set PIN window (for the user you selected) now opens. Note: If already set, the Update PIN window opens.
- 4 At the Set or Update PIN window, enter a valid **PIN** in the New PIN box.
- 5 Enter the **PIN** again in the Confirm PIN box.
- 6 Click **Ok**.



The screenshot shows a window titled "Manage RSA Tokens for: dreavis" with a close button (X) in the top right corner. Inside the window is a table with the following data:

1 RSA User	Serial #	PIN	Is Valid
NewUser102	000103727187	Required	✓
NewUser102	000103727188	Required	✓
NewUser102	000103727186	Required	✓
NewUser214	000103727508	****	✓

Below the table, there is a dialog box titled "Update PIN" with a close button (X) in the top right corner. The dialog box contains two text input fields: "New PIN:" and "Confirm PIN:", both containing seven asterisks (\*\*\*\*\*). At the bottom of the dialog box are "OK" and "Cancel" buttons. In the main window, there is an "Update PIN" button at the bottom right and "OK" and "Cancel" buttons at the very bottom.

# Introducing the User Interface

# 3

This chapter includes the following topics:

- The Dashboard
- The Launch Window Overview
- The Networks Navigation Tree
- The Automation Library Navigation Tree
- Using Contextual Launch

## The Dashboard

When you first login to Network Configuration Manager, select the **Dashboard** feature (if it is not already displayed).

- 1 Click **Tools**
- 2 Select **Dashboard** from the menu options.



Tools	Window	Help
Networks Navigation		F6
<b>Dashboard</b>		<b>F8</b>
Automation Library		F3
Schedule Manager		F7
QS Inventory		F9
Event Manager		F11
Data Field Manager		
Metadata		F12
System Administration		F4
EMC M&R		
Change Audit		Ctrl-U
Global Device Search		Ctrl-S
Single Device Auto Discovery		
Template Merge		
Change Password		
Change RSA Tokens PIN		



From the Dashboard, you can:

- View device changes that have occurred over the past 24-hours, using **Change Audit**
- Launch **EMC M&R**
- Work with various **Quick links** to go to features and functions
- Select from **Your recently opened Views** of the devices

Dashboard x

VMware® Smart Assurance™  
Network Configuration Manager

vmware  
Smart Assurance™

Welcome **sysadmin** to VMware Smart Assurance Network Configuration Manager

**TIP OF THE DAY**  
You can select a specific view (or all "Devices") to act as the default view for a network. When there is a default view, double-click the Network name in the Network tree will open the default view.

Name	Date
Cust1-Devices	21/10/2019

**EMC M&R**  
EMC M&R

**Quick Access Links**  
Schedule Manager  
Change Audit  
Change Password

**Changes within the past 24 hours - ( No Change )**

Device Name	File Name	Revision	Type	Network	Modified	User
-------------	-----------	----------	------	---------	----------	------

**VMware Smart Assurance Network Configuration Manager is licensed to**

Company: emc  
Department / Division: dev  
Devices: 100,000 licensed  
(3 currently being managed)  
Serial Number: 02052016  
Support: <https://www.vmware.com/support.html>

To close and then reopen the Dashboard at a later time, select **Tools -> Dashboard**.

**Note:** The Network Configuration Manager user interface has been enhanced by including a link to launch the EMC M&R user interface. This enhancement is available in the NCM Welcome screen, the Dashboard screen, and also from the "Tools" menu. During installation, if the EMC M&R IP address is provided, then the EMC M&R URL in the NCM user interface and Welcome/splash screen is updated automatically.

## The Launch Window Overview

The Launch window is the primary window of Network Configuration Manager. This window remains open until you select to close it.

You can immediately begin working with the features and functions. You should first begin by opening the **Dashboard**. (This may already been displayed when you login.)

- 1 Select **Tools**, then select **Dashboard**.

Tools	Window	Help
Networks Navigation	F6	
Dashboard	F8	
Automation Library	F3	
Schedule Manager	F7	
QS Inventory	F9	
Event Manager	F11	
Data Field Manager		
Metadata	F12	
System Administration	F4	
EMC M&R		
Change Audit	Ctrl-U	
Global Device Search	Ctrl-S	
Single Device Auto Discovery		
Template Merge		
Change Password		
Change RSA Tokens PIN		

**Note** You can move the Dashboard anywhere, by selecting to undock the window, or minimize it to work with it later. You can still have all your tasks and windows open in Network Configuration Manager, and have the Dashboard open and ready to use at the same time. The Dashboard stays open until you decide to close it.

- 2 Become familiar with the Dashboard, and its various sections. The Changes section is a new feature that gives you a report on the changes that have occurred to any devices within the last 24 hours.
- 3 For more information, go to [The Dashboard](#)

VMware® Smart Assurance™  
Network Configuration Manager

Welcome **sysadmin** to VMware Smart Assurance Network Configuration Manager

**TIP OF THE DAY**  
You can select a specific view (or all "Devices" to act as the default view for a network. When there is a default view, double-click the Network name in the Network tree will open the default view.

Name	Date
Cust1-Devices	21/10/2019

**EMC M&R**

- EMC M&R

**Quick Access Links**

- Schedule Manager
- Change Audit
- Change Password

**Changes within the past 24 hours - (No Change)**

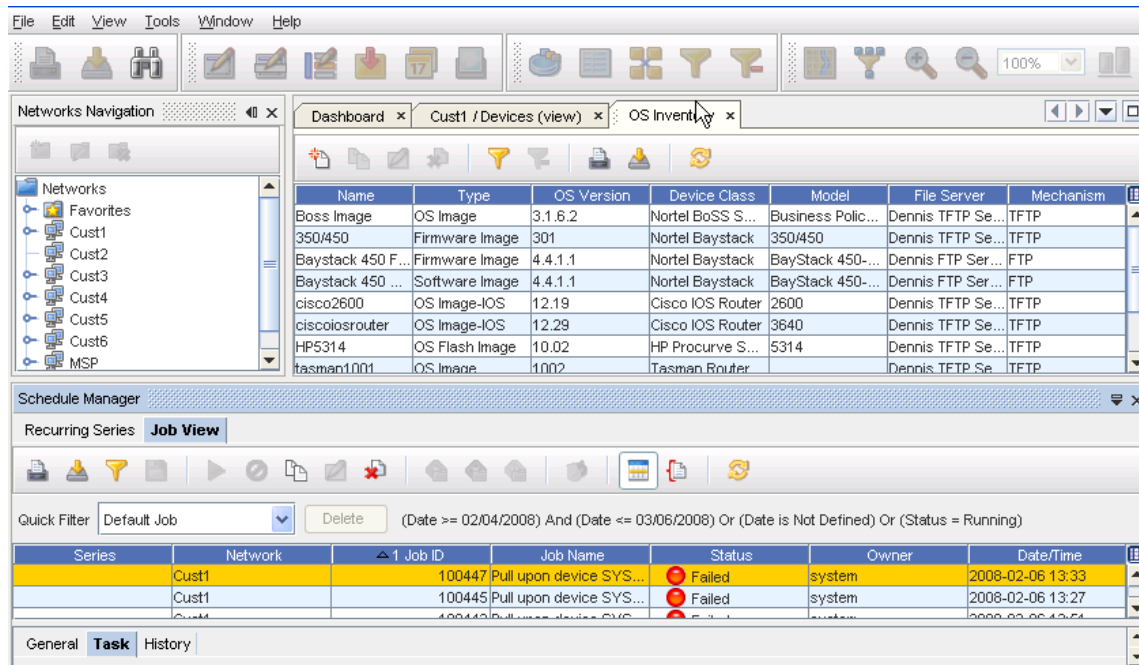
Device Name	File Name	Revision	Type	Network	Modified	User
-------------	-----------	----------	------	---------	----------	------

**VMware Smart Assurance Network Configuration Manager is licensed to**

Company: emc  
 Department / Division: dev  
 Devices: 100,000 licensed  
 (3 currently being managed)  
 Serial Number: 02052016  
 Support: <https://www.vmware.com/support.html>

The Launch window allows you to open various views (using the **menu bar**), and to have multiple open windows displayed as tabs and headings within the work area of the application. This allows you to quickly go between windows and views without having to open and close multiple windows. You can click on a tab or heading to see the information displayed in that view, and toggle between tabs to quickly view system information.

For example, in the following graphic, the **OS Inventory** and the **Schedule Manager** are opened (by selecting them from the **Tools** menu) in the work area. You can view information, and toggle from tool to tool.



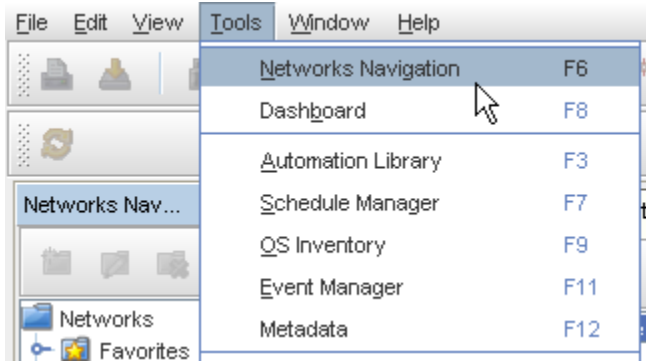
## New User Interface Format

The Graphical User Interface (GUI) of Network Configuration Manager has been redesigned using Netbeans™. You can take advantage of all the customizable features of Netbeans, including the docking and undocking feature, as well as the new three-panel working area.

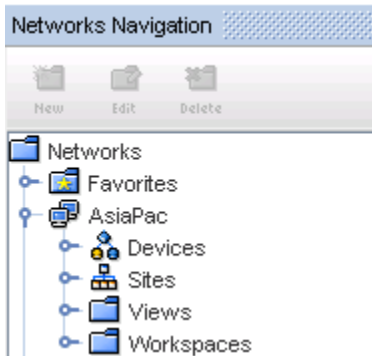
- [Menu bar options](#)
- [The Dashboard](#)
- [Work area](#)
- [Working with Networks](#)
- [Automation Library Navigation pane](#)
- Working with Netbeans

## The Networks Navigation Tree

If the Networks Navigation tree is not displayed, go to **Tools - Networks Navigation**.



From the Launch window, you can now view the **Networks Navigation** in the left pane.



## Networks Navigation Tree

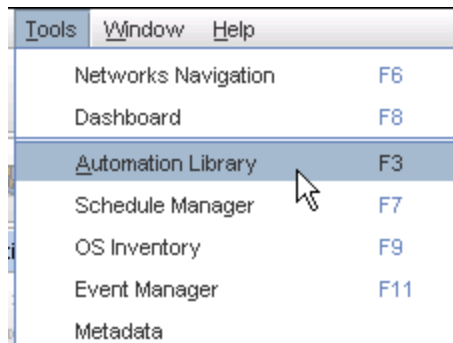
From the **Networks Navigation** tree, the following can be accessed. Click each link for more information on working within the Networks.

<a href="#">Working with Networks</a>	Network configuration is the "backbone" of the application. All other aspects of your network are created and managed from a network.
<a href="#">Favorites Overview</a>	Can include groups of views, screens, and results that you frequently access. Designating a specific View as a Favorite allows you quick access to the information.
<a href="#">Devices Window Overview</a>	A specialized view that contains <b>all</b> network devices.
<a href="#">Sites Overview</a>	A hierarchical structure that allows physical segmentation of devices. Sites are viewed and updated in the Site view of a network by authorized users only. Sites use locations to reference the devices network organization. For example, geography, building, and rooms.

<a href="#">Views Overview</a>	A folder containing user-defined views. Views contain user-defined groupings of operational network devices.
<a href="#">Workspaces Overview</a>	A folder containing user-defined Workspaces. Workspaces are "sandboxes" for storing and staging device configuration changes, and can be used for design and for complex changes.

## The Automation Library Navigation Tree

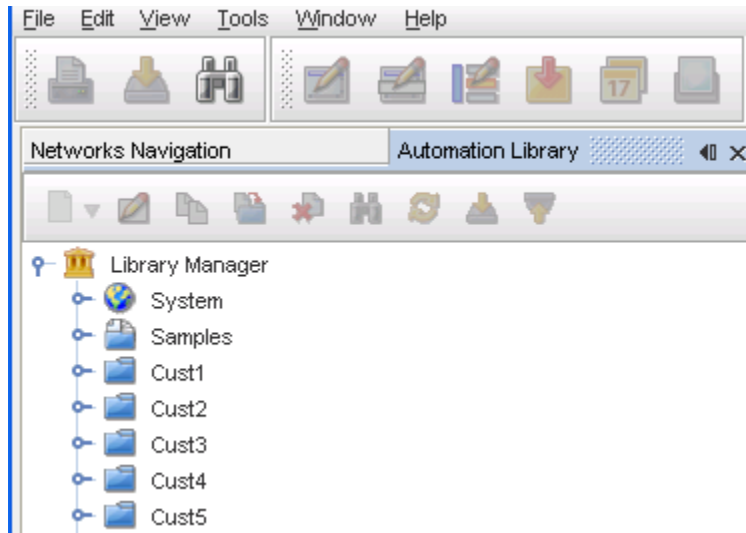
- The **Automation Library** is a powerful tool available in Network Configuration Manager, and is used for creating and storing Standardized Templates, Saved Commands, Policies, and Compliance Standards, along with engineering Metadata that can be used to create customized tests and enforce your corporate best practices.
- The Automation Library (selected from **Tools** in the menu bar) is a stand-alone tool. It is not necessary to have Networks, Sites, or Views open to create or modify Templates, Attribute Queries or Attribute Tests. Once opened, the Automation Library displays the **Library Manager**.
- In the Library Manager, you can establish Tests, Standards, and Policies, and work with the new Compliance Steps.
- The Library Manager allows you to create templates to be used globally (for any network managed by Network Configuration Manager), or for a specific network.




---

**Note** The Automation Library is used mostly by Network Administrators.

---



## Using Contextual Launch

Entering a **pre-defined URL**, a user or an external application can launch the Network Configuration Manager application, and then go directly to a specific location within the application to view device details or job status.

The system has the ability to launch the application in context, via a URL. The user is taken directly to information on specific jobs or devices based on the parameters of the URL. This is especially useful in integrations.

One scenario is where an external system receives an event or SNMP trap about a network device. Users in the external system can click a URL that then launches into the Network Configuration Manager system; directly to the device for detailed information.

Another scenario is where job warnings or failures are issued. A URL can launch the user directly to the offending job for a detailed description of the problem. The URL is constructed as follows:

```
http://<server-ip>:8881/contextual-launch/launch?<param_name=value>
```

or,

```
https://<server-ip>:8880/contextual-launch/launch?<param_name=value>
```

where server-ip is the IP Address of the machine where the server is installed. Refer to the "List of allowed query strings" sections for the allowed param\_names.

For example, a URL to launch to job number 10005 would be as follows:

```
http://<server-ip>:8881/contextual-launch/launch?jobId=10005
```

Various parameters are available as query strings. Where multiple entities could be returned from the query, the user can select the entity they are most interested in.

The URL query can also further restrict the scope of the launch by including a network parameter. This parameter must be used in conjunction with one of the above parameters. For example, to launch to any device that contains an IP address of 192.168.1.1 in a network called MyNetwork, the URL would be as follows:

`http://<server-ip>:8881/contextual-launch/launch?networkId=MyNetwork&anyDeviceIP=192.168.1.1`

The contextual launch capability was specifically designed to give the integration developer flexibility. It is intended to allow tighter integrations between disparate systems with less effort.

## List of Allowed Query Strings

Param Name	Type	Search Target
jobId	int	Specific job number
deviceAlias	string	Device with indicated alias
deviceIP	ip address (management)	Management ip
anyDeviceIP	ip address (management/ interfaces)	Device with management ip as specific
deviceHostname	string	Host name of device
deviceFQDN	string	Any device where the FQDN, alias, derived name, or hostname match the parameter
deviceName	string	Device whose name has been derived by a method specified by the system administrator
anyDeviceName	string	All known names for the device
derivedName	string	Device whose name has been derived by a method specified by the system administrator
anyDeviceNameOrIP	{string, ip address}	A combination of the previous two – the system will check any name or ip address on the device
value	{int, ip address, string}	The system determines whether the value is a job number, device name, or ip address, and then launches to the appropriate entity

**Note** TheNetworkID can be used in conjunction with deviceName or deviceIP.

# Accessing Help and Additional Documents

# 4

This chapter includes the following topics:

- [Accessing the Online User Guide](#)
- [Accessing Documents in the Reference Library](#)
- [Using Keystroke Shortcuts](#)
- [The Application icons](#)

## Accessing the Online User Guide

Welcome to the Online User Guide. The purpose of this guide is to provide you with procedures you need to complete tasks, to help you in quickly locating information, and to make accessing tools and views as easy as possible.

HTML and PDF versions of the NCM Online Help are as follows :

- [NCM Online User Guide HTML File - Network Configuration Manager Online Help.](#)
- [NCM Online User Guide PDF File - Network Configuration Manager Online Help.](#)

---

**Note** Voyence University is now discontinued and you will not be able to launch or access Voyence University from the user interface.

---

- 1 Select **Welcome to Network Configuration Manager**, and review each of the items contained within that book to further introduce you to the application.  
  
Click the **Introducing the User Interface** book, and review the information (topics) contained within that section as well.
- 2 To review more information offered within the Online User Guide, select **Accessing Help and Additional Documents**. Contained within that book is a complete **glossary** of terms and acronyms, along with definitions of tools and features. Also included is a **Reference Library** where additional Network Configuration Manager documents are stored and can be accessed.



3 After reviewing the information referred to in Steps 3, 4 and 5, click the book for your appropriate **user type** from the following options:

- **END USER** - Getting Started
- **SYSTEM ADMINISTRATOR** - Getting Started
- **NETWORK ADMINISTRATOR** - Getting Started

Each user-named section has the information you need to complete specific tasks, and to gather additional Network and Device information.

## Accessing Documents in the Reference Library

This **Reference Library** contains a list of Network Configuration Manager documents and Network Configuration Manager Document Contents. You can access all the Network Configuration Manager documents from VMware Online Support: <https://www.vmware.com/in/support.html>.

Depending on your user status; System Admin, Network Admin, or End User, these documents will prove helpful when using Network Configuration Manager.

The NCM documentation set is now streamlined and the number of individual documents is reduced. The Installation Guides are now consolidated into a single document for all NCM components. The Release Notes and the User Guides are also consolidated into a single document for all NCM components. A new Device Driver Toolkit Technical Notes document is also created in this release. The DSR Release Notes are merged with the NCM Release Notes. Product documentation is available as a download from VMware Online Support.

Document Title	Document Contents/Details	Who should read this document?
VMware Smart Assurance Network Configuration Manager Application Program Interface (API) Programmer's Guide	Application developers will use this interface to programmatically access data and/or functionality of the Network Configuration Manager system.	Network Admin
VMware Smart Assurance Network Configuration Manager Application Program Interface (API) Javadoc Reference Guide	Access the Network Configuration Manager API Reference Guide (Javadoc) at the following location: <a href="https://SERVER_IP_ADDRESS:8880/ncm-webapp/javadoc/">https://SERVER_IP_ADDRESS:8880/ncm-webapp/javadoc/</a> Where SERVER_IP_ADDRESS is the IP Address of the machine where the server is installed. API_VERSION is the version of the API Installed.  <b>Important</b> You must <b>first</b> have the API installed to successfully link to this document.	Network Admin
VMware Smart Assurance Network Configuration Manager Installation Guide	Provides information on the backup and restoration utilities pre-configured to backup the critical data in your environment.	Network Admin, System Admin

VMware Smart Assurance Network Configuration Manager Device Access Scripting Language (DASL) Specifications Guide	Describes the Data Access Scripting Language (DASL) for use in creating device-independent access methods to allow products to provide multiple-vendor support.	Network Admin
VMware Smart Assurance Network Configuration Manager Installation Guide	Gives needed information that is common to all integration modules.	Network Admin
VMware Smart Assurance Network Configuration Manager Regular Expressions (RegEx) Guide	Contains an overview of how RegEx is used within Network Configuration Manager. This document is not intended to be used as a definitive RegEx source, but only as a reference as it relates to Network Configuration Manager.	Network Admin
VMware Smart Assurance Network Configuration Manager System Management Console Guide	Addresses control features allowing you to complete basic monitoring tasks, and to make adjustments to the services running on Network Configuration Manager.	Network Admin, System Admin

## Using Keystroke Shortcuts

Keystroke shortcuts are included to allow quick access to tools and windows within Network Configuration Manager.

**Important** You may want to print this information to use as a quick reference.

F1	Opens Help Contents.
F3	Opens Automation Library.
F4	Opens System Administration.
F5	Refreshes the window.
F6	Opens the Networks Navigation View.
F7	Opens Schedule Manager.
F8	Opens the Dashboard View.
F9	Opens OS Inventory.
F11	Opens the Event Manager.
Alt+E	Opens Editor options on menu bar.
Alt+F	Opens File options on menu bar.
Alt+H	Opens Help options on the menu bar.
Alt+P	Opens the Properties for Device - (device view).
Alt+T	Opens the Tools options on the menu bar.

Alt+R	Refreshes the Workspace.
Ctrl+A	Selects All data or text - in a window pane or editor window.
Ctrl+B	Opens the Bird's Eye View - in Devices View.
Ctrl+D	Diagram Toggle - toggles between Diagram and Table view (in Devices View).
Ctrl+F	Search - in Devices View.
Ctrl+G	Opens the Configlet Editor.
Ctrl+I	Opens the Interface Editor.
Ctrl+L	Saves the current layout.
Ctrl+M	Opens the Command Editor.
Ctrl+N	Opens Create Virtual Device.
Ctrl+O	Opens existing Workspace or Network.
Ctrl+P	Opens the Print widow.
Ctrl+R	Opens the Container Properties window.
Ctrl+S	Opens the Device Search window.
Ctrl+T	Displays the Table layout in devices view.
Ctrl+U	Opens the Change Audit window.
Ctrl+W	Closes the current open window.
Ctrl+Y	Completes a redo of the last qualified undo.
Ctrl+Z	Completes an undo of the last qualified action.
Ctrl+	(on number pad) Zooms in on Diagram layout in Devices view.
Ctrl-	(on number pad) Zooms out on Diagram layout in Devices view.

















## The Application icons

In Network Configuration Manager, various icons are used to represent tasks, settings, device status, functions, and actions that can be completed while using the application. Depending on the window and view, icons change as the available functions change.

For example, you can find icons available for a specific network, and other icons available for all networks. Moving your cursor over an icon gives you the description of that icon (**a tool tip**). For example, in the **Schedule Manager**, the **Print** icon is displayed with the name associated to that action.

Schedule Manager

Recurring Series **Job View**

Quit **Print** er Default Job  (Date >= 02/04/2008) And (Date <= 03/06/2008) Or (Date is Not Defined)

Series	Network	Job ID	Job Name
	Cust1	100447	Pull upon device SYSLOG event
	Cust1	100445	Pull upon device SYSLOG event
	Cust1	100443	Pull upon device SYSLOG event
	Cust1	100441	Pull upon device SYSLOG event
	Cust1	100439	Pull upon device SYSLOG event
	Cust1	100437	Pull upon device SYSLOG event

**Note** Note that, a number of icons have been added and updated for this release.

# END USERS - Getting Started

# 5

This chapter includes the following topics:

- Getting Started - End User Overview
- Getting Started - End Users Tasks
- Working Within a Network
- Working with Favorites
- Working with Devices (Devices View)
- Working with Global Device Search
- Working with Sites
- Working with Views
- Working within a Workspace
- Multi-Configuration File Support
- Working with Editors
- Scheduling Jobs
- Working with the Schedule Manager
- Working with the Data Field Manager

## Getting Started - End User Overview

As an **End User** you have specific tasks that you can complete, as well as access to specific information contained within VoyenceContol. For example, you can complete global Device Searches, View Devices properties, and more.

As an **End User**, you can access information, work with Networks, Sites, Views and Devices, Schedule jobs, and work with Editors. For a complete list of the tasks you can complete, go to [Getting Started - End Users Tasks](#).

Tasks that are listed under the **END USER - Getting Started** are the tasks that you would normally complete while using Network Configuration Manager.

---

**Important** You must have permission from your System Administrator to view the Event Manager, or to approve a job that has been scheduled. If you have any questions on your permissions or access to other tasks, or to procedures within Network Configuration Manager, see your System Administrator.

---

## Getting Started - End Users Tasks

As an **End User**, you have been granted certain privileges by your System Administrator. These privileges make it possible for you to access information, and work with Devices.

You also have been granted privileges to complete tasks, such as scheduling jobs, and working with Editors.

---

**Note** Depending on the permissions granted to you, you can (in most cases) complete the following tasks.

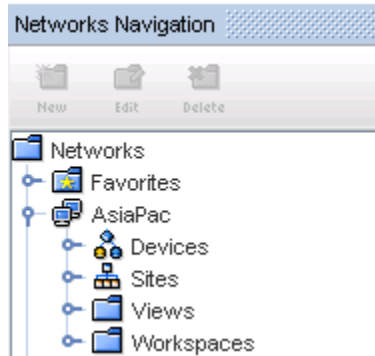
---

- [Setting RSA PINs](#)
- [Favorites Overview](#)
- [Working with Networks \(Networks Navigation\)](#)
- [Devices Window Overview](#)
- [Using Find in the Devices Window](#)
- Work with a Network's [Views Overview](#) , [Sites Overview](#) , and [Workspaces Overview](#)
- Work with [Editors Overview](#) and Schedule jobs
- Work with the [Schedule Manager Overview](#)
- [Changing Token Pins](#)

## Working Within a Network

### The Networks Navigation View

The **Networks Navigation** view is where all the Networks are listed. This also gives you access to the listing of Devices within that Network, along with access to Sites, Views, and Workspaces that have been created within that Network.




---

**Note** The **Favorites** folder (also associated to a specific Network) is used to store shortcuts to Network views or Workspaces you use most often.

---

Networks are containers for a collection of devices. While devices within a Network generally have a common association, such as customer or location, there may not be any relation to devices in a Network Configuration Manager Network.

Devices are associated with a Network through two methods:

- Network Auto Discovery
- Device assignment

The Network sub-containers, consist of the following:

- **Favorites** - A storage facility for the Favorites you select
- **Devices** - A listing of all devices associated with a Network
- **Sites** - A hierarchy representing the physical location and relationships of devices in the Network
- **Views** - A folder structure containing a group of logical devices associations. Views can be both statically or dynamically constructed.
- **Workspaces** - A folder structure for storing "work in progress" designs of Network devices before deployment into the Network. Workspaces can contain copies of existing deployed devices, or virtual devices to be deployed.

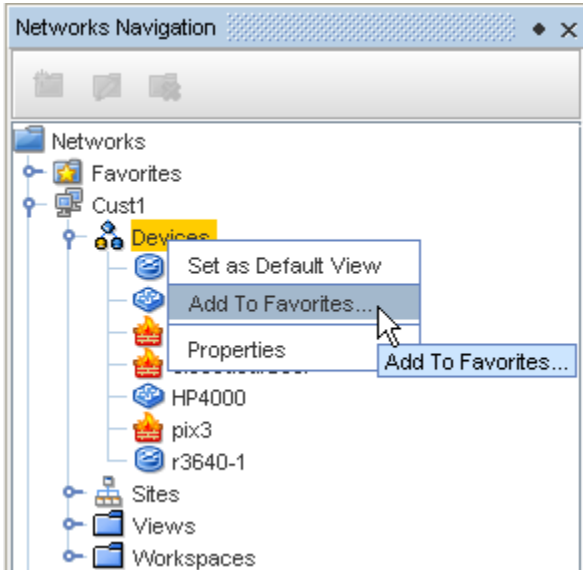
## Working with Favorites

### Favorites Overview

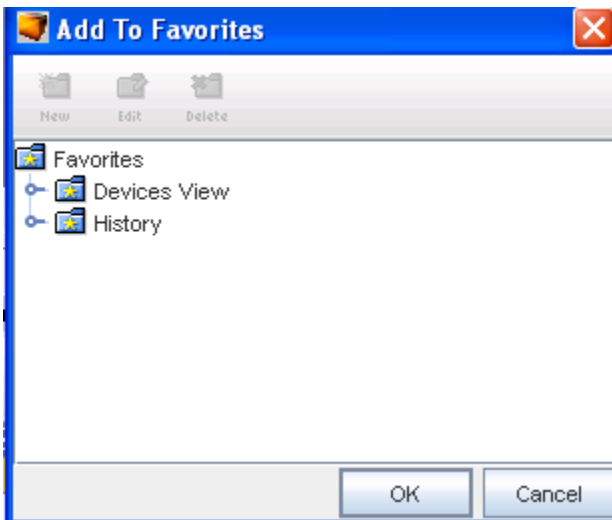
Within Network Configuration Manager you can create a **Favorites list** for Views and Workspaces. These designated favorites can then be selected from the Networks Navigation pane (under Favorites), allowing you to quickly access the Views and Workspaces you use most often.

To add a Favorite to your Favorites list,

- 1 Under **Networks Navigation** , select a **View** or **Workspace** from the navigation pane.
- 2 Once selected, right-click on the **View** or **Network** name to display the options available.

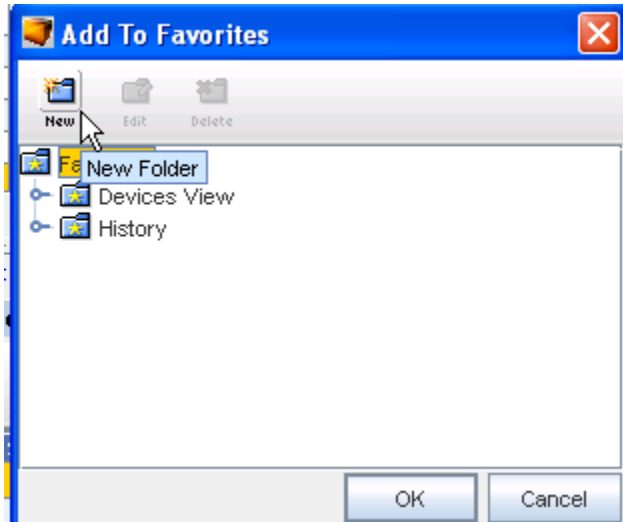


- 3 From the drop-down menu options, select **Add to Favorites**. The Add To Favorites window opens.

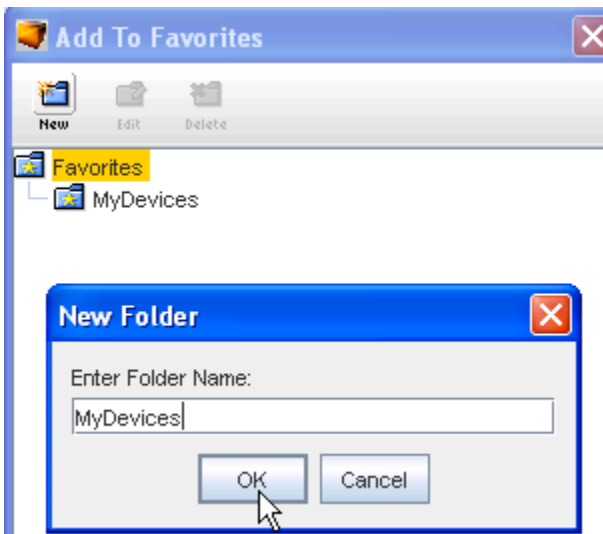


- 4 In the **Add to Favorites** window displayed, you can:
  - Select an existing folder where this Favorite can be stored.
    - Select the folder where you want this new Favorite to reside.
    - Click **OK** when you have selected the folder name.
  - Create a new folder to store the Favorite.
    - Click **Favorites** in the window.



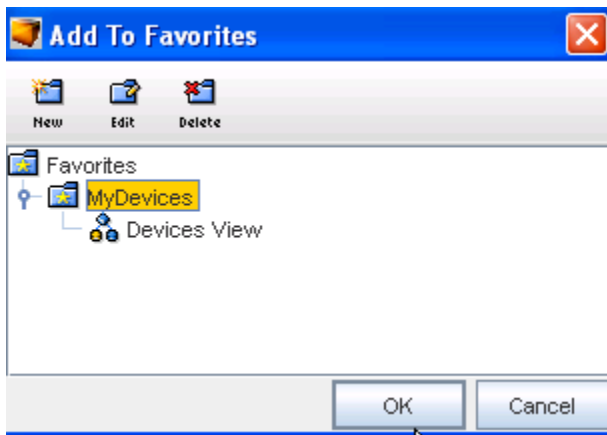


- Click the **New** icon, and enter a **new folder name** in the field.



- Click **OK** after you have entered the new folder name.

5 Now, select the new folder name from the list displayed in the **Add to Favorites** window.



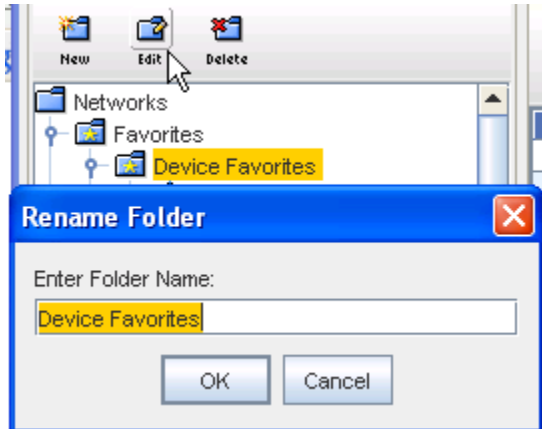
- 6 Click **OK** to add this Favorite (View or Workspace) to the folder you selected.

## Editing Favorites Names

You can designate views and workspaces to be stored into Folders you create within the Favorites feature. Once a folder is created, you can **change** the name (edit) of the folder.

To edit a Folder Name in your Favorites list,

- 1 While your Favorites list is open, you can select any folder from the list, then click the **Edit** icon.



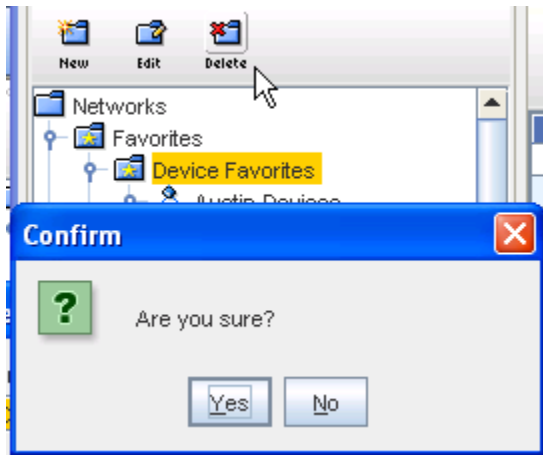
- 2 From the Rename Folder window, you can change the Folder name by entering a new folder name. Click **OK** when you have renamed the folder.

## Deleting Favorites from the List

You can designate views and workspaces to be stored into Folders you can create within the Favorites feature. You can also **delete** any folders that are no longer needed within the Favorites list.

To delete a Folder Name in your Favorites list,

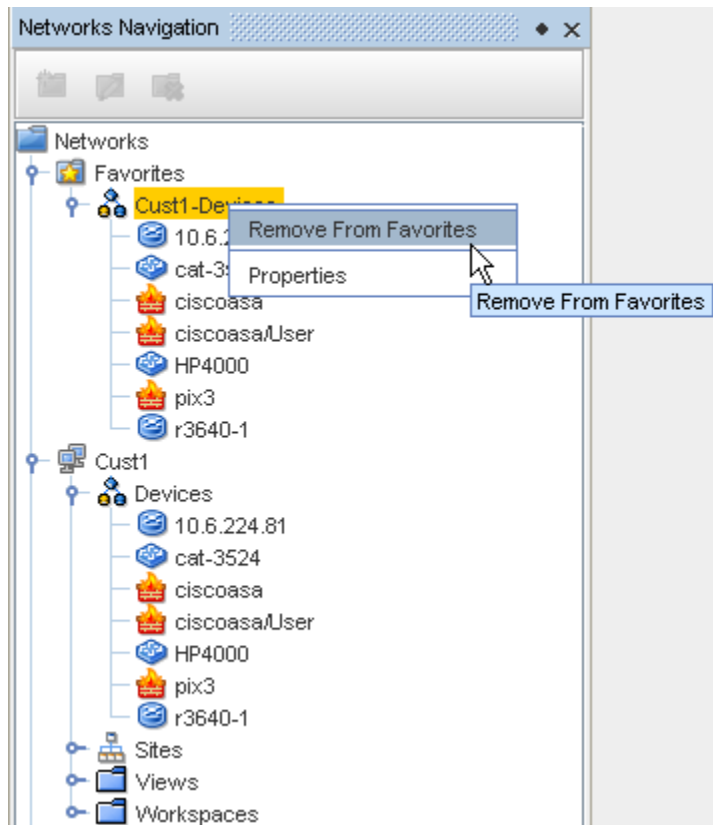
- 1 While your Favorites list is open, you can select any folder from the list, then click the **Delete** icon.



- 2 At the confirmation message, click **Yes** to delete this folder from the Favorites list. All views and workspaces contained within that Folder are also deleted from the Favorites list.

**You can also Delete Favorites from the Navigation Tree**

You can delete any favorite (views or workspaces) that you have added to the Favorites from the navigation tree.



- 1 To remove a previously defined favorite, select that favorite directly from the Networks Navigation tree, and right-click to display the options.

- 2 Select **Remove From Favorites**. Your selection is removed from the list of Favorites.









## Working with Devices (Devices View)











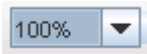
### Options on the Device View Tool Bar





Here are the options located on the **tool bar** when Devices are displayed.



The options include the following:

Icon	Icon Meaning	Action
	Print	Takes you your browser's print facility, where you can print the current view
	Export	Takes you to the Save window where you can select the location to save this view, and in what format you want to save
	Device Search	Takes you to the Device Search window where you can enter information to search on a specific device
	Config Editor	Takes you to the Config Editor. This editor is designed for editing a single, full running configuration file that affects one or more devices
	Configlet Editor	Takes you to the Configlet Editor. This editor is used to edit whole or partial configurations that are Pushed to the network.
	Interface Editor	Takes you to the Interface Editor. This editor is used to <b>make changes to multiple interfaces on multiple devices</b> - Global area
	Command Editor	Takes you to the Command Editor. The intent of the Command is not to change or update a device's configuration, although a Command can be used for this purpose. The intent is to provide access to device-level information for completing actions.
	Schedule	<b>Note</b> This feature is only available for Workspaces.

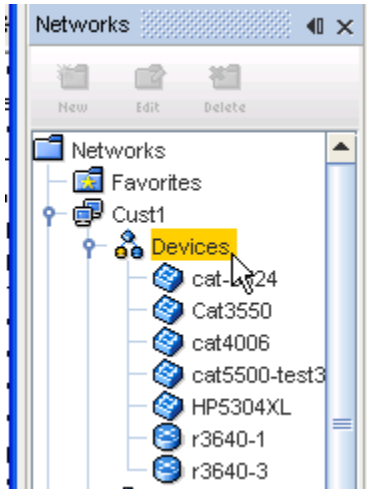
Icon	Icon Meaning	Action
	New Virtual Device	Only available in the <b>Workspace</b> view. This allows you to create a device that can be added to a workspace for testing or creating "possible" networks.
	Properties	When accessed, the Device Properties tabs are displayed
	Table View	Displays the list of devices in a table format
	Diagram View	Displays the list of devices in a diagram format. When accessed, you can switch between Diagram and Table format
	Apply Filter	Use this to access the Device Display Filter window, and select other filter criteria
	Cancel Filter	Use this to cancel a filter you have just selected, or to cancel a pre-existing filter or set of filters
	Birds-Eye View	Displays a birds-eye view of the network only in Diagram view
	Connection	Displays the Network connections
	Zoom In	Allows you to zoom in on the Diagram view
	Zoom Out	Allows you to zoom out on the Diagram view
	Enlarge/Reduce	Only available in the Diagram view. This can be used to enlarge or reduce the sign of the viewing window.

Icon	Icon Meaning	Action
	Align	<ul style="list-style-type: none"> <li>■ Bottom aligns all devices along the bottom of the window</li> <li>■ <b>Horizontal</b> aligns all devices horizontally in the window</li> <li>■ <b>Left</b> aligns all devices to the left of the window</li> <li>■ <b>Right</b> aligns all devices to the right of the window</li> <li>■ <b>Top</b> aligns all devices along the top of the window</li> <li>■ <b>Vertical</b> Aligns all devices vertically in the window</li> <li>■ <b>Horizontal</b> aligns all devices horizontally in the window</li> <li>■ <b>Around</b> not active in this layout.</li> </ul>
	Rearrange Connections	<p>Rearranges the current view of the connections. Including:</p> <ul style="list-style-type: none"> <li>■ Around</li> <li>■ 90 degrees</li> <li>■ Stagger</li> <li>■ Top/Left</li> <li>■ Bottom/Right</li> <li>■ Arrange Connections</li> </ul>
	Legend	<p>Takes you to the legend list. This list contains all the symbols used for the various device states, devices, and connections.</p>
	Refresh	<p>After making changes, use the Refresh icon to refresh your current view</p>

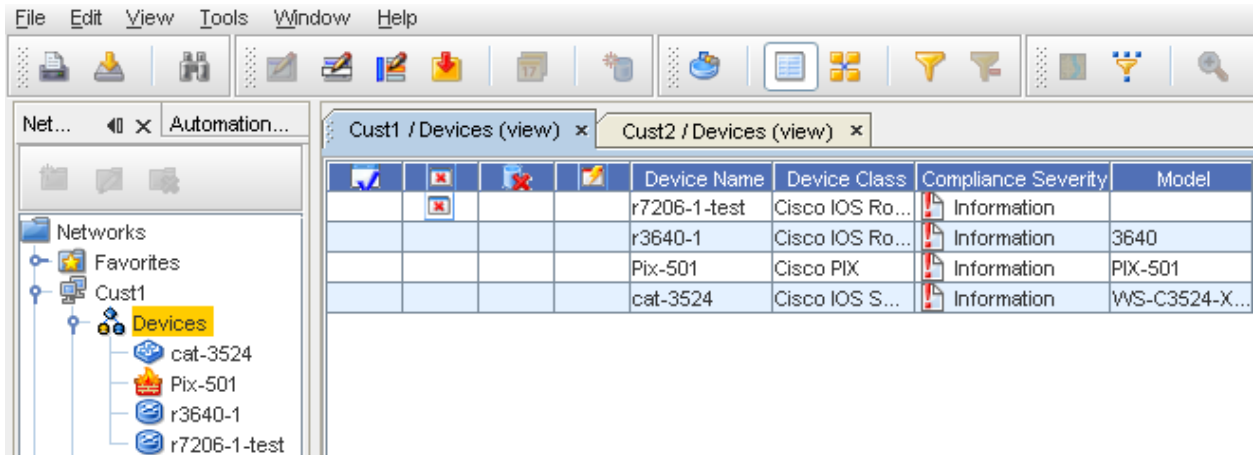
## Devices Window Overview

A **Device** can be a piece of equipment, and can also be routers, switches, firewalls, VPN concentrators, and OS images.

Access the Devices Window by selecting **Devices** from a specific Network listed in the Networks Navigation tree. The devices are displayed in the right pane. For example, the Devices within the **Cust1 network** are shown in a list.

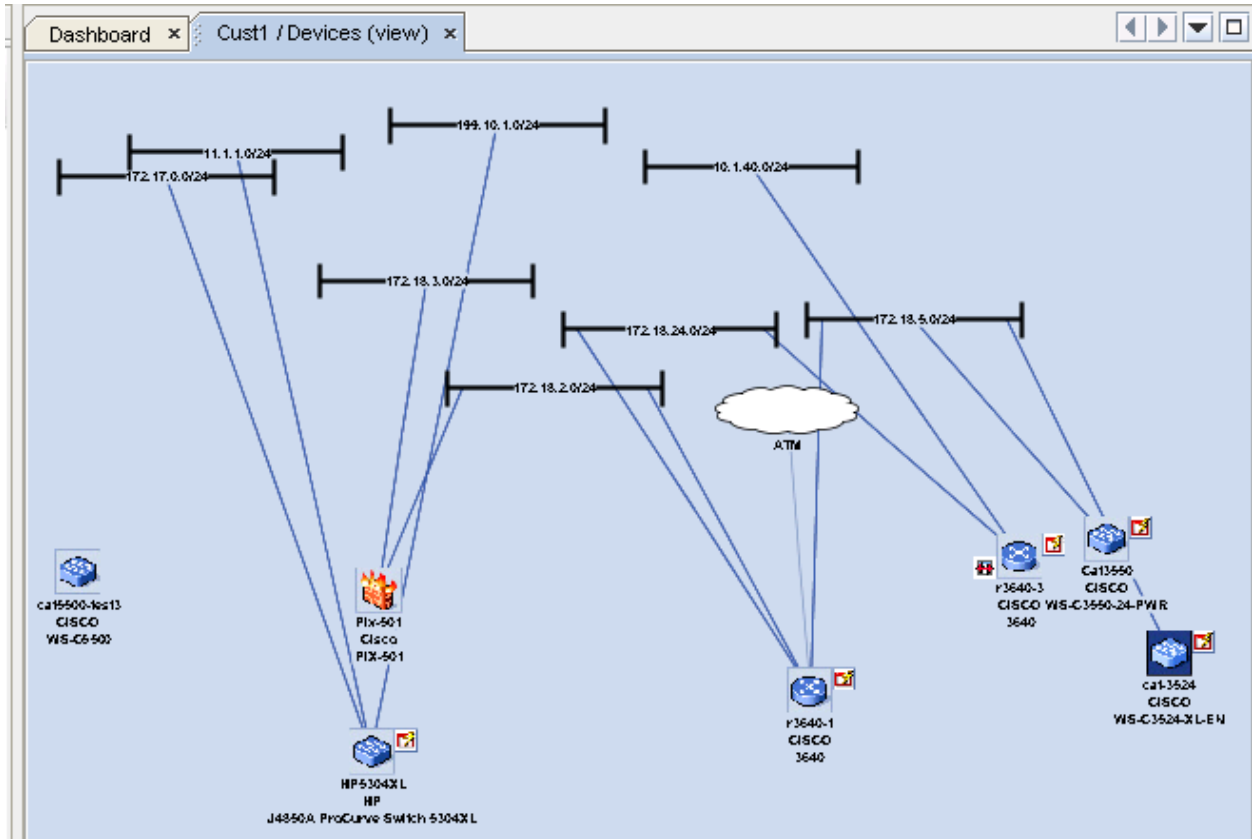


The Devices window has two interfaces you can use to monitor your networks. Each of these views is accessed by using the icons in the Devices tool menu bar. You can switch between the views.



- Table view** - A display of all the devices in a network shown in **table format**. The table icon selection in the tool bar is used to display the devices in the table view.

**Note** Due to the large size that networks can become, when opened most Devices views default to a table view.



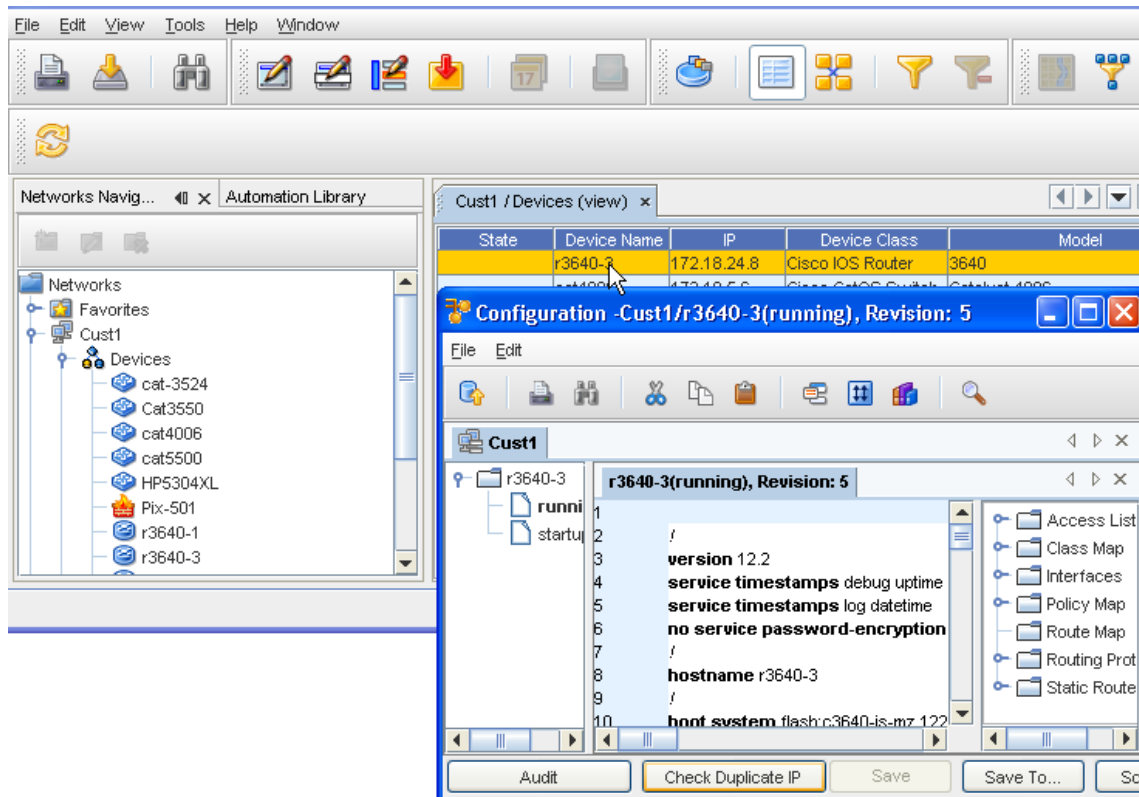
The graphical diagram for a Site, View or Workspace show the devices and their connections. Connections can be filtered by technology type, or presented as logical layer (layer 3) connections.

- Diagram view** - A graphical representation of the **interconnections** of all the devices in a network. The diagram view icon selection is used to display the devices in the diagram view.

### Additional information

While viewing the devices listing in the Devices view, you can double-click the Device name, and view the **running Configuration** . For example, when the 23640-2 Device Name is double-clicked, the running Configuration for that device is displayed.

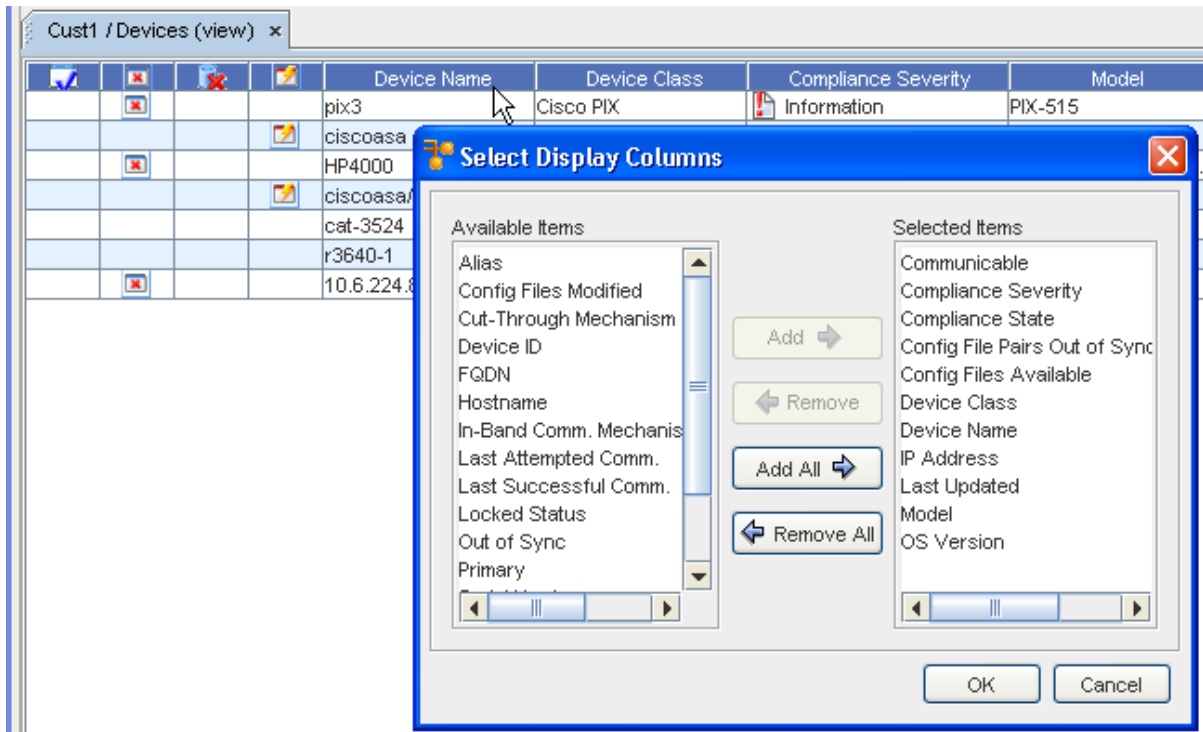




## Displaying Column Headings in the Devices View

Table columns (and the information they contain) can be added or removed to customize your display.

- 1 With the Devices View displayed (shown here as Network **Cust1/Devices (view)**), right-click within any column heading to view the **Select Display Columns** window.




- 2 From here, determine **which of the column headings** you want displayed.
- 3 Make your selections by highlighting the columns you want displayed from the **Available Columns** pane, then use the **Add** or **Add All** arrows to move the headings you chose into the **Selected Columns** pane.
- 4 To hide column headings (and the information within that column) highlight the column heading in the Selected Columns pane, and using the **Remove** or **Remove All** arrows, move the headings you select back into the **Available Columns** pane.
- 5 Click **Ok** to keep your final selections.

Only those column headings within the Selected Columns pane display on the Devices View in a table layout.

Once you have determined the column headings you want to display, you can then change the size of each column to view all the information that column holds by dragging the column table lines to the right or left to enlarge any specific column.

State	D...	Ali...	FQDN	Device ID	Hostn...
	ca...		cat-3...	1003	cat-35...
	Ca...		Cat3...	1001	Cagg...
	ca...		cat4...	1004	CatOS...
	ca...			1007	cat55...
	HP...		HP53...	1005	HP-53...
	r3...			1002	r3640...
	r3...			1006	r3640-3

Using the right and left arrows  you can increase or decrease the size of each column to view more or less column information. Within Network Configuration Manager, you can change the size or location of any column that is displayed within a table in the application. You can also move the columns horizontally (by dragging and dropping) to place a column anywhere within the table.

Following are the various states the devices can currently be classified in. Run your cursor over each icon to view the status.



## Sorting Columns by Priority

Notice the number **1** in the **Device Name** column . This indicates that the table is sorted, based on this column. The number **1** indicates a Primary sort, **2** (shown here in the **IP** Address column) indicates a Secondary sort, and so on.

To have a secondary and Tertiary sort, hold the Shift key down, and then click within the column headings. The following example shows 3 sort levels (shown here in the **Device Class** column).





1 Device N...	2 IP	3 Device Class	Model
voyenceM7i	172.20.4.11	Juniper	M7i
r3810-11	172.20.4.51	Cisco IOS Router	MC 3810
r3810-1	172.20.4.50	Cisco IOS Router	MC 3810
r2514-2	172.20.54.1	Cisco IOS Router	2514
r2502-2	172.20.51.2	Cisco IOS Router	
r2502-1	172.20.50.2	Cisco IOS Router	2500
ns5gt-wlan	172.20.4.10	Netscreen	NS5GT-WLAN
ns208	172.20.4.9	Netscreen	NS208
cat2950-1	172.20.4.4	Cisco IOS Switch	350-24

## Viewing the Device State Columns

Now you can view the new columns that classify **devices by Device State**.


Compliance State	Device Name	Device Class	Compliance Severity	Model	IP Address	OS Version	Last Update
	r2514-2	Cisco IOS Ro...	Information	2514	10.6.226.5	12.1(5) ENTE...	06/23/2008 0
	10.6.226.10	Netscreen	Information	NS208	10.6.226.10	ns200.5.0.0r...	06/23/2008 0
	ns5gt-wlan	Netscreen	Information	NS5GT-WLAN	10.6.226.9	ns5gt.5.0.0-...	06/23/2008 0
	r2502-2	Cisco IOS Ro...	Information	2502	10.6.226.134	12.2(1d) ENT...	06/23/2008 0
	r2501-1	Cisco IOS Ro...	Information	2501	10.6.226.129	11.3(11c) EN...	06/23/2008 0
	voyenceM7i	Juniper	Information	M7i	10.6.226.11	JUNOS Base...	06/23/2008 0
	r3810-2	Cisco IOS Ro...	Information	MC 3810	10.6.226.16	12.2(10a) EN...	06/23/2008 0
	cat2950-1	Cisco IOS S...	Information	WS-C2950-24	10.6.226.8	12.1(22)EA4...	06/23/2008 0

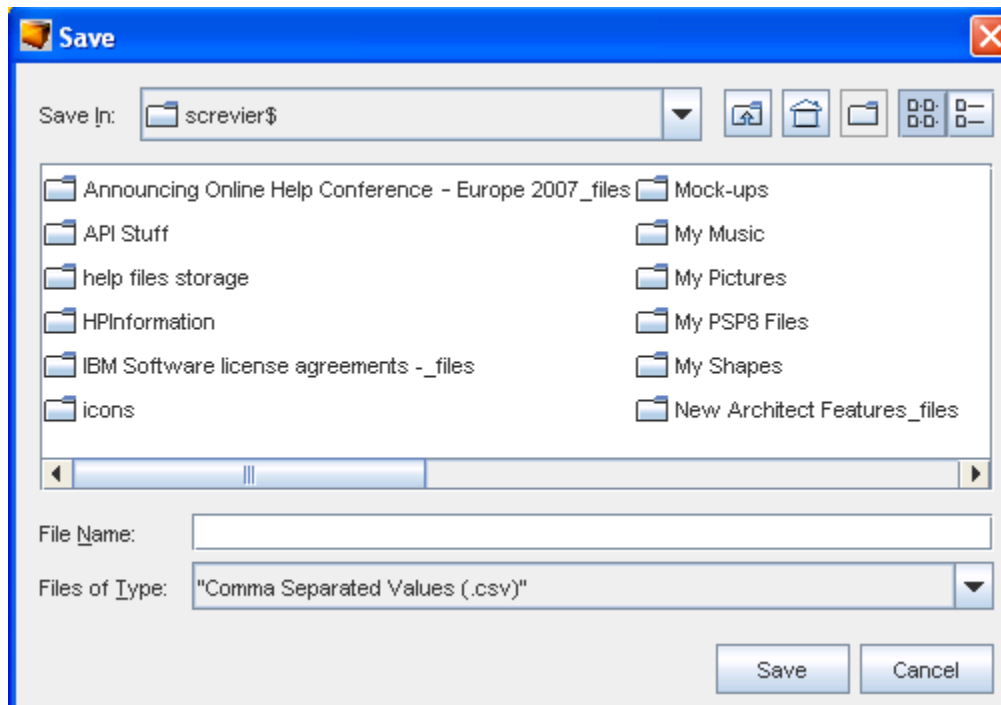
**Note** By moving your cursor over the icon, you can get a **tool tip** and see the type of state in that column.

State Identifier	Icon
Compliance State	 = Compliant
Config Files Available	 = No Config
Communicable	 = No Communication
Config File Pairs out-of-sync	 = Run v/Start Sync

For more information, see [Device States](#).

## Exporting the Devices View


- 1 From the Devices View menu bar, select the **Export**  icon.
- 2 A Save window opens. From here, determine where you want to save this Devices view. Include a **File Name**, as well as the **File Type** selection.
- 3 Click **Save** when you have made your export selections.

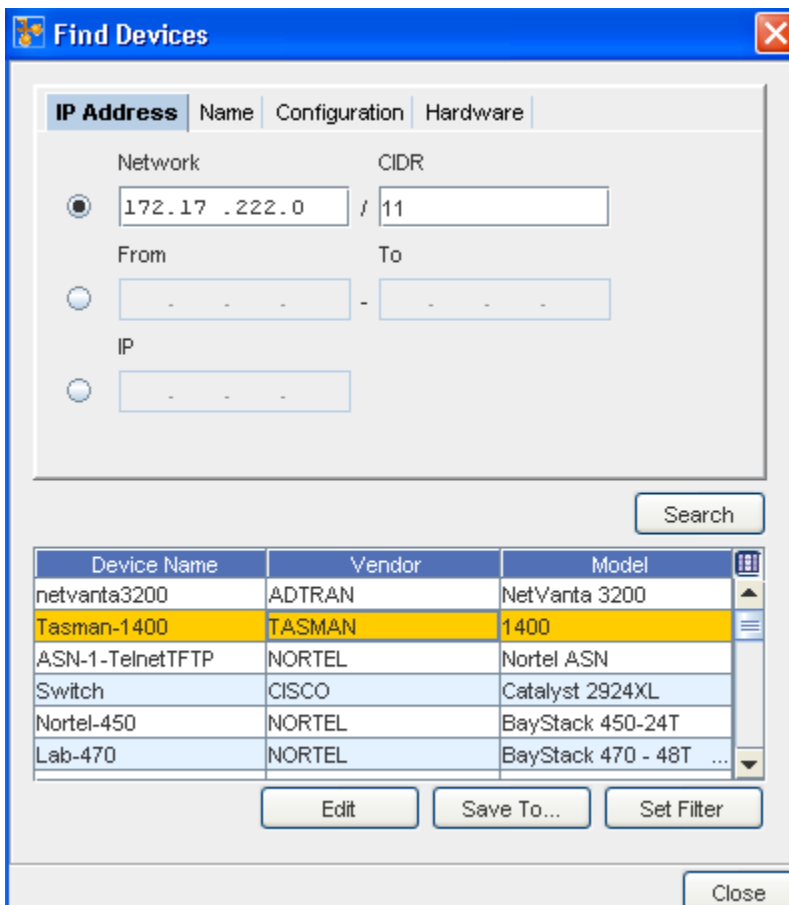


## Using Find in the Devices Window

Network **Find** capabilities include the ability for you to search configuration files with simple find criteria and RegEx. You can also search to find hardware attributes, such as line cards, as well as search by IP Addresses and Hostnames.

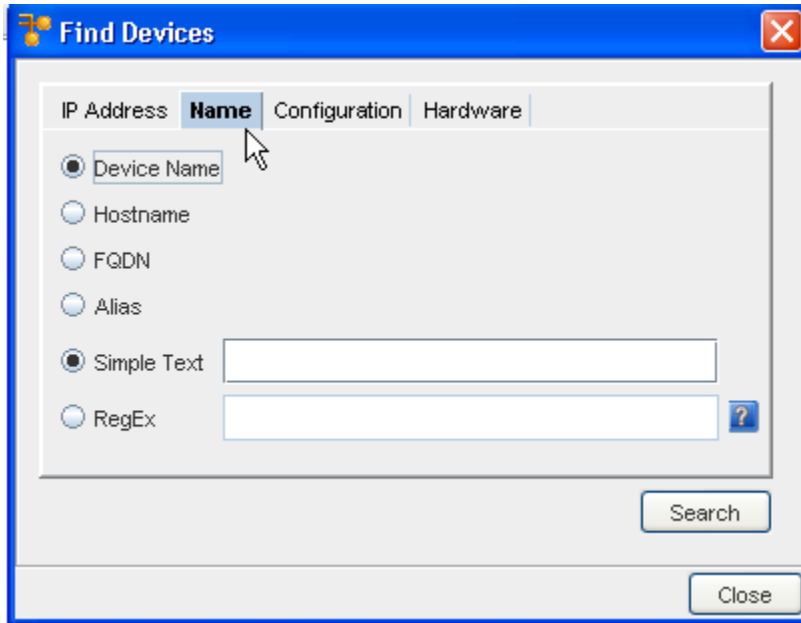


- 1 From the Devices View menu bar, select the **Find**  icon.
- 2 A Find Devices window opens. From here, determine the criteria you want to use in your find. You can search by selecting from the following tabs:
  - IP Address
  - Name
  - Configuration
  - Hardware
- 3 After entering your find criteria into the appropriate tab (shown here in the **IP Address** tab), click **Search**.



- **Edit** - to go to the Configuration editor, and edit if needed
  - **Save To...** - to save the results to a specific location
  - **Set Filter** - to change any existing filters
- 4 Click **Close** when you have completed working with the search results.

## Find Devices by Name



- 1 Select the name type you are using; Device Name, Hostname, Fully Qualified Device Name (FQDN), or Alias, by clicking within the appropriate radio button.
- 2 Enter the **string** into the Search String field to narrow your search, then click **Search**.

---

**Note** You can use the following wild cards when entering search strings.

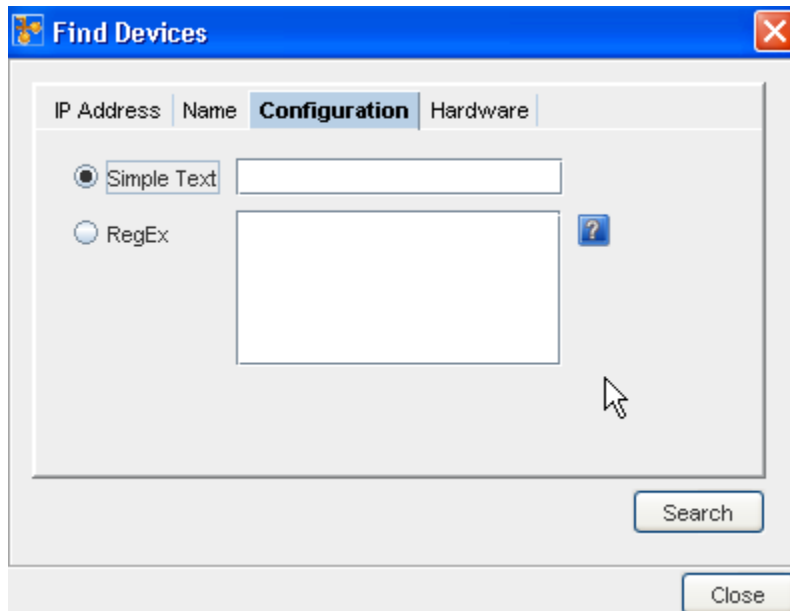
---


- An asterisk (\*) for sequences of characters
- A question mark (?) for a single character

- 3 View your **search results** at the bottom of the screen.

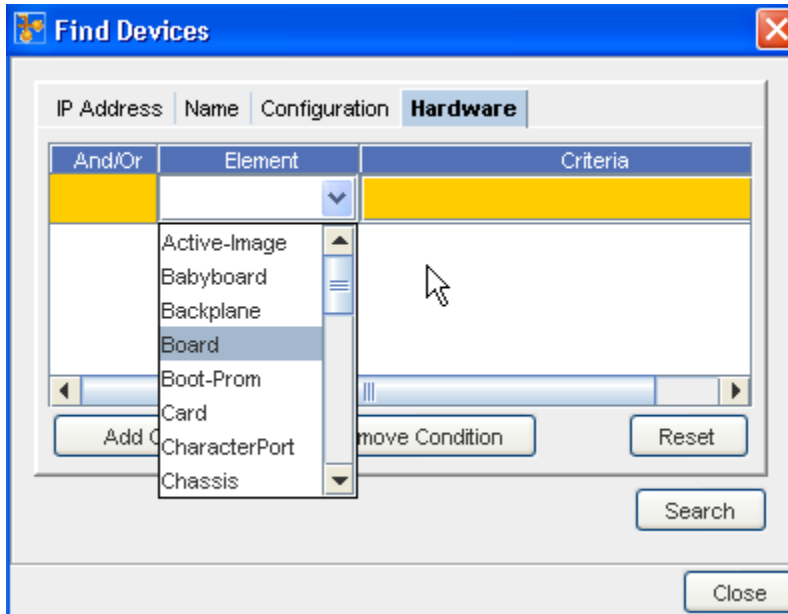
You can also view the **Details** and the **Network** from this window.


## Find Devices by Config tab

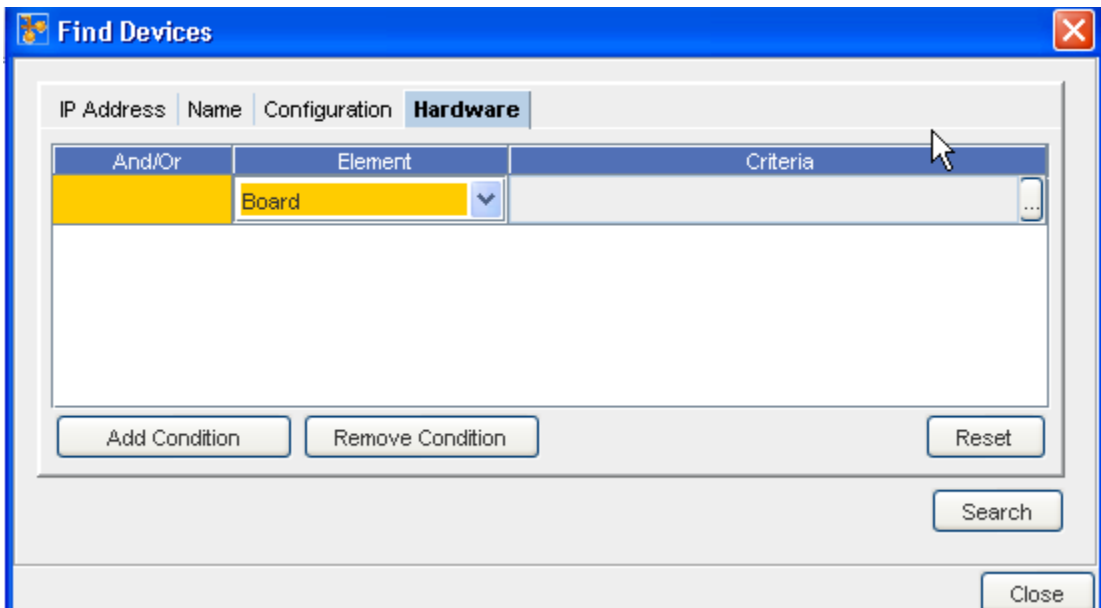


- 1 Select between **Simple Text** and **RegEx**.
  - If using Simple Text, click within the radio button, then **enter the text** you want to use for a search criteria.
  - Click within the **RegEx** radio button to view RegEx.
  - Click the icon  to get more information on using RegEx, and enter the **appropriate expression**.
- 2 After entering your search criteria, click **Search**.
- 3 View your search results at the bottom of the screen.
- 4 You can select a result, then click either **View Details** or **View Network** to get additional details.

## Find Devices by Hardware



- 1 You can define your find criteria by adding conditions (or removing existing conditions). Click **Add Condition**, and select from the Element drop-down options.
- 2 Next, select the drop-down in the Criteria column  to go to the **Criteria for the Element** window you just selected.
- 3 Click the **Add Condition** button to activate the Criteria for Element window.



- 4 Make And/Or, Attribute, Operator, and Expression selections for your search. Note that you can also Remove any existing Conditions, if necessary.





**Note** If you need to make changes to the criteria you have selected, click the **Reset** button to clear the fields, and begin again.



- 5 After making your selection on this window, click **OK**.
- 6 At the Hardware Tab window, click **Search**.
- 7 You can now view your search results at the bottom of the window. **View Details** and **View Network** information is also available from the tabs at the bottom of the window for any device listed in the Search results.

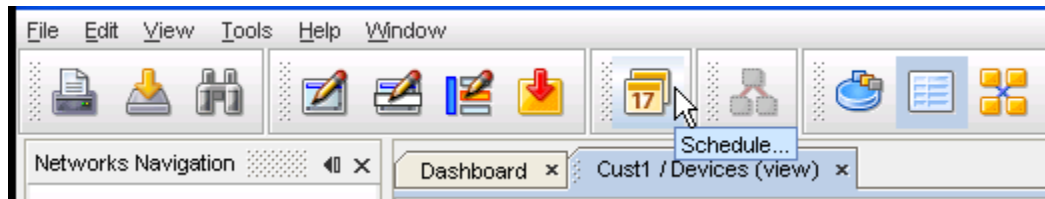
## Accessing Editors in the Devices View

From the Devices View menu bar, you can select an **Editor** from the Editor section. You can access the:

- Config (configuration) Editor 
- Configlet Editor 
- Interface Editor 
- Command Editor 

## Scheduling a Device

From the Device view, you can select to **Schedule** a Device to be pushed.



- 1 After selecting the device from the device's view, click the **Schedule** icon on the tool bar.
- 2 Next, complete all information needed in the Schedule Job tab, Tasks, and Notifications tabs.

---

**Note** A Data Field must have been created for the Data Fields tab to display.

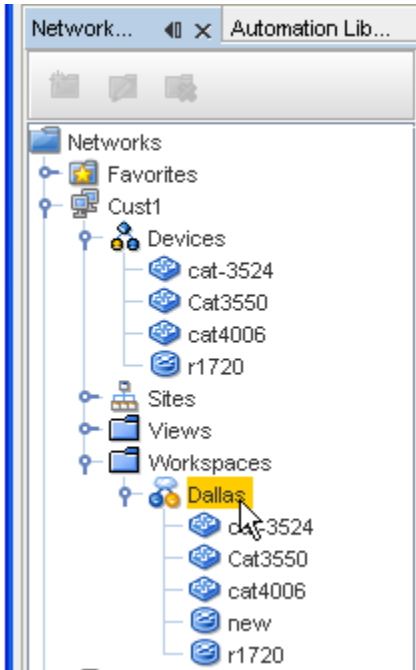
---

## Working with Virtual Devices

After creating the **Workspace**, you can begin configuring the layout using Virtual and Network devices.

To add virtual devices,

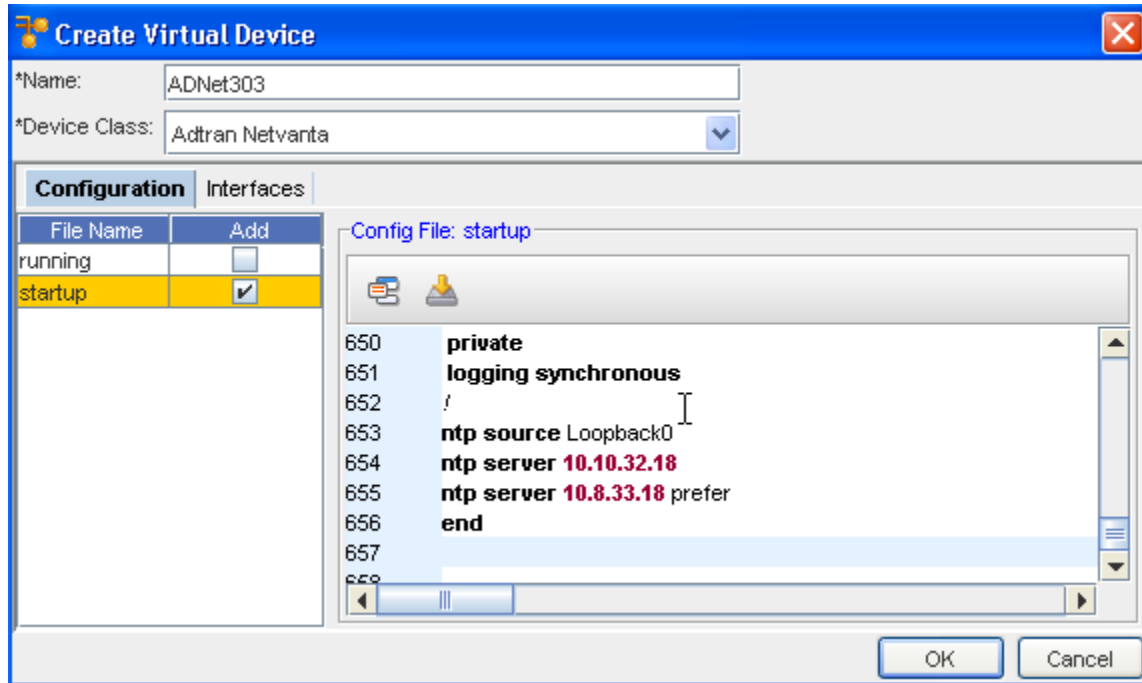
- 1 With the Devices View displayed, select the **Workspace**.



2 Select the **Virtual Device icon** from the menu bar. The Create Virtual Device window opens.



- 3 Type a Virtual Device **Name**.
- 4 From the **Device Class** drop-down arrow, make an appropriate selection from the list.
- 5 Click **Ok**, or continue to make other selections in your virtual device using the Configuration and Interfaces tab.



Working with the Configuration tab,

- 1 At the **Configuration** tab, click the **Add** check box to select the current running configuration.
- 2 You are now linked to the **Library Manager**, and can select a template by going through the various windows. If the template you selected does not match the vendor of one or more of the devices, click **Yes** at the informational box, then make your template selections from the Template Variable Substitution window. Click **Preview** to see the preview of the template, then click **OK**.

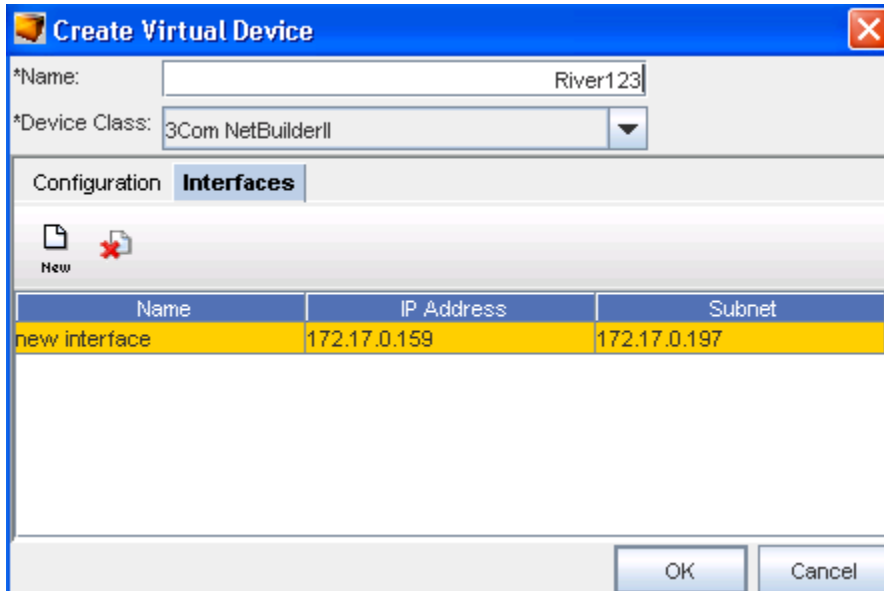
---

**Important** You can also select the **Insert File** icon  to insert a file contents. You can also select to insert a Template.

---

Working with the Interfaces tab,

- 1 Click the **Interfaces** tab.
- 2 To get the Add New Interface window in the **Interfaces** tab, click **New**
- 3 Enter the **Name**, **IP Address** and the **Subnet** address in the fields.
- 4 Click **Ok**.



- 5 Click **OK** to close the Create Virtual Device window.

The workspace refreshes as each device is added. Note the new state of the Device. The new state shows the device has been "Locally Modified".

## Using the Birds-Eye View

---

**Note** You must be viewing your devices in the **diagram layout** to use the Birds-eye feature.

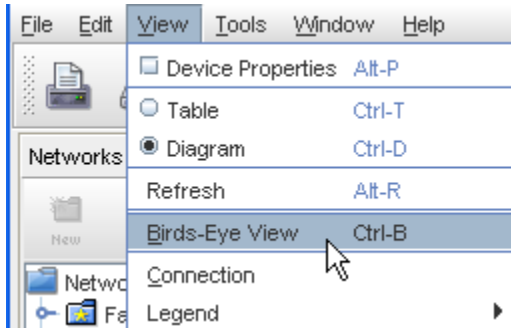
---

The birds-eye view is a snapshot of your network at a 1,000 foot view. The birds-eye view is similar to the **zoom** tool in the diagram toolbar. The zoom tool allows you to enlarge the window to a specific area of your network. Devices outside of the zoomed-in view are not seen in the browser window.

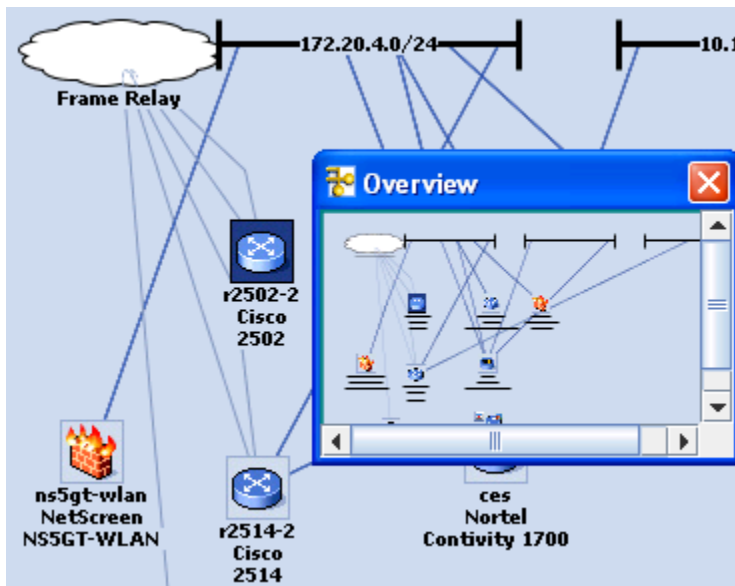
The birds-eye view actually zooms out far enough to see the entire network. A rectangle is used to identify the portion of the network that is seen in the browser window. The intent of the window is to allow you to have a spatial orientation of where you are in your network diagram.

To open the birds-eye view,

- 1 In the menu bar, click **View**. Note that you must first be in **diagram mode** displaying your devices.
- 2 Select **Birds-eye View** .




The Overview window opens in the upper left corner of the application. The birds-eye view is re-sizable, as needed. Use arrows to enlarge the width or length of the view.



## Device States

The Device State can be seen from either the Devices or Workspaces views.

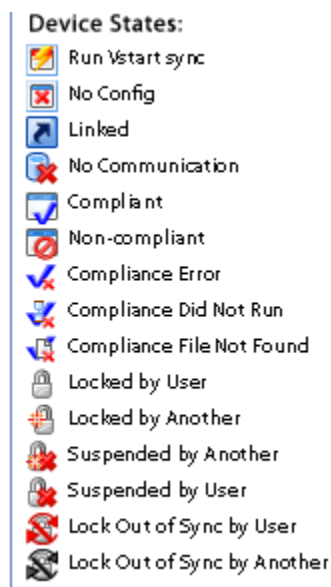


Click the Legend  icon to view the various states.

Listed are the classifications for **device states** :

- Run vs. Start (out-of-sync)
- No Config
- Linked
- No Communication
- Compliant
- Non-Compliant

- Compliance Error
- Compliance Did Not Run
- Compliance File Not Found
- Locked by you (the user)
- Locked by another user (with an entirely different login and password)
- Suspended by another
- Suspended by user
- Lock Out-of-Synch by a user
- Lock Out-of-Synch by another user



This column indicates, by icon, the *state* (or *status*) of the device in your local view, the view of the devices in your network is local. Therefore, a device can be *out-of-sync* with the network. To update a device's config, see [Scheduling Network Level Config and Hardware Spec Pull Jobs](#).

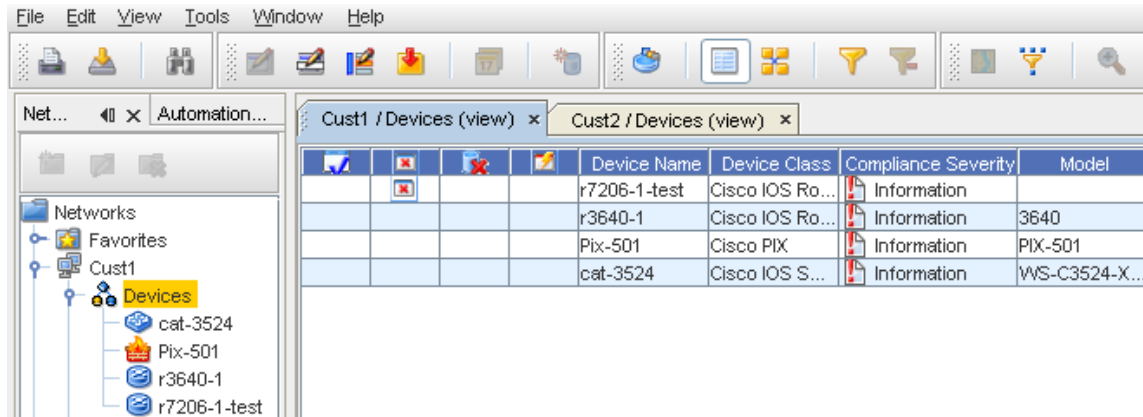
---

**Note** You can place your cursor on the icon within the **State** column to see the name (description) of that specific state.

---

## Devices View of Device State

Following is an example of the device states viewed from the Devices View. In this example, the device r7206-1-test has **not** been configured, and there is no configuration associated to it.




## Sorting on Device States

You can click within any column to **sort** the contents of that column into either ascending or descending order. This holds true as well for the device State columns. Click on the device state icon to sort, then click again to reverse that sort order.

## Clearing Device Flags

The device state is displayed in the table format of the Devices View. Note that there are "flags" or icons that indicate the status of the device.

You can **remove Compliant and Non-Compliant flags** from the Devices view, and not have them visible. This will be in effect until you logout, and login again to Network Configuration Manager.

For example, this icon  alerts you that this device is in a **Non-compliant** state.

To remove a **Compliant or Non-Compliant flag** from the Device View State column, complete the following steps:

- 1 Create a **test policy** containing both a Standard and a Test. This then makes the device **Non-Compliant**.
- 2 Create a **revision** on that device.
- 3 After the push is completed, refresh the devices view.
- 4 Now, create a **dummy policy** (without Standards included).
- 5 Select the device, then right-click the **Non-Compliant device** to get to the right-click menu. Select **System** from the Look In: drop-down arrow. Now, click **Open**. From the Select Item window, select the **dummy policy** you created, and click **Select Item**. At the confirmation message, click **Yes** to continue. The flag marking that device as Non-Compliant is now removed.

## The Devices Legend



When visualizing any Network in the Diagram view, there are multiple icons that are used to represent connections, device states, and device types. Depending on the makeup of the Network, some of the components are shown.



The **Legend** is used to identify the devices and their connections, if any, within the network. There are three sections to the Legend:



The first section is **Connections**. This identifies the connection method devices use to communicate with one another.



The second section is **Devices**. This identifies device types within the network. Each device in a network is represented by a corresponding icon.



The third section is **Device States**. This identifies the state of the device's configuration.

**Note** Note that Device States may change if the actual state of the device changes while in the Devices View.

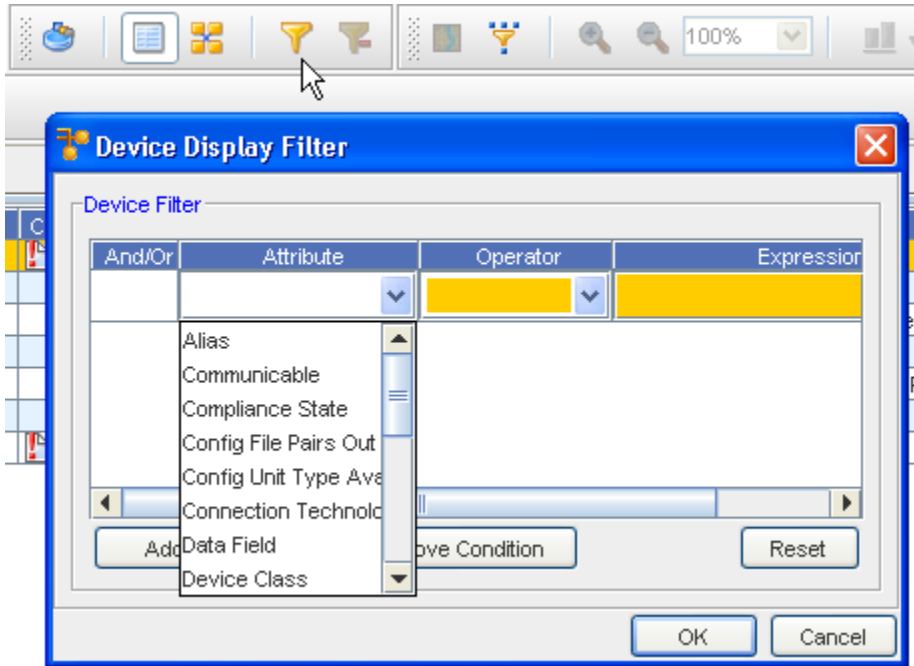
## Filtering Devices

Network devices can be filtered in any Site, View, or Workspace, so only those devices applicable to your tasks are displayed. Each attribute has its own set of application operations. Device filtering allows you to manage a select set of devices, based on a selected criteria.

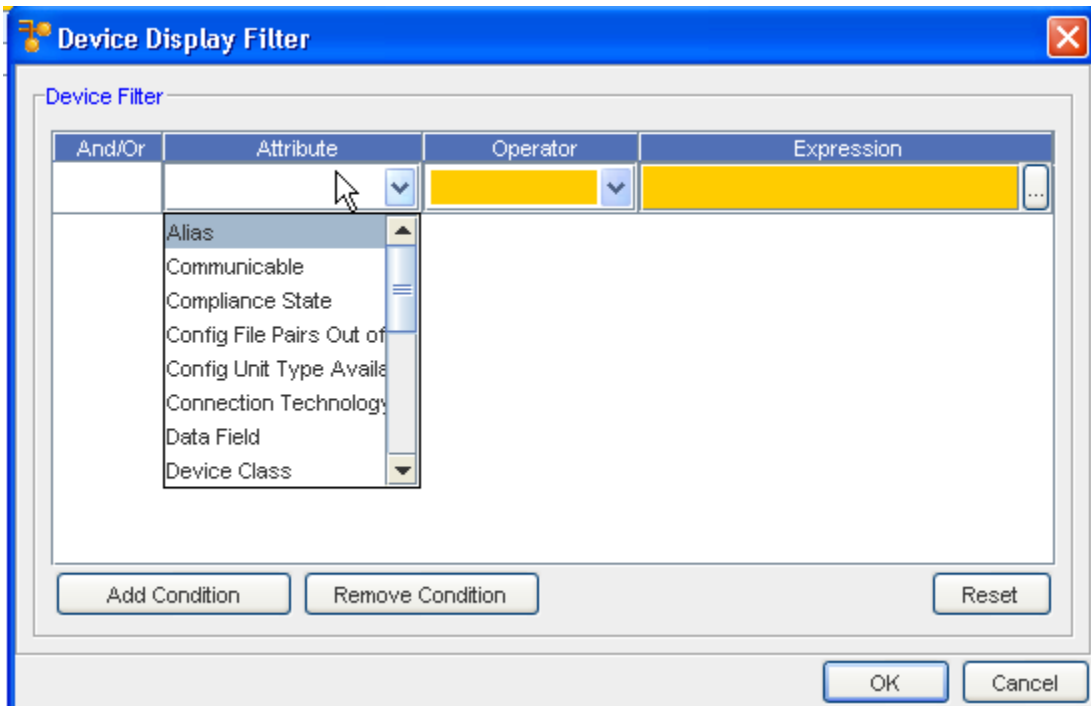
There are four ways you can create filters for devices:

- And/Or
- Selecting the Attribute
- Defining the Operator
- Entering an Expression

1 To Filter devices, select the filter icon ( **Apply**) on the tool bar. The Device Display Filter window opens.

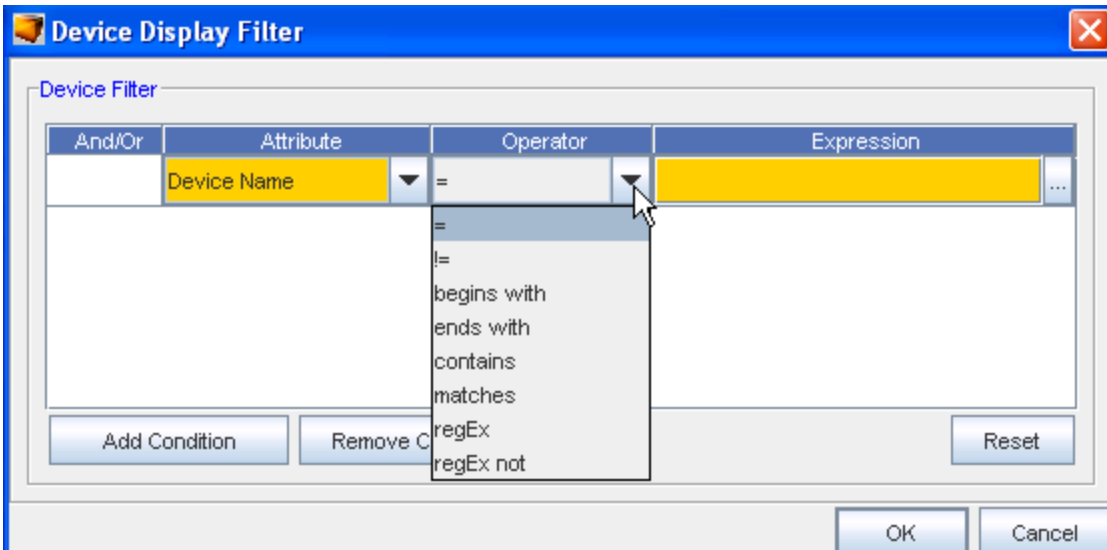


- 2 Select **Add Condition**, then select **And/Or** to allow your filters to be as specific as needed.
- 3 Although you may want to design a workspace with a large number of devices, you may also want to view specific devices based on certain criteria. These criteria are called Attributes. This is the lowest common denominator and cannot be a single filter setting. When an Attribute type is selected, you can enter either an **Operator** and/or an **Expression**. The Attribute options are similar to the following:



**Note** Additional filter attributes have been added that allow the user to create views, based on the Communication State (Communicable), Compliance State, Config File Pairs Out of Sync, and Config Unit Type Availability.

Note that you can select, and then **Remove** an existing condition. You can also select **Reset** to reset all condition selections.

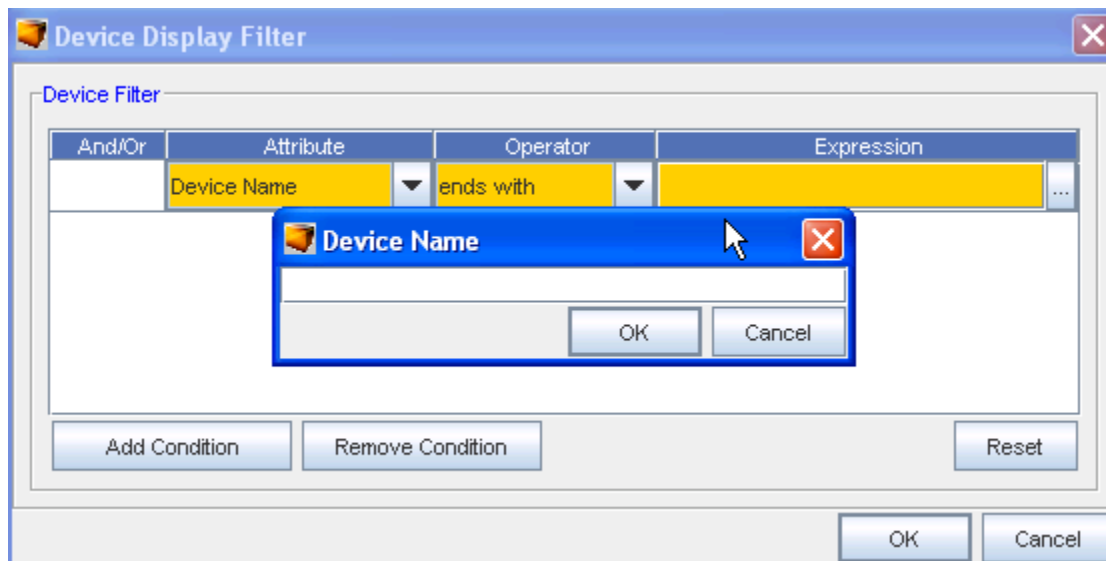


- 4 When configuring attributes, you can use one several options to specify what criteria is generated. For example, you can use one of the following:
  - = refers to the same or equal.

- **begins with** means the attribute begins with the defined expression.
- **ends with** means the attribute ends with the defined expression.
- **contains** means the attribute is include in the defined expression.
- **matches** indicates that your filter should match exactly those attributes you have selected.

**Note** The selections offered in the Operator drop-down depend on what is selected from the Attribute drop-down.

- 5 When the attributes Device Type or Connection Technology is selected, a list of selectable expressions are displayed. You can select either single-select or multi-select these options. The items that you multi-select are OR'ed together in the Expression field.



For all other Attributes, the Expressions field is an editable text field, where you specifically define the criteria. Using the filter settings as described above, allows you to filter the devices that display in the window work area.

- 6 Click **Ok** when you have added your expression.

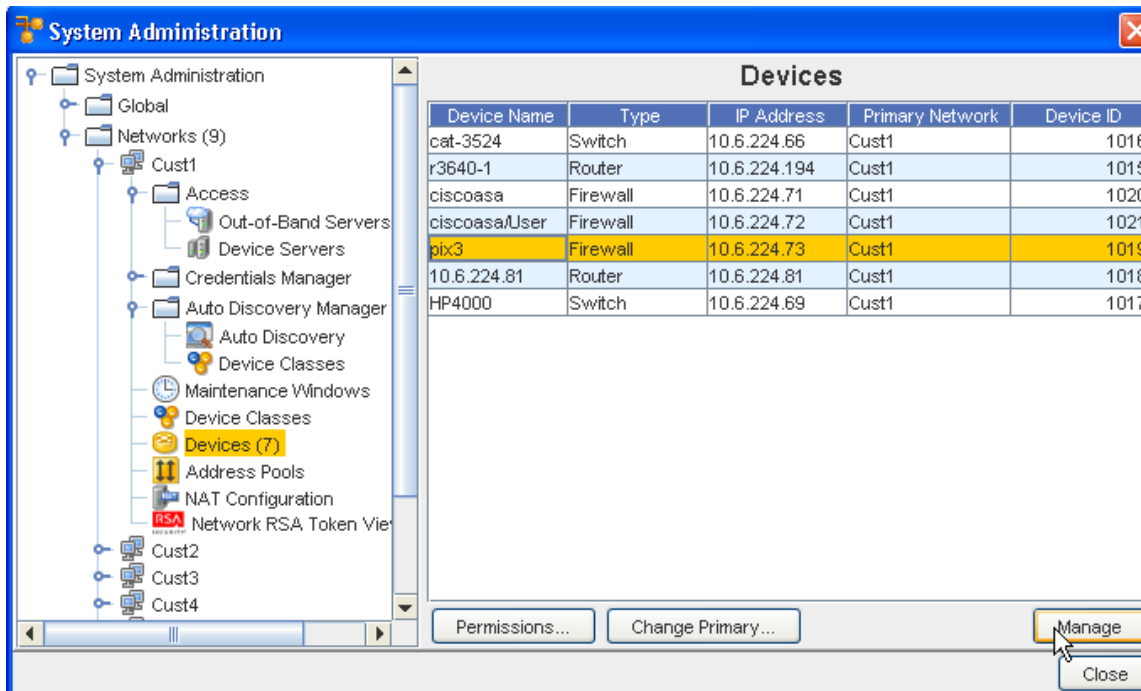
**Important** Use the **Cancel** Button to close this window.

## Deleting a Device

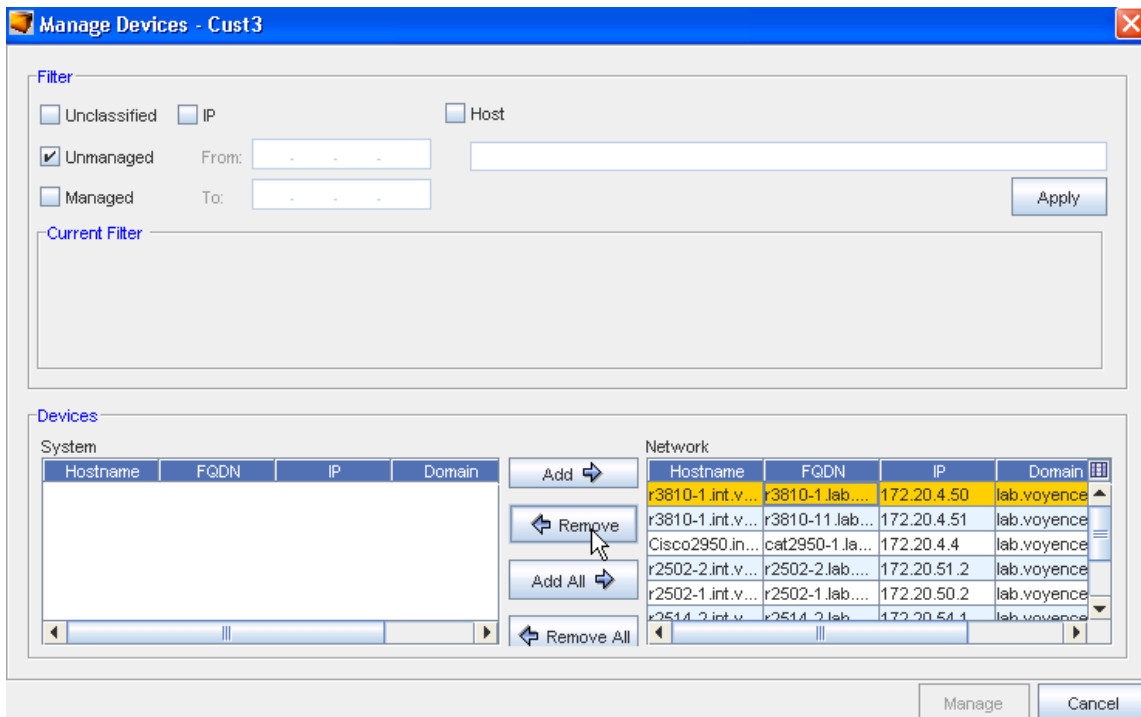
**Important** To delete a device, you must first ensure the device has been unmanaged.

To delete a device,

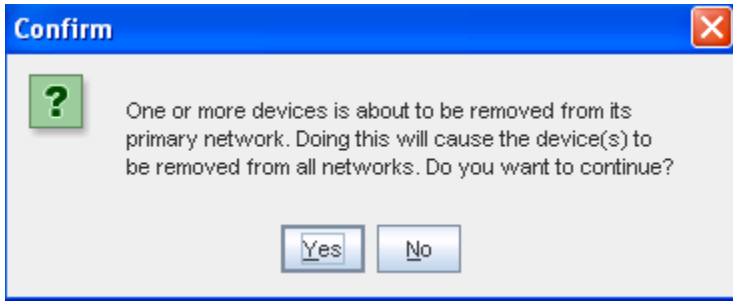
- 1 At the System Administration tool, select **Networks**, then select **Devices**.
- 2 Select the device you want to remove from the list, then click **Manage**.



- 3 Select the **Unclassified** option in the top portion of the window, then click **Apply**. The Device is being retrieved.



- 4 Next, from the bottom **Devices** section, **remove the device** from the Network using the left arrow ( **<-Remove**), moving the device from the Network pane into the System pane.
- 5 Click **Manage**.
- 6 Select **Yes** at the confirmation message to remove the device from its Primary Network.



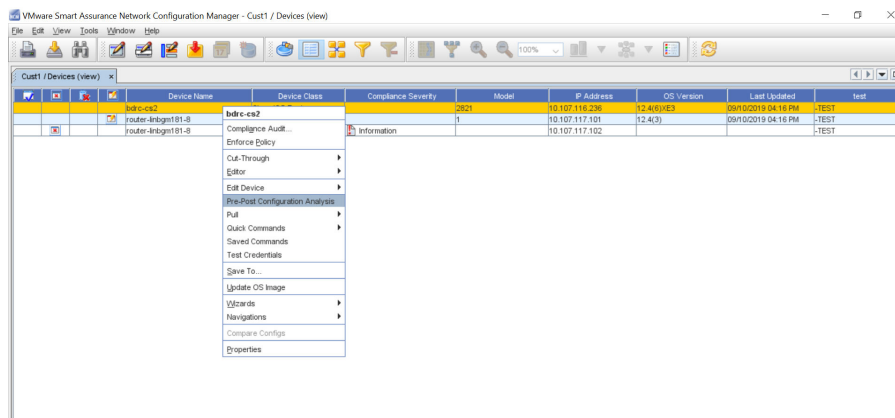
- 7 Next, select **Yes** .
- 8 You can now go to the System Administration tool, and from **Global -> Access select Devices** .
- 9 After selecting the device, click **Unmanage** to change the state of the device to Unmanaged.
- 10 Now that you have placed the device into the **Unmanaged state**, you can remove the device. Once again, select the device from the list, the click **Remove** .

## Using Right-Click Options

### Right-Click Menu Options Overview

The right-click feature in a **Devices view** (when the view is shown in a Table format) provides access to the following links. You can also access the same options when you right-click a device in the Diagram format.

Using these links allows you to complete a number of tasks, and view a great deal of device information.



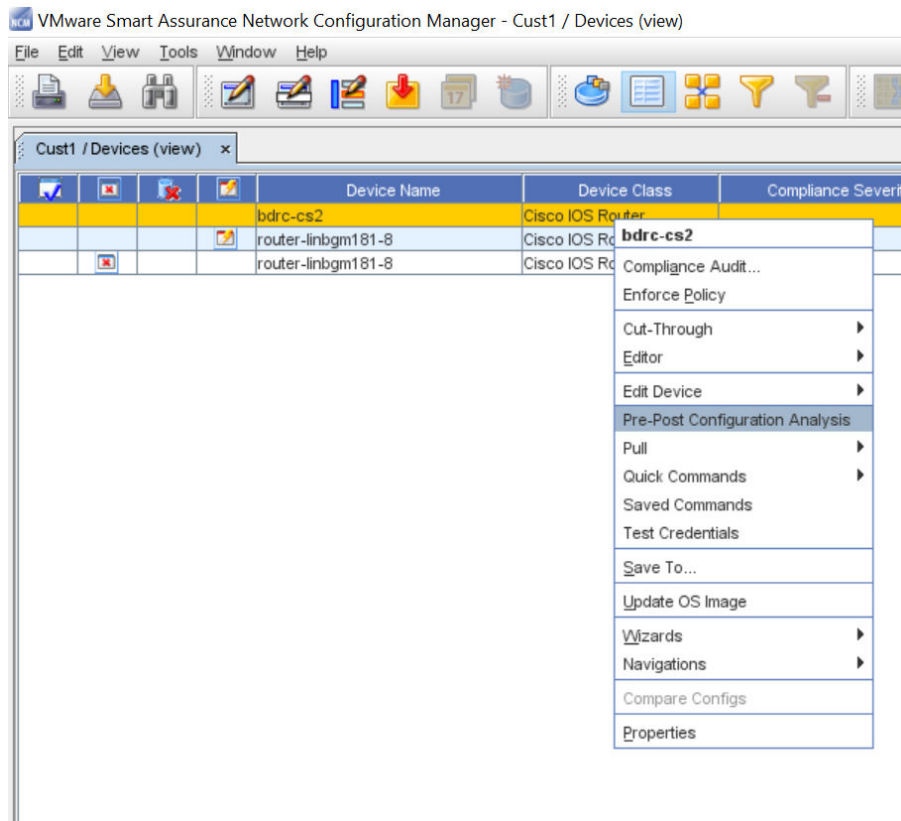
### Important Information!!

You must have the appropriate permissions to successfully complete some specific tasks you can access from the Devices View right-click menu options.

For example, in Cut-Through (In-Bound and Out-of-Bound), Quick Commands and Saved Commands, you are required to respond and correctly enter the appropriate information in the Job Credentials Input pop-up screen when this screen is displayed to continue to complete the selected task. See your System Administrator for more information.

**Note** Any task that is not accessible to you from the right-click options listing (appears dimmed), and automatically lets you know that you do not have the appropriate permissions to complete that task, or that you have not made a correct selection (as in Compare Configs - you must select two devices from the list).

You can also use the right-click menu in the Navigation tree . You can select any device within the Network, and right-click to display the options.



Access each link to get more information on the tasks you can complete.

- [Compliance Audit](#)
- [Enforce Policy](#)
- [Cut-Through](#)
- [Editor](#)
- [Edit Device](#)
- [Pull \(Immediately\)](#)
- [Using Quick Commands](#)

- Using Saved Commands
- Test Credentials
- Updating OS Images
- Wizard Overview
- Navigations
- Compare Configs
- Compare Configs
- Device Properties Tabs(when applicable)

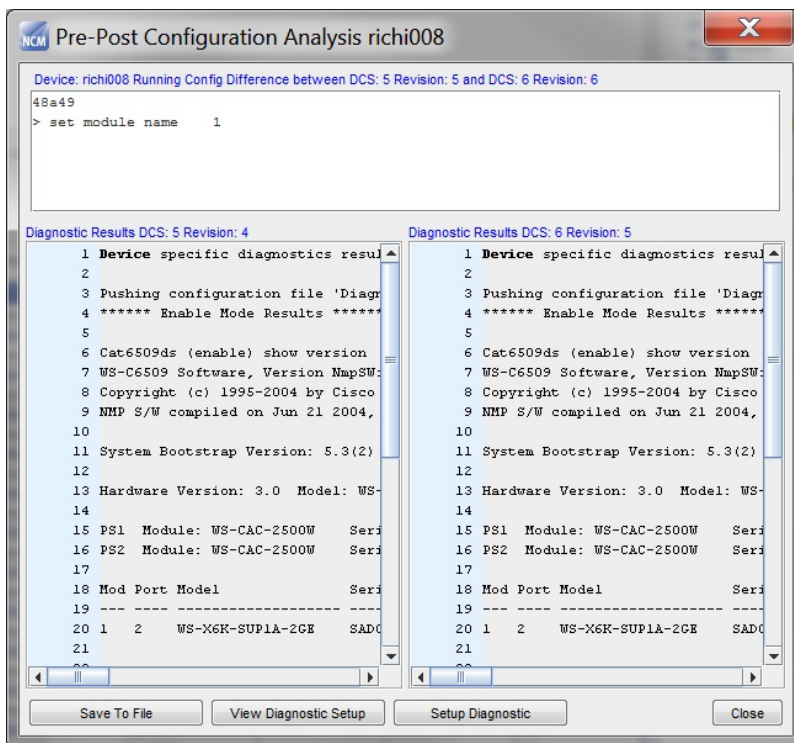
### Pre-Post Configuration Analysis

Network administrators may use the **Diagnostic Utility** to:

- Validate configuration changes made to a device.
- Create a report which functions as a proof of changes made to devices. You can download the comprehensive report which details the diagnostic results and differences between current and previous configuration revisions.

To generate a report:

- 1 Select **Pre-Post Configuration Analysis**. A comprehensive report displays.



- 2 You may perform these operations:

- Save to File (saves the results of the diagnostics to a Microsoft XLS file)



- View Diagnostic Setup
- Diagnostic Setup

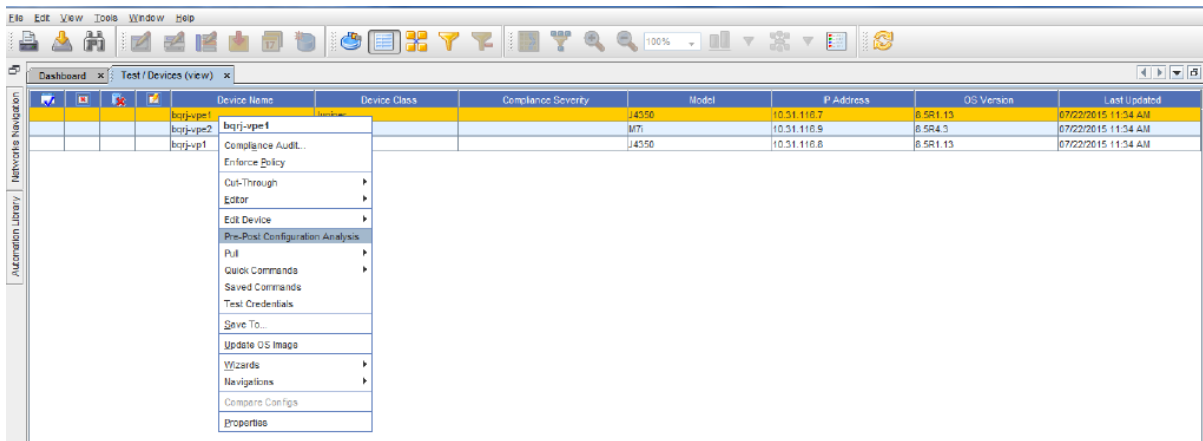
## Compliance Audit

The Compliance Audit tool allows you to **create standards and tests used to compare with configured devices** . Devices that are out-of-compliance are not configured correctly, and must be put into compliance using this tool.

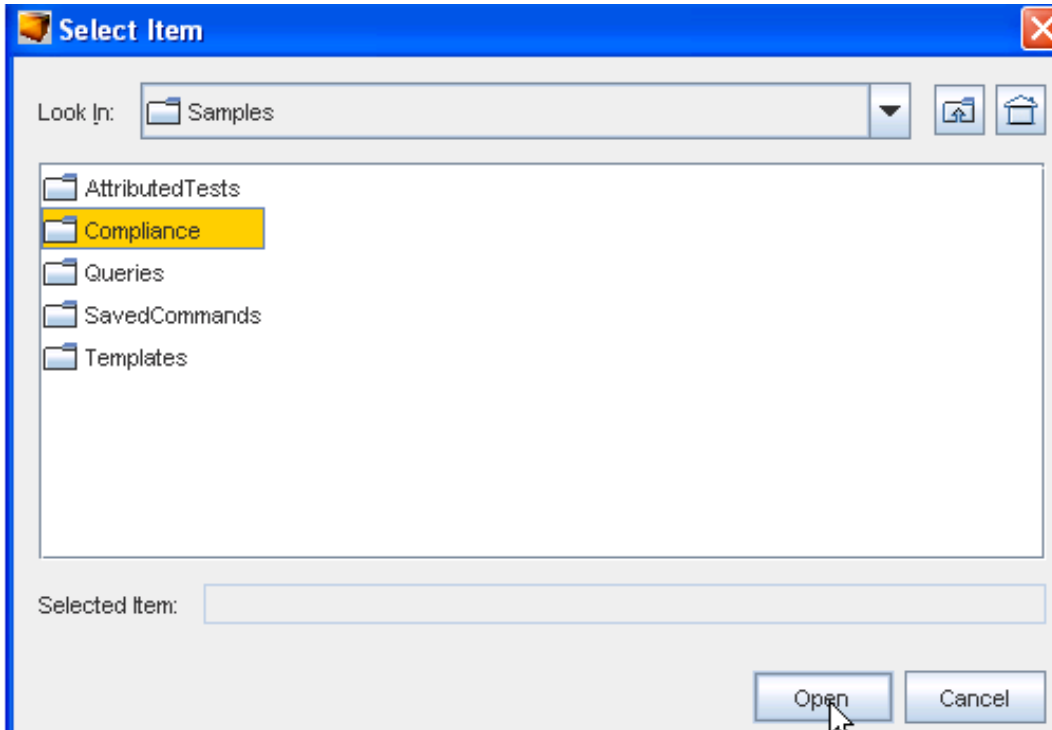
**Note** Compliance Audit can be executed on one or more devices.

From the right-click menu in the Devices View, you can access the **Compliance Audit** tool for any device that is in the out-of-compliance state.

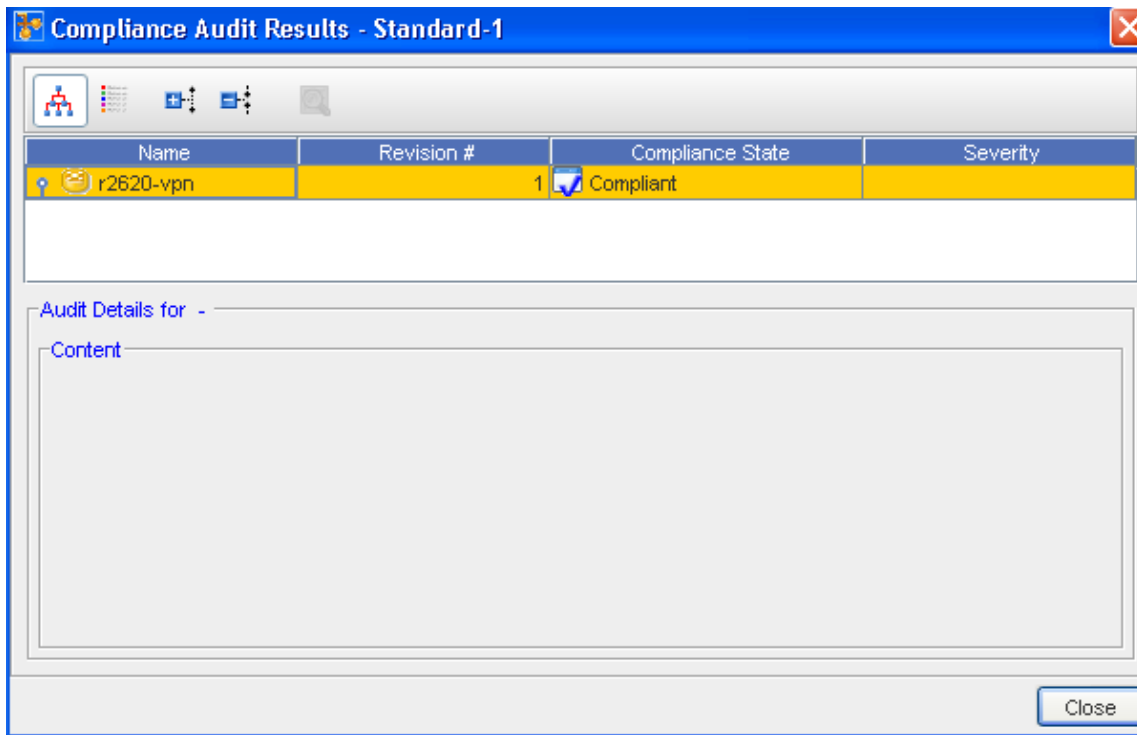
- 1 In the Device View, select **one or more devices**, then right-click to get the Device options.
- 2 Select **Compliance Audit** from the menu.



- 3 The Select Item window opens. From here, select the **Location**, then select the **item**.



4 After making your selection, click **Open**. The Compliance Audit Results window opens.



As you can see in the above example, the state for the device selected is **Non-Compliant**. The lower section (Audit Details) allows you to view the details of the audit results if needed.

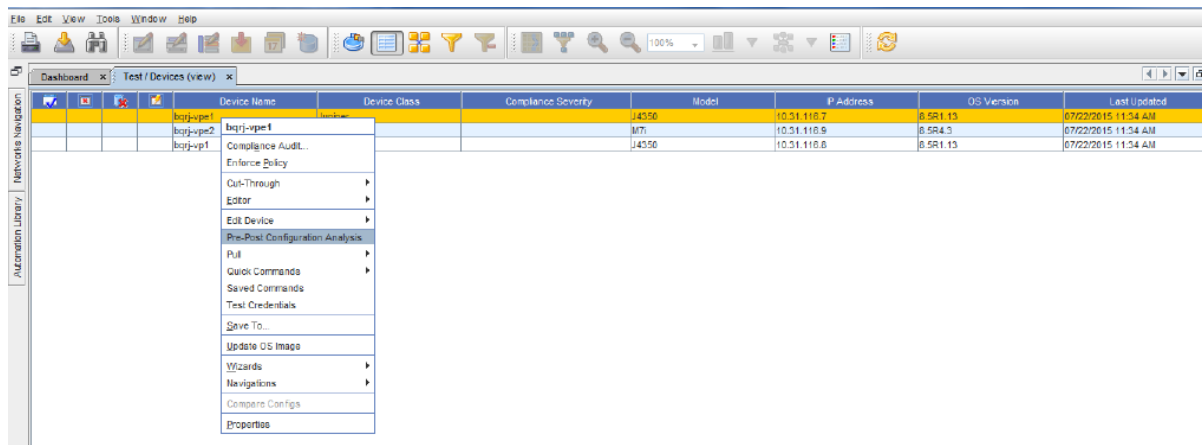
The icons located in the top left allow for the following:

- View in tree format
- View in a list
- Expand the selected view
- Collapse the selected view
- View the results of a selected device

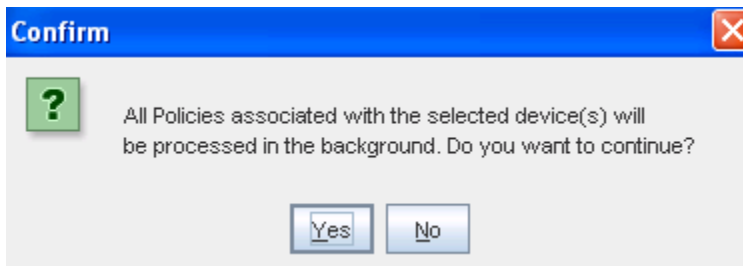
## Enforce Policy

From the Devices View, you can right-click on a device, then go through the steps needed to enforce a previously defined policy on that specific device.

**Enforce Policy** allows you to take a policy and **immediately** apply it against one device, or an entire group of devices. When Enforce Policy is selected, every other policy associated with that device is also enforced.



- 1 Select **one or more devices** from the Devices view.
- 2 Right-click, and select **Enforce Policy** from the options. A confirmation message displays.



- 3 If **Yes** is selected, all policies are then loaded, and enforcement is completed in the background. Click **Yes** to continue, or click **No** to stop the processing.

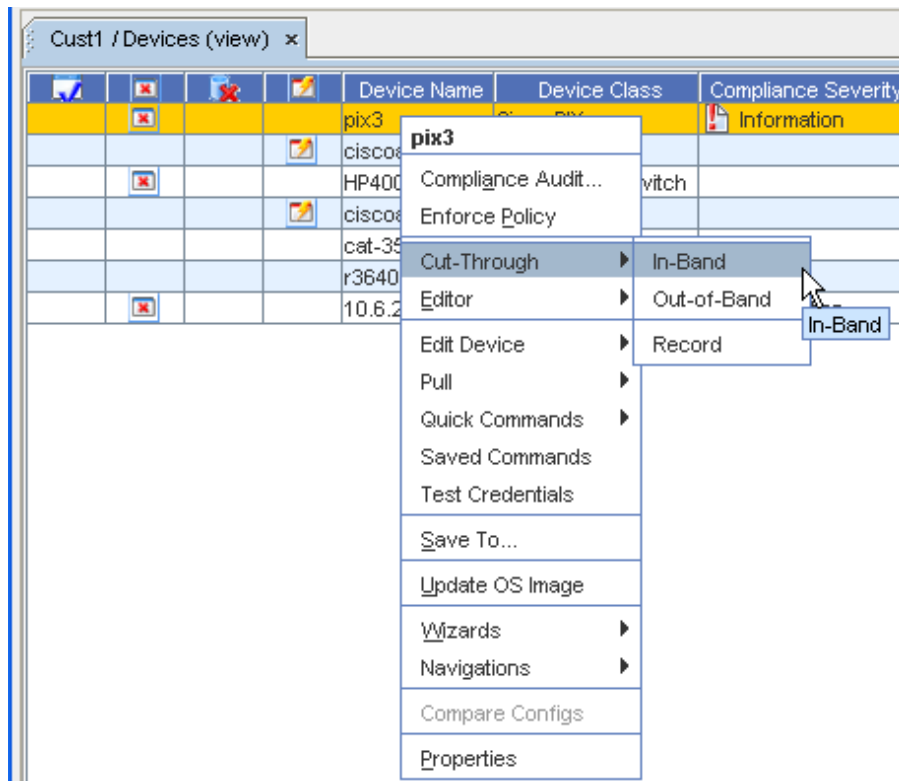
**Note** Devices are flagged as to their policy status (in or out-of-Policy). You can remove the device status (or state) flags. For example, if you prefer not to see any non-compliant flags for devices (for any reason). Go to [Clearing Device Flags](#) for more information and instructions.

## Cut-Through

The Device cut-through allows you to create a secure, 128-bit encrypted connection tunnel to a device. The secure tunnel uses a single port pair from client through application sever, and device server to the end device.

For most clients, you can establish which Telnet client you want to execute, such as PuTTY, CRT, or Secure\_CRT. Cut-through also supports creating recorded Save Commands.

From the right-click menu in the Devices View (either diagram or table format), you can access the Cut-through menu.



- 1 Select **one or more devices** from the devices listing that you want to complete a cut-through on, then **right-click** to get the right-click menu.
- 2 From the right-click menu options, select **Cut-Through**, then select a cut-through option.

From this option, you can select In-Band, Out-of-Band, or Record to work with device properties.

---

**Note** Any task that is not accessible to you from the right-click options listing (appears dimmed), automatically lets you know that you do not have the appropriate permissions to complete that task .

---

### In-Band

When the In-Band option is selected, the In-Band communications is established, and a Telnet session is opened where you can make needed changes or enter information. Notice that this is a **secure site** , and you must have permission to work within this feature.

From this session, you are communicating directly with the device , and can issue and execute commands to the device.

### Out-Of-Band

When the Out-of-Band option is selected, the Out-of-Band communications is established, and a Telnet session is opened where you can make needed changes or enter information. Notice that this is a **secure site** , and you must have permission to work within this feature.

From this session, you are communicating directly with the device, and can issue and execute commands to the device.

### Record

The recorder window displays behind the cut-through session. Recordings can be paused, saved, resumed, or cancelled during the cut-through session.

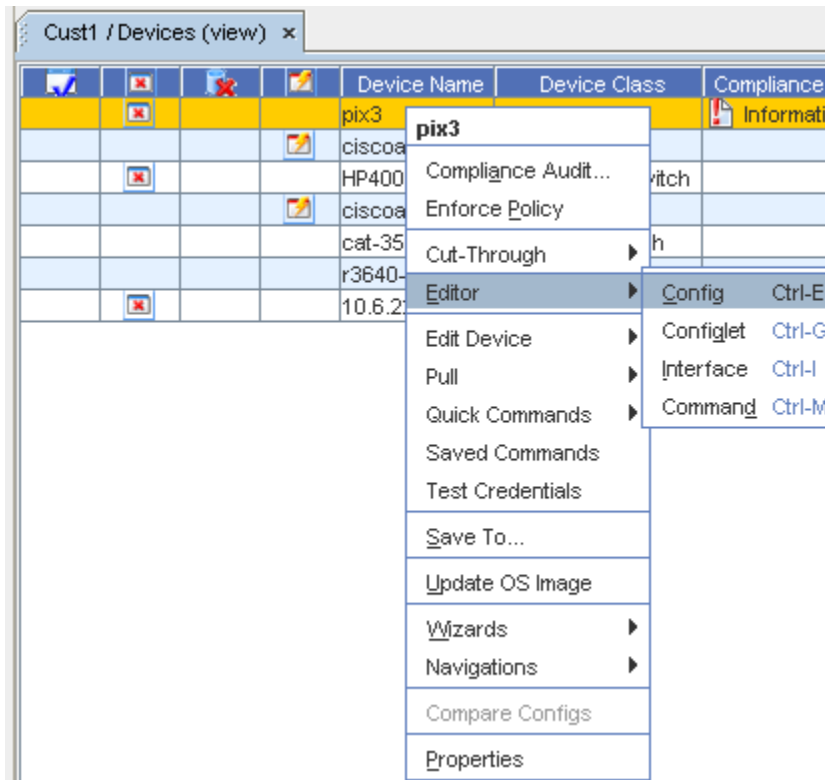
When this option is selected, you can determine if you want to select either the In-Band or Out-of-Band session for recording. This is used to automatically record, and then alert users to run tasks, or to follow instructions. What you enter into the window is automatically copied into another window, and is then recorded (much like a tape or VCR recording), and can be played back as directed.

- Recorded sessions saved in the Automation Library can be edited, moved, and copied from within the Automation Library.
- Recorded sessions can be executed and scheduled as Saved Commands.

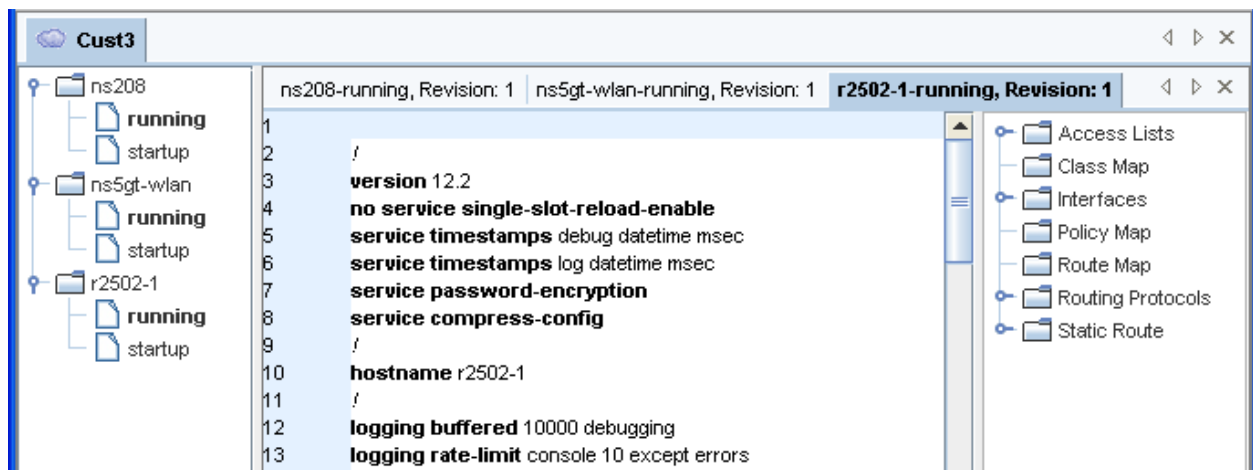
### Editor

From this selection in the Devices View right-click menu options, you can access any one of the four editors.

- 1 Select **one or more devices** from the view.



2 Next, right-click, and select **Editor** from the listing. In this example, **Config** was selected.



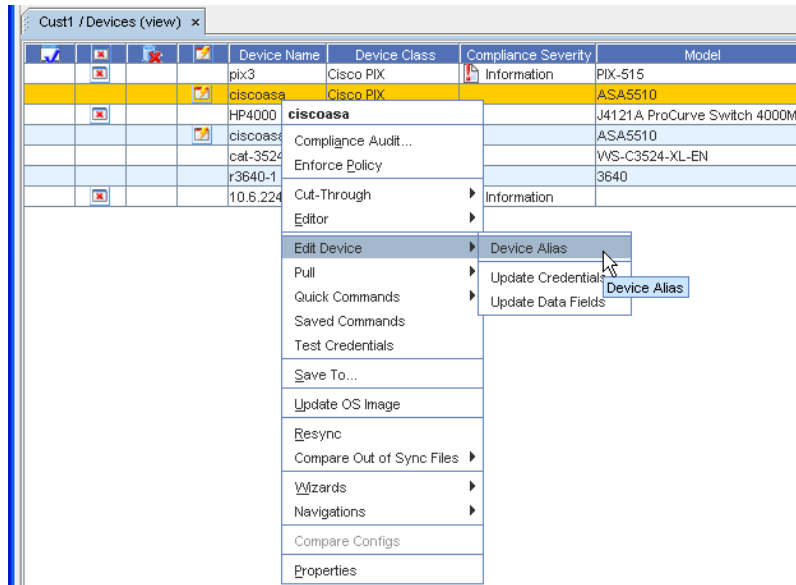
You can now view the results of each device , using the separate device-named tabs that run along the top. You can also expand or collapse the device information displayed using the list in the left .

**Important** The listing on the **right** can be expanded to view additional information associated to the selected device.

For more information, see [Editors Overview](#).

## Edit Device

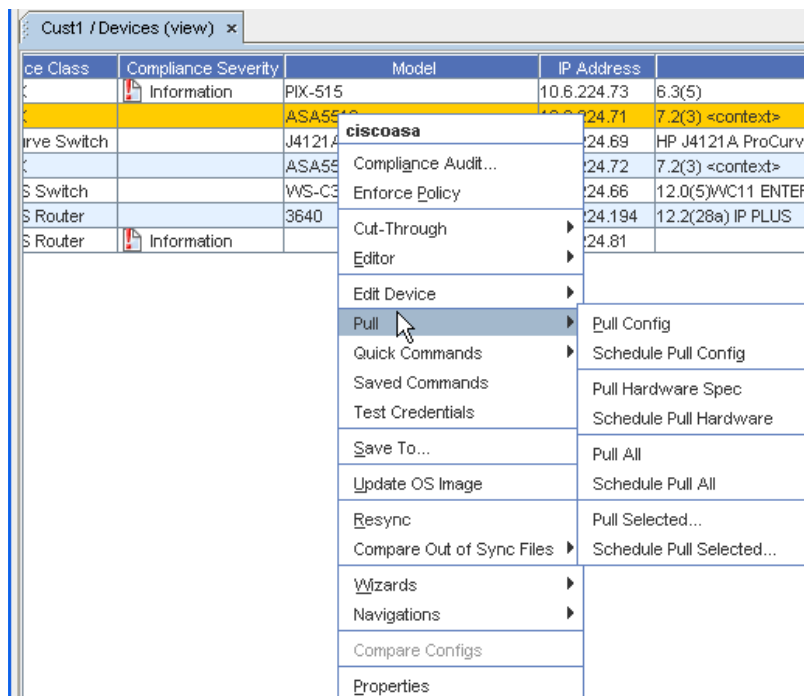
When using the right-click menu in the Devices View (either table or diagram layout), you can edit a device or update credentials by accessing either the Update Credentials window, or the Update Data Fields widow.



### Pull (Immediately)

While viewing the Devices in either the Table or Diagram view, you can use the right-click feature to access a selection of **Pull** and **Schedule** options, including **Pull the Configuration** , or **Pull the Hardware Spec** (for a device immediately).

You can also use the option to go through the Schedule Manager, and then schedule the pull.



## Using Quick Commands

Quick Commands allow you quick access to standard diagnostic tools. Quick Commands are executed immediately, and the results are displayed in a separate window. Some Quick Commands can be executed across device classes. You can create additional Quick Commands through DASL scripting.

The **Quick Commands** option allows you to access quick commands, including Ping, Trace route, assorted Views, and more!

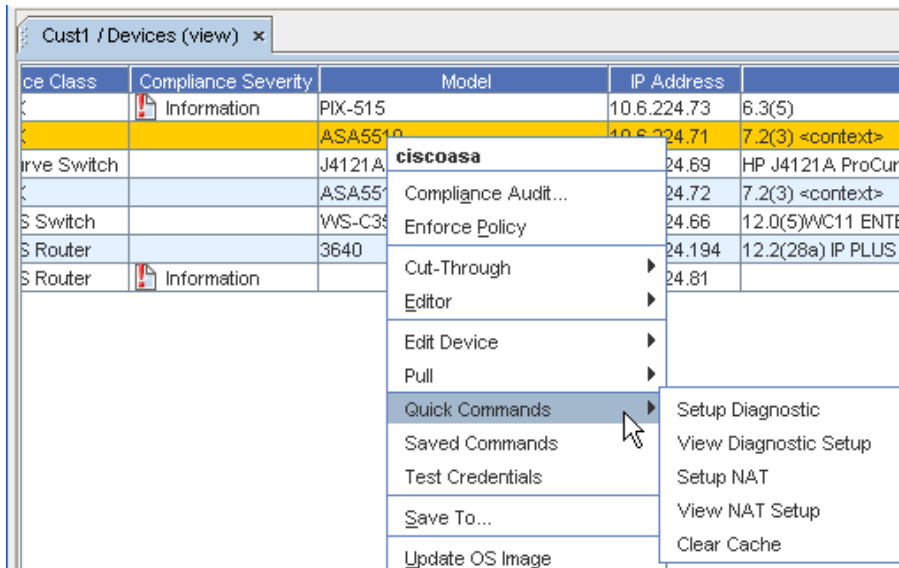
Quick Commands can be used with the following views:

- Devices
- Sites
- Workspaces

**Note** Any task that is not accessible to you from the right-click options listing (appears dimmed), automatically lets you know that you do not have the appropriate permissions to complete that task.

To access Quick Commands from Devices,

- 1 Expand **Devices** in the navigation pane to show the **Devices view** in table format.
- 2 Right-click to get the drop-down menu. You can also right-click on the device in the Diagram view.
- 3 From this menu, select **Quick Commands**.

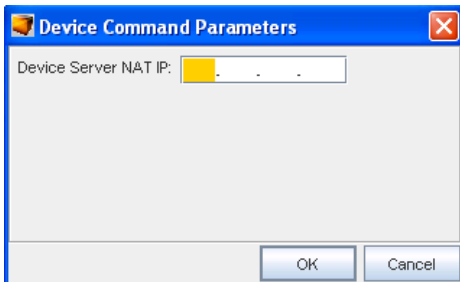


Quick Commands differ based on the device.

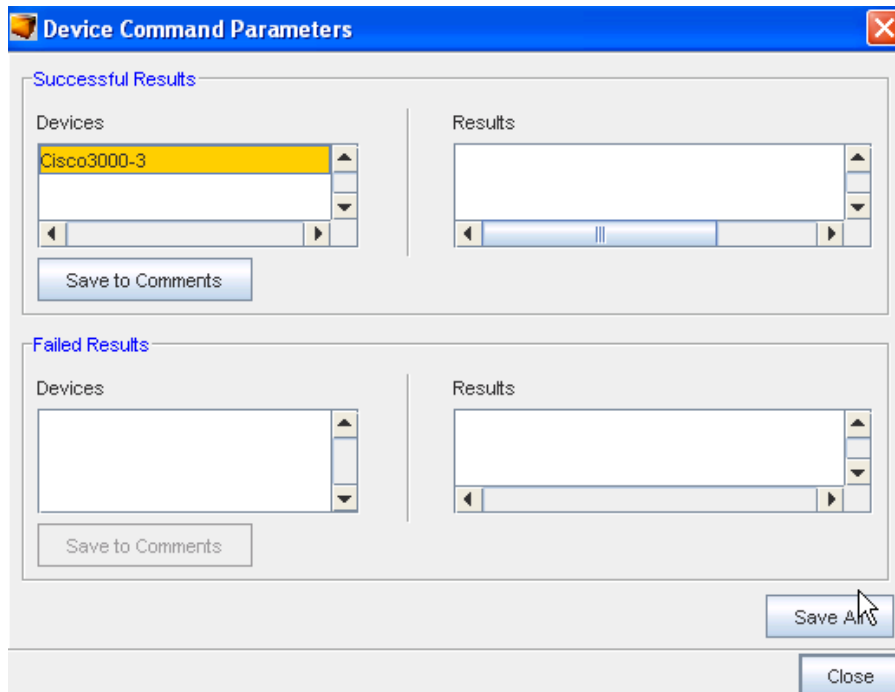
**Important** Some quick commands can only be executed if the devices are first set up with device credentials.



- When a command is selected, if there are command parameters needed to execute this command, you must include the parameter information in the **Device Command Parameters** window. If parameters do not need to be defined to execute this command, the command automatically executes.



- After entering the Device Command Parameters, click **Ok** , and the command executes. Results of the quick command are detailed. From this window you can **Save All** .
- After saving the quick command results, click **Close**.



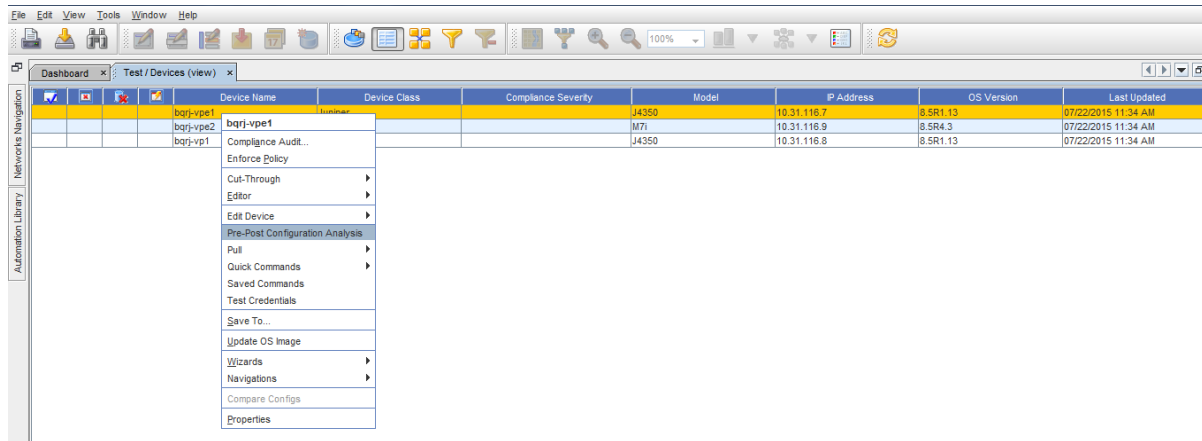
## Using Saved Commands

Saved Commands can be created within the Automation Library, or through recorded cut-through sessions. Save Commands selected can be executed immediately, and can have the results displayed.

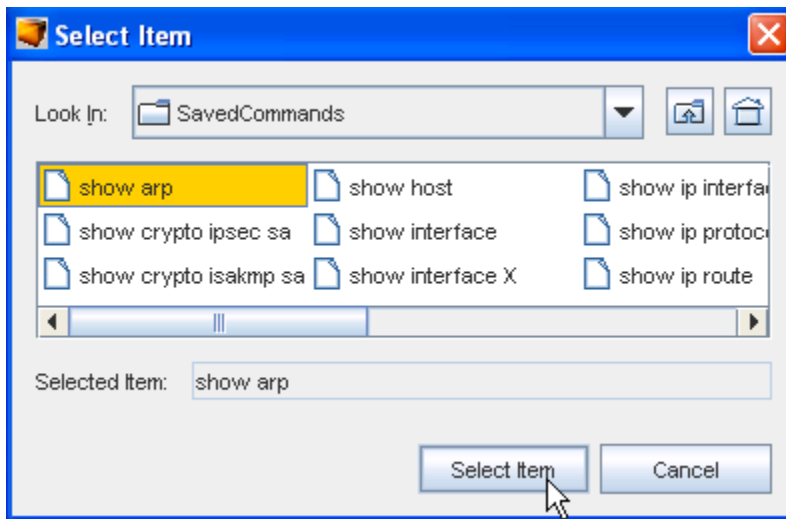
The Saved Command option allows you to **access saved commands** you have previously created, and **execute those commands** immediately.

**Note** Any task that is not accessible to you from the right-click options listing (appears dimmed), automatically lets you know that you do not have the appropriate permissions to complete that task.

From the Devices View (in either the table or diagram format), you can access Saved Commands using the right-click feature.



- 1 From this window, use the drop-down arrow to select where you want to **Look In** to see any saved commands you may want to use.
- 2 Click **Select Item** when you have made your selection.
- 3 Next, click **Open**. The Saved Command is now executing.



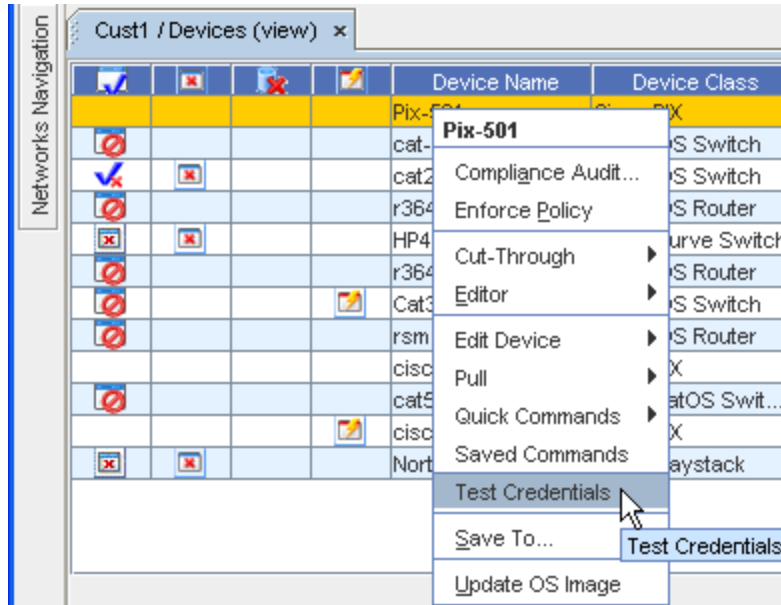
The **Device Command Parameters** window is displayed for you to see if the command executed successfully, and where you can save the Results.

4 Click **Save All** to save these results, then click **Close**.

For more information on Save Commands, see [Creating a Command](#).

## Test Credentials

This option of the right-click menu allows you to run a test (schedule a Push job) on the credentials for that specific device.



When Test Credentials is selected from the Devices View right-click menu, the Schedule Push Job window opens. See [Scheduled Push Job](#) for more details.

## Updating OS Images

From the Update window you can select each device to be updated, select the target location for the image, determine if there is adequate space for the upgrade, and set the device, memory, and partition preferences.

OS updates are scheduled in the same manner as any other job - through the Scheduler.

### Prerequisites to Updating OS Images

Prior to updating the OS Image you must ensure the following tasks have been completed:

- [File Servers Overview](#)
- [Adding OS \(Image\) Inventory](#)

---

**Important** Ensure that the File System information displayed in the [Device OS information](#) section is the most current information for the devices (as shown in the Last Hardware Pulled Time section, and from the Device Partition Information - see the following graphic).

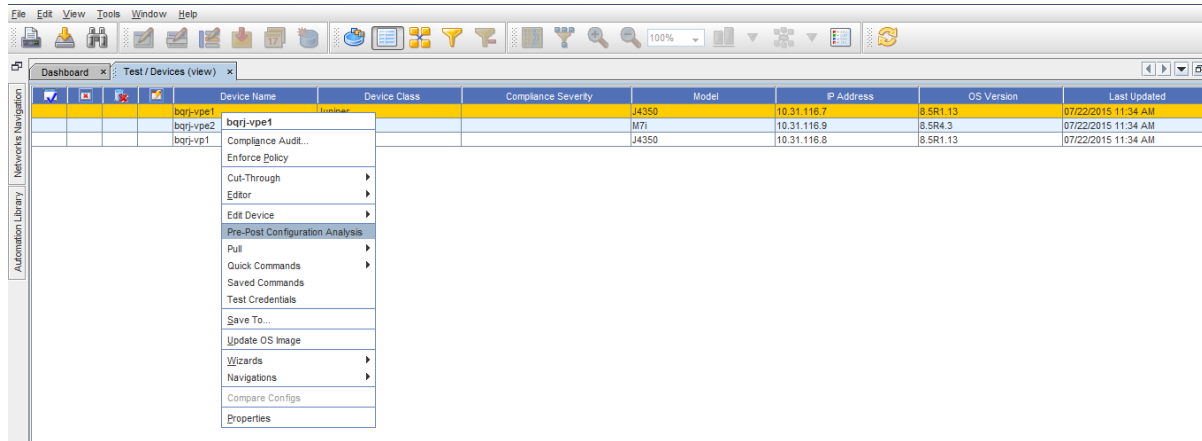
---

If the most current information is not displayed, you can complete a Hardware Pull on the devices. Go to the Devices View, and right-click to get to the [Pull option](#), then select Pull Hardware Spec from the options list.

To update the OS Image,

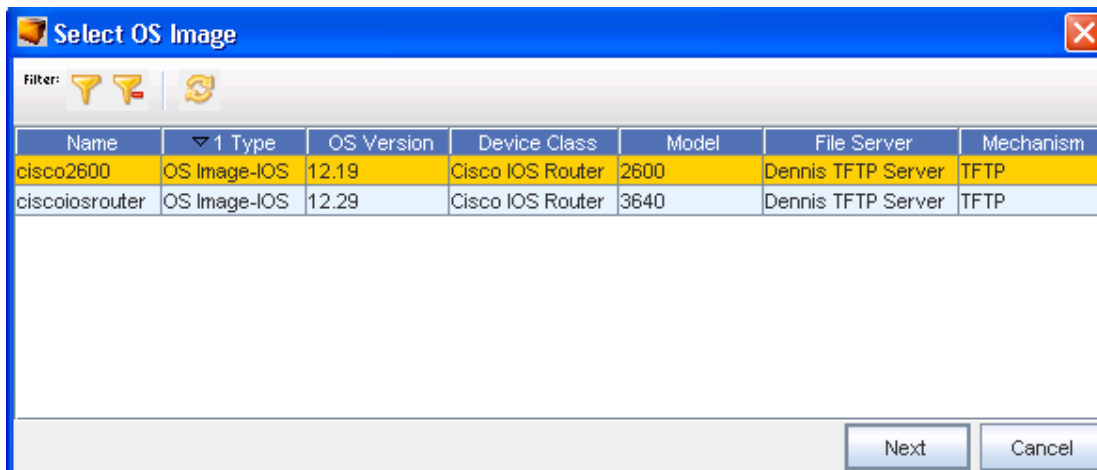
The Update OS Image option allows you to **replace** the device's current OS Image.

From the Devices View (in either the table or diagram format), you can access the Select OS Image window to update the OS image for the device.

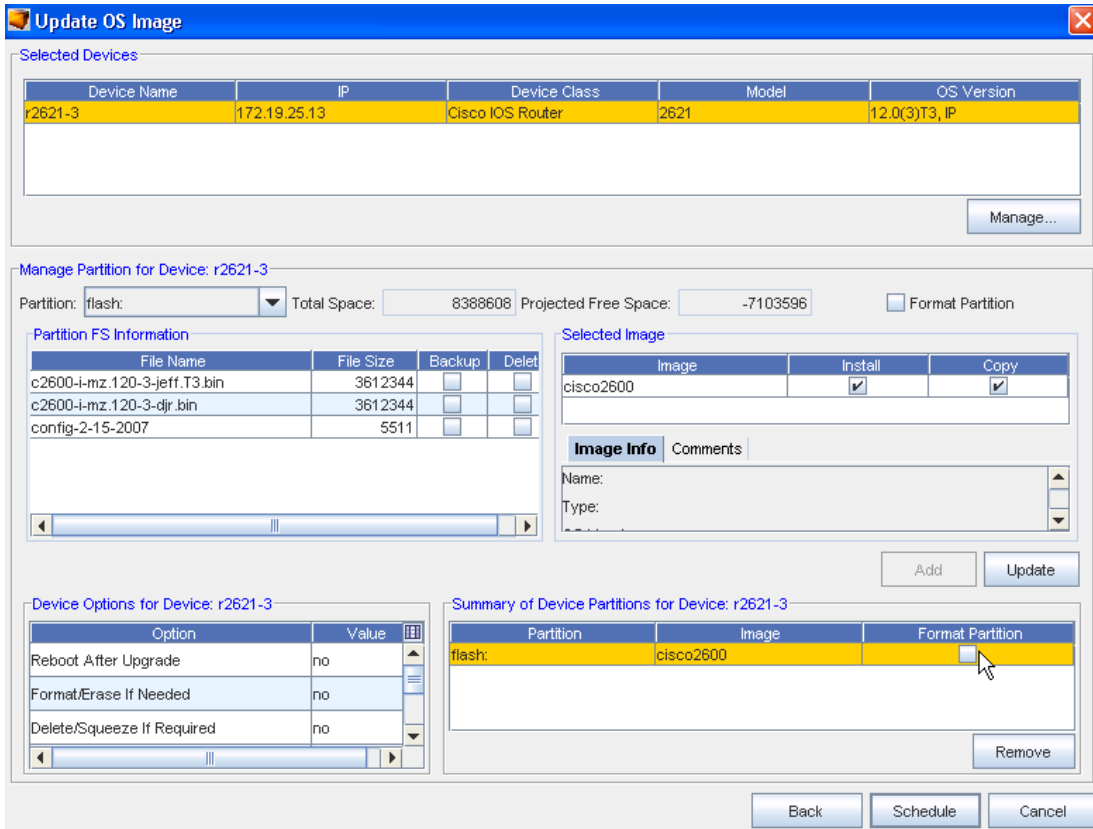


**Device (or a number of devices)** from the listing of devices, then right-click to see the menu.

- 1 From the menu, select **Update OS Image**.
- 2 From the Select OS image window, select any **existing OS Image** . You can also create a new OS Image (if needed).

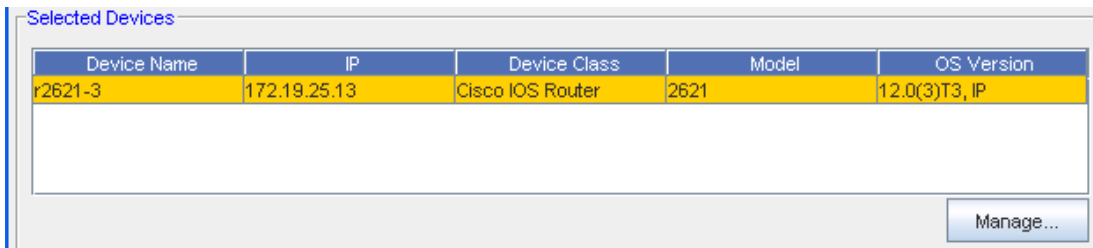


- 3 Click **Next**. The Update OS Image window is displayed. You may get an informational message, inquiring if you want to continue. Click **Yes** if appropriate. Note that there are three sections to this window.



4 At the first section, you can view the **Selected Devices** , and the information for that device.

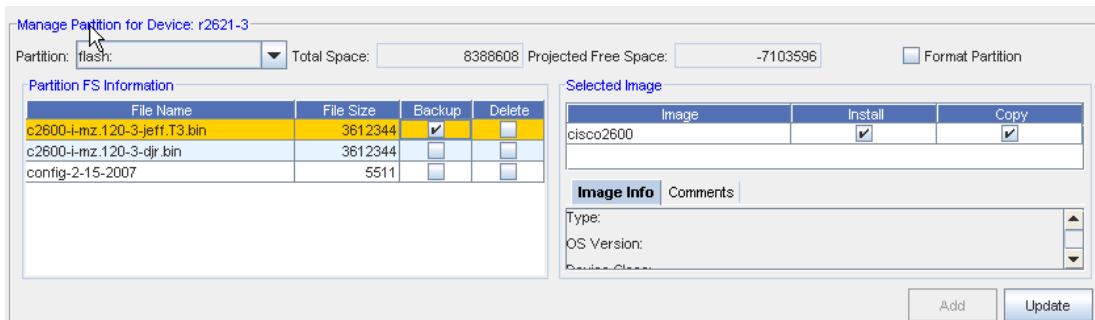
**Note** From this window you can also click **Manage** to see a listing of devices to add more devices to the Selected Device list (from the Update Device).



5 If more than one device was selected (from the Devices View) and is displayed, select a **Device** from the list.

6 In the next area ( **Manage Partition for Device:**) there are several steps that need to be completed.

- In the Partition section, either accept the **default Partition** , or click the drop-down arrow to select another Partition. This area of the window also shows the Space; both Total and Projected Free. Note that you can select to Format the selected Partition if needed from this area. If you select to Format the Partition, you will start with a clean partition and all the available free space.
- To force a format of the partition during the OS upgrade, click within the **Format Partition** check box.



**Important!!** If you select the Format Partition, you will lose all data on the specific partition of the device.

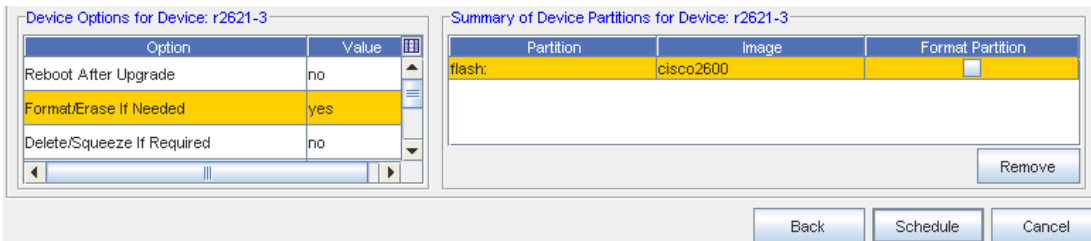
**Important** Do not use a partition where there is insufficient Projected Free Space for the OS Image. The Image size is noted in the Image Info tab.

- From the **Partition FS (file system) Information** section, you can determine if you want to **Backup** or **Delete** existing files. If Backup is selected, these files will be backed up before the new OS Image is installed. If you select to Delete these files, they will be deleted before the new OS Image is installed.
- To add a selection from this partition information, first select the File Name from the list, then click **Add**. This adds the information into the Summary section (at the bottom of the window).

**Note** To ensure that the displayed information contained within the Partition FS Information section is the most current information, complete a Hardware Pull on the device. Go to the Devices View and right-click to get to the Pull option, then select Hardware Spec pull from the options list.

- At the **Selected Image part** , you can select the OS Image by **clicking on the image name** , and see the Image Info and Comments tab. This information and the comments were created when the OS image was created. Once the Image is selected, the **Image Info** and **Comments** tabs are displayed. Use the scroll bars to go to the top and bottom of the **Image Info** data. Click the **Comments** tab to view any comments previously recorded.

- 7 Once you have determined the Partition, Partition FS Information, and the Selected Image, click **Add**. This ensures that the OS image is now added and designated as the **Selected Image**. The selected image is now shown in the last portion of the Update OS Image window. The **Update** button is used if you make changes to the **Install or Copy check boxes** in the OS Image section, or if you decide to use the **Format Partition checkbox** (and force a partition) in the Partition section. Once changes to existing selections are made, click **Update** to make sure the current selections are used.



- 8 At the **Device Options for device:** section you can view the options, and then make any changes to the Value if needed. Click within the **Value** column to see and select options.

**Note** Some Device Options (in the Option section) may vary from Device Class to Device Class. For example, the following options are currently supported for CISCO IOS Routers and CISCO IOS Switches, but not supported for Juniper Device Classes.

Option	Meaning
Reboot after upgrade	This reboots/reload the device at the end of the OS Image upgrade process.
Format/Erase If Needed	<p>If yes is selected, this option allows Verifying Installation. After the installer completes, you can verify the installation (if desired) by completing the following steps:</p> <ul style="list-style-type: none"> <li>From any Network Node Manager sub-map window, select Tools. You should see a Network Configuration Manager menu item.</li> <li>From any Network Node Manager sub-map window, select Tools-&gt;SNMP MIB Browser. Then double-click Private and Enterprises. You should see voyence listed.</li> <li>From any Network Node Manager sub-map window, select Options-&gt;Event Configuration. You should see voyence (Enterprise ID .1.3.6.1.4.1.6615) listed in the Enterprise Identification window. (You may need to scroll through the window.) Selecting voyence populates the Event Identification window with all the Network Configuration Manager events.</li> <li>From the Event Configuration window, complete the following: Network Configuration Manager to reformat the partition to create more free space (if needed).</li> </ul> <p><b>Note</b> If the Format Partition check box is checked, the partition will always automatically be formatted, whether you select Yes or No as the value for this option.</p>
Delete/Squeeze If Required	If yes is selected, this option allows Voyence to delete and squeeze the partition to create more free space (if needed).

Option	Meaning
Delete Old Image After Upgrade	This deletes the old OS Image from the device partition.
Backup Current Image	This backs up the current OS Image to the Network Configuration Manager Device Server directory (\$VOYENCE_HOME/data/devserver/cm/devxfr) before the OS Image upgrade process begins.

**Note** Specifically for CISCO IOS Class B and Class C devices are supported.

**Supported Options for Compacting CISCO IOS Non-Volatile Memory:**

**Class A** - squeeze/format <partition> - Delete/Squeeze If Required or Format/Erase If Needed

**Class B** - erase <partition> - Format/Erase If Needed

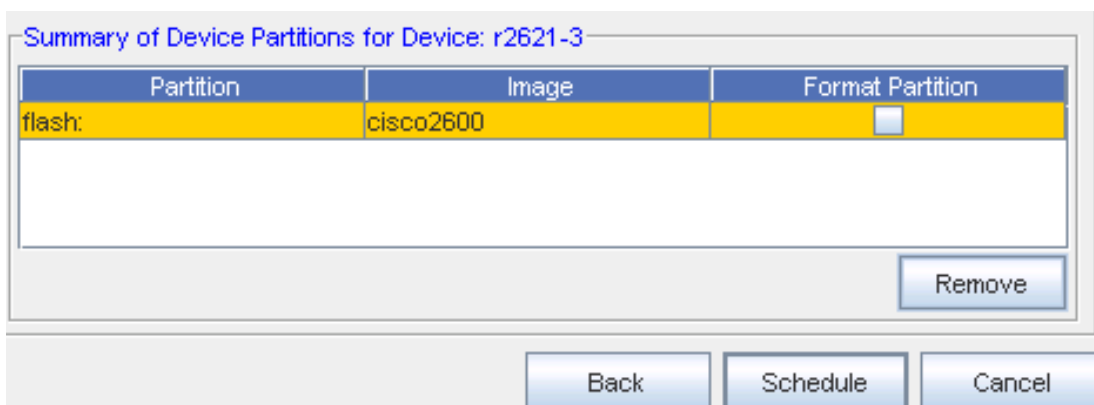
**Class C** - format <partition> - Format/Erase If Needed

If there is not enough free space available, and you have not checked the Format Partition check box, but you want Network Configuration Manager to free the space needed, select the **Format/Erase** option, or the OS Image upgrade will fail.

At the **Summary of Device Partition for Device** section, this information automatically displays a summary of the selections made for this device, after the Add or Update button has been selected. From this section, you can also Add or Remove partitions, and the eventual ending information is once again displayed within the Summary section.

To change the information contained with the Summary section, begin again from the **Selected Devices** section of the window, and then re-select options, then click **Update**. These new selections (options) are now displayed in the Summary section.

**Note** In the Partition section of the **Summary of Device Partitions** (for a specific device) there may be more than one default, however, the highest priority of the default is displayed. For example, the highest priority default for CISCO IOS devices is flash.





You can select information within the Summary section, then click **Remove** to completely remove any updates to a partition on a device. This removes the partition from the Summary listing, as well as from the Partition FS section.

- You can also use the **Back** button to return to the previous screen to begin the process again by selecting a different OS Image.
  - If you previously checked the **Format Partitions** check box, the check is also displayed as checked in this Summary section.
- 9 With all the selections made from this window, you can now click **Schedule** to schedule this OS Image Upgrade (Schedule a Push Job).

## Resyncing Devices

While viewing the Devices in either the Table or Diagram view, you are alerted (by the out-of-sync icon in the State column) that you have devices that are out-of-sync. This indicates that the running configuration for a specific device is not "in sync" with the saved device configuration, and should be **brought back into sync** to preserve the running configuration when the application is rebooted.

There are three ways to get the device back "into sync":

- Using the **Resync** button provided in the Device Properties
- Using the **Schedule Manager** to complete a config pull
- Using the option in the **Devices View right-click** menu

---


**Note** Any task that is not accessible to you from the right-click options listing (appears dimmed), automatically lets you know that you do not have the appropriate permissions to complete that task.

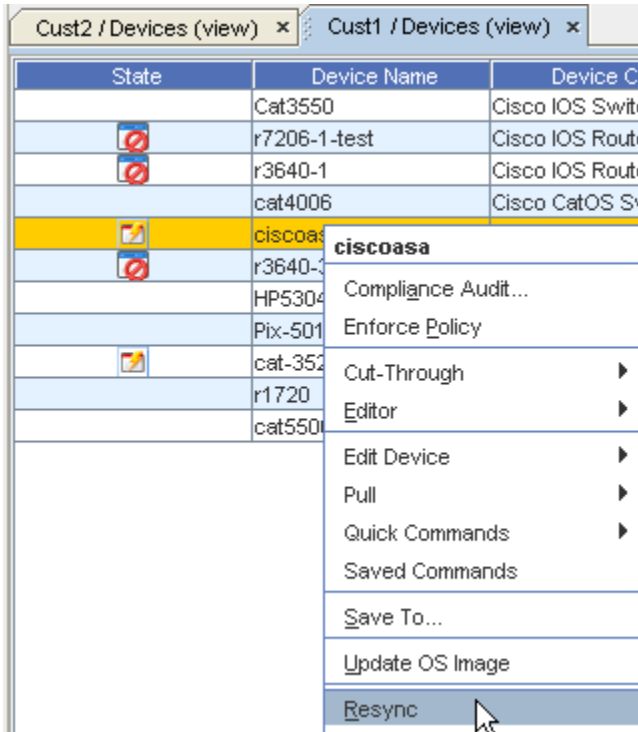
---

**Important** Make sure you refresh the Devices view after each resync is completed .

---

Using the right-click menu to Resync,

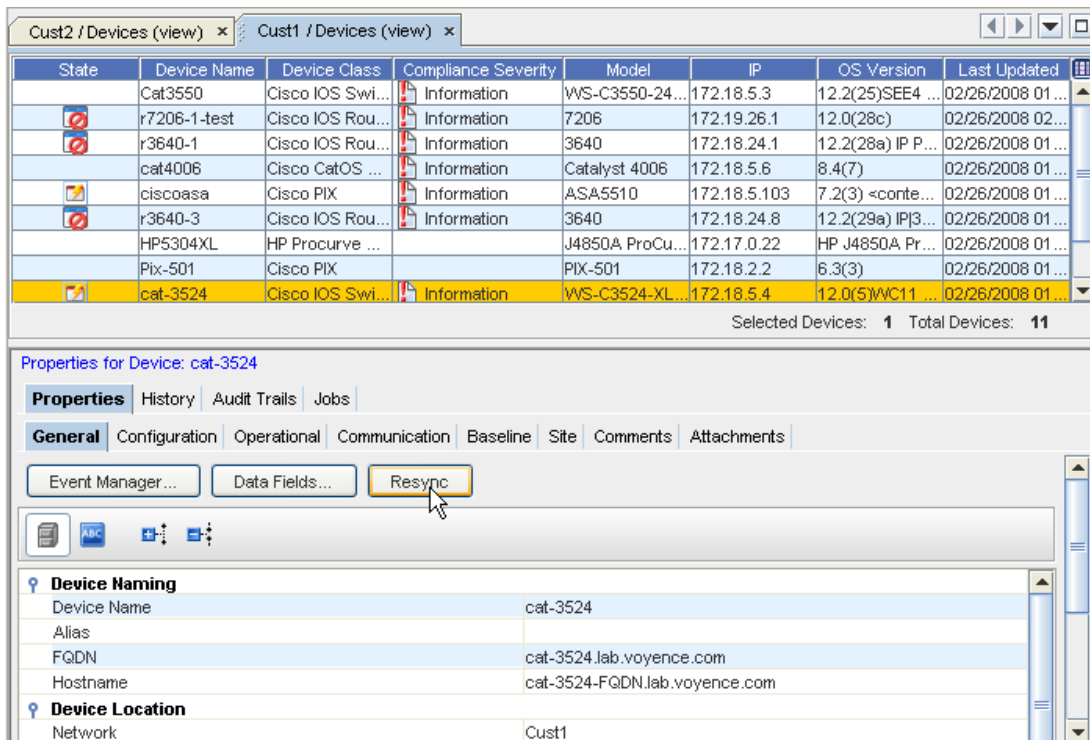
- 1 To bring a single device, or **multiple devices configuration** back into "sync", display the devices using the table layout.
- 2 From the Navigation tree, display the listing of devices to determine if you have any devices out of sync, as indicated by the icon  in the **State** column.
- 3 Select the **device**, then right-click on the device to show the options in the right-click menu.



4 Select **Resync** from the list of options to resync the device configuration.

5 Now, the **Schedule Push Job** window opens.

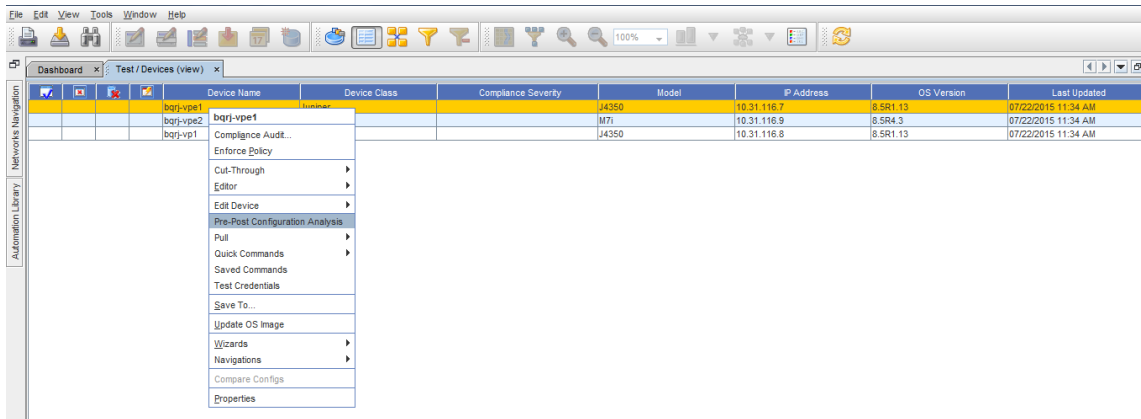
You can also view and "Sync" the device using the Properties - General tab.



## Wizards

Building on the concept of standardized templates, Wizards deliver intelligent automation to configuration tasks. Wizards generate Cisco IOS 12.0 and above code.

- 1 Wizards are accessible in the Table or Diagram view of any network. Select at least once device, then right-click on a device, and select **Wizards** from the right-click menu.

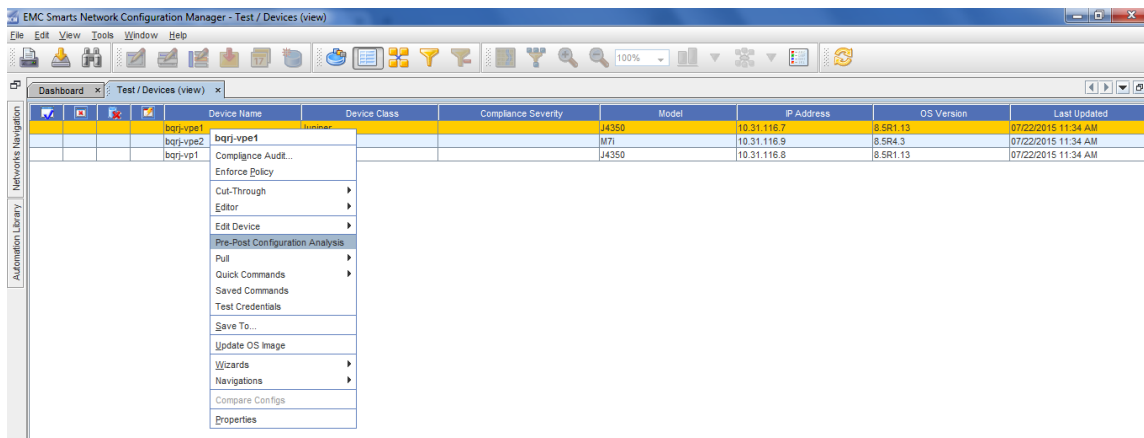


- 2 For more information, go to [The DNS Wizard Overview](#).

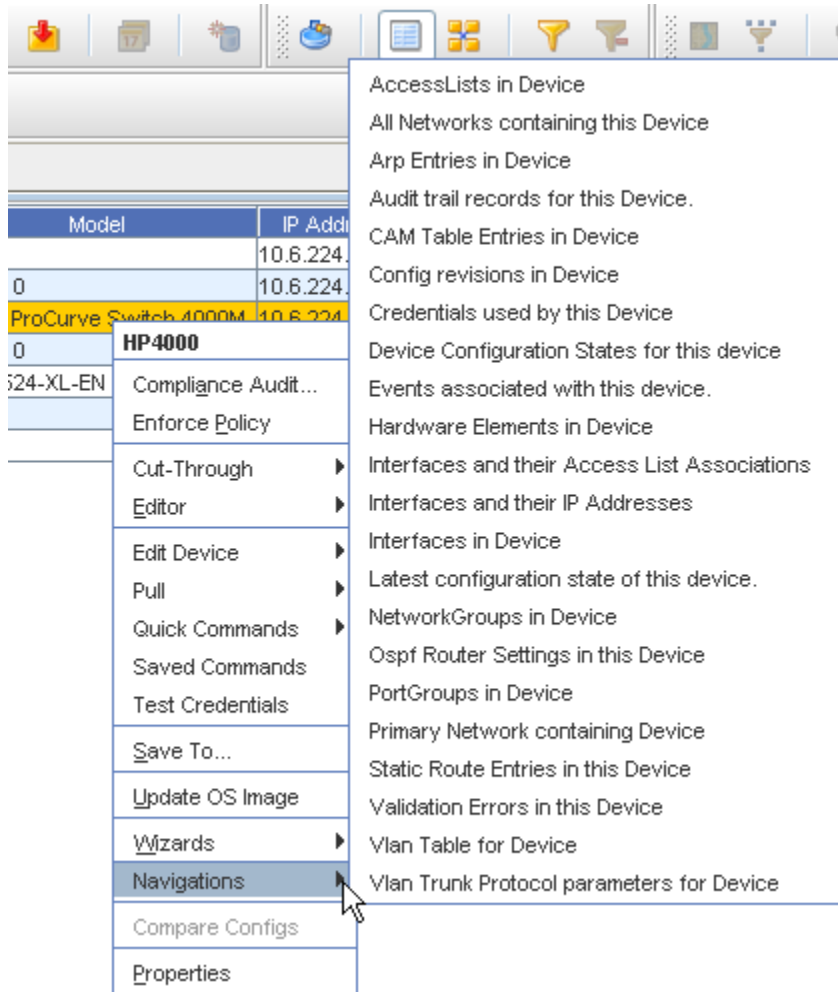
## Navigations

From within the Devices view you can **Navigate** to the Query Results that apply to that device.

- 1 First, select **Navigations** from the right-click options.



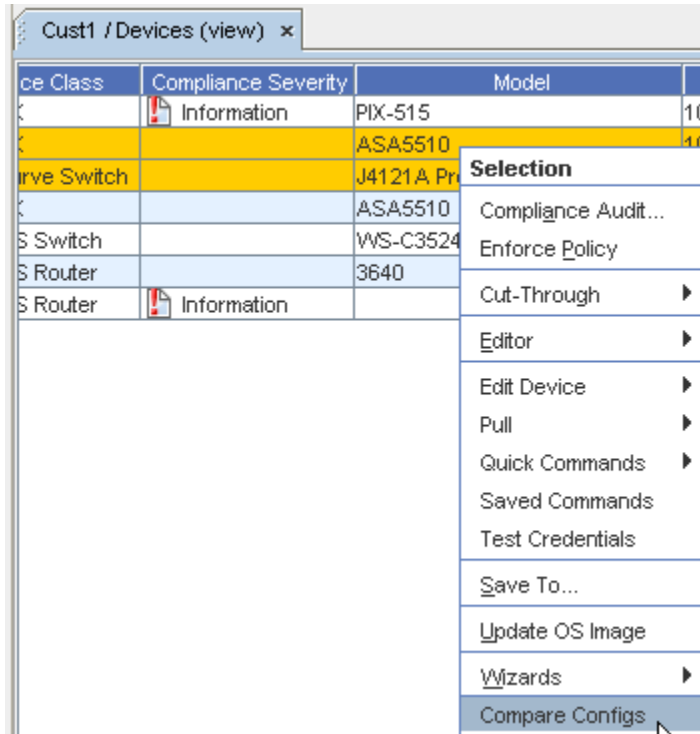
- 2 You then have several choices listed for the Navigations option. Selecting any one of these items takes you into the **Automation Library**, where the information for the data (Metadata) is stored. For example, when selecting Navigations, the listing of options displays.



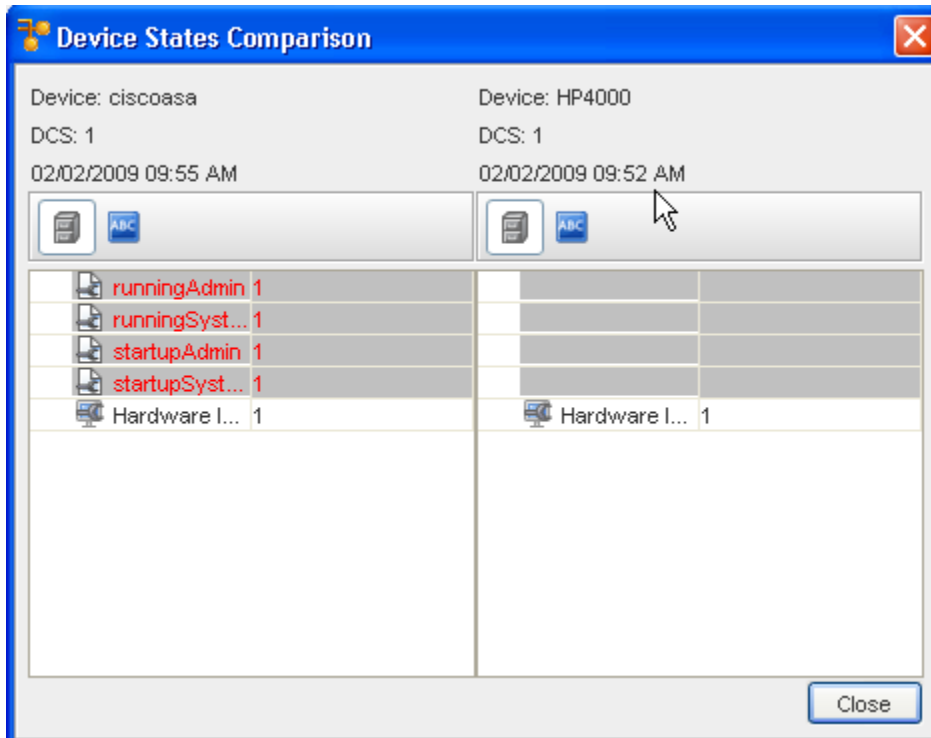
- 3 If the AccessLists in Device option is selected, this allows you to directly navigate to the Results that are displayed when that Query is run. All other selections in the list automatically navigate you to that specific information (displayed under Navigation) as well.

## Compare Configs

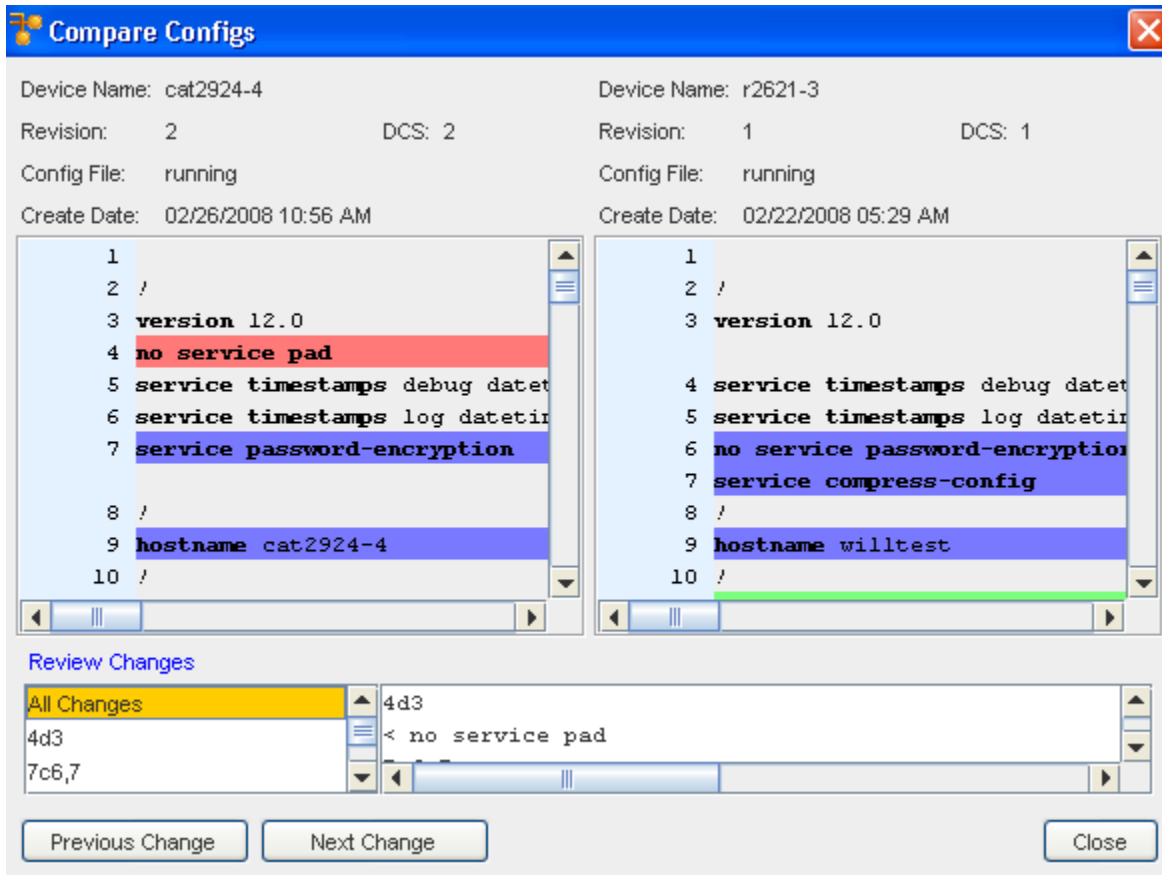
From the right-click menu options in the Devices View, you can **Compare Configurations** on any two devices.



- 1 Once the devices are selected from the listing, right-click, then select the **Compare Configs** option. This is helpful for comparing device states, and for a detailed view of the configuration.



- At the Devices States Comparison window, note the differences. You can highlight, and then **click the state** (for example, in the above graphic you would click running on the cat2923-4 device) to view the entire Config.



- You can now view the **Previous Change** or the **Next Change** of configurations on this device.

## Compare (Run/Start) Out-of-Sync Files

While viewing the Devices in either the Table or Diagram view, you can compare the Running vs. the Startup configuration on devices.

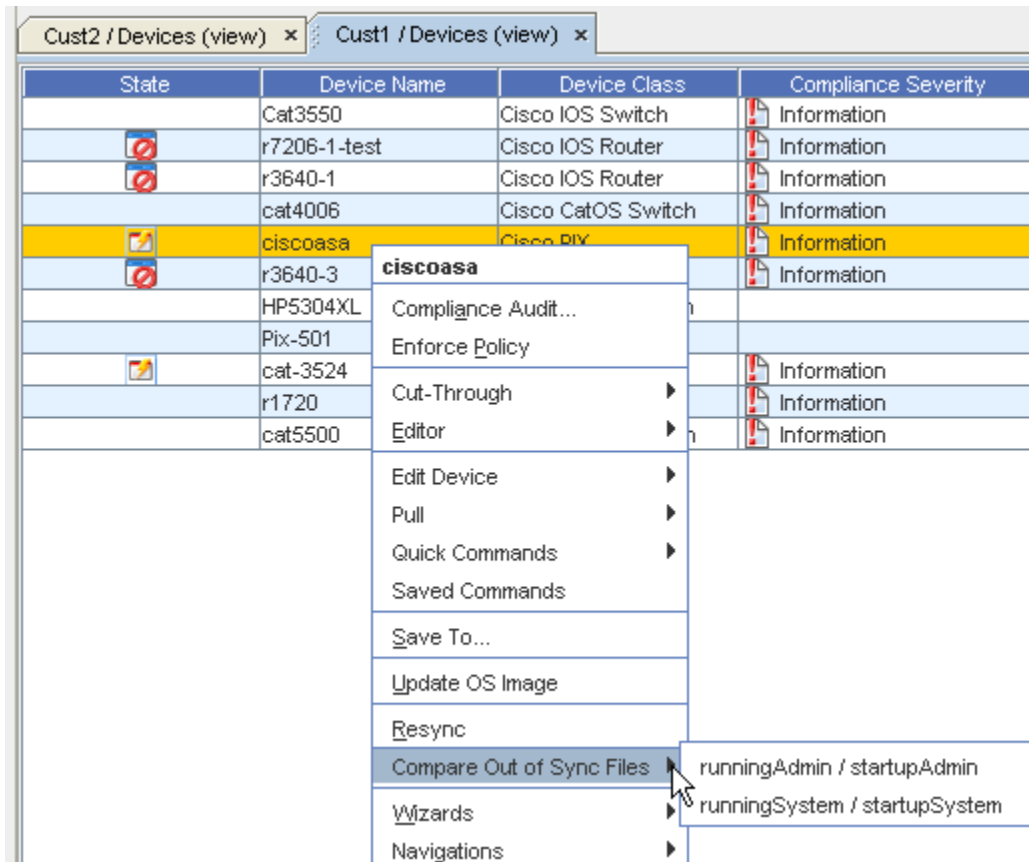
---

**Note** This can only be completed on Out-of-Sync devices.

---

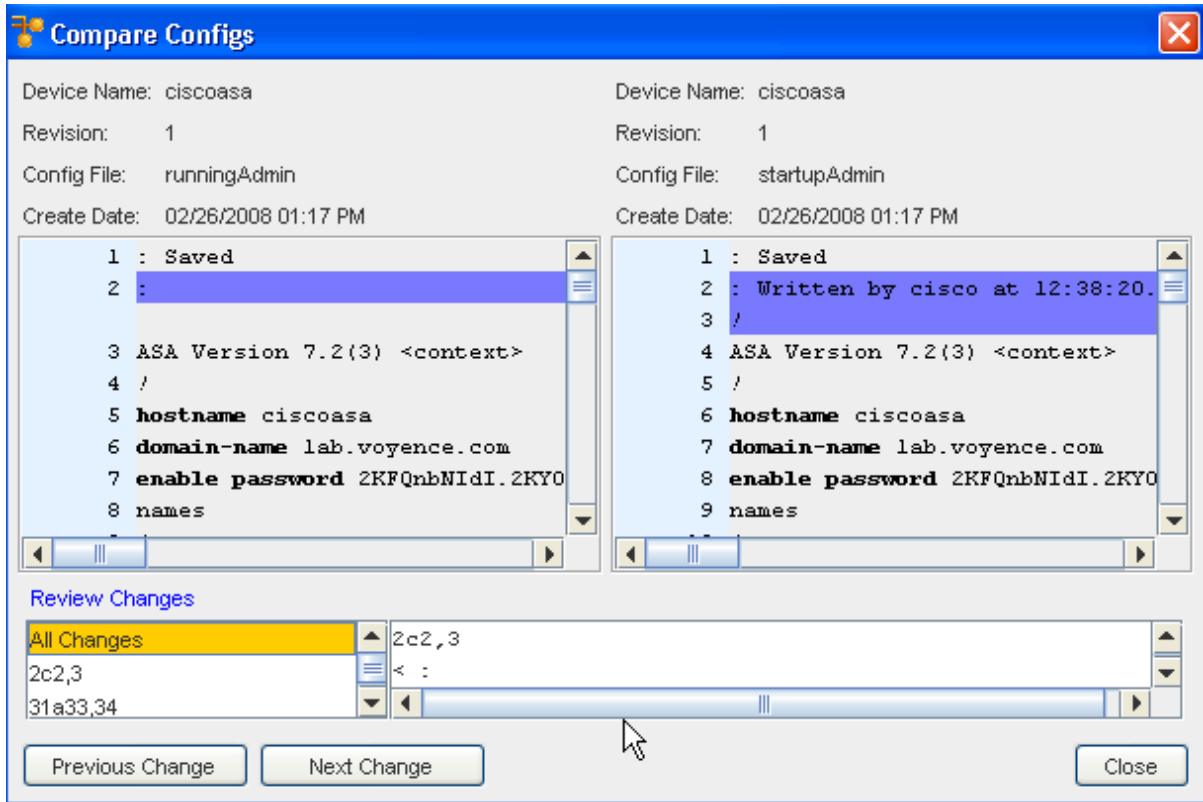
Using Compare Out of Sync Files option,

- To compare the **Running/Startup Admin and System** configurations, have your devices displayed in a Devices view.

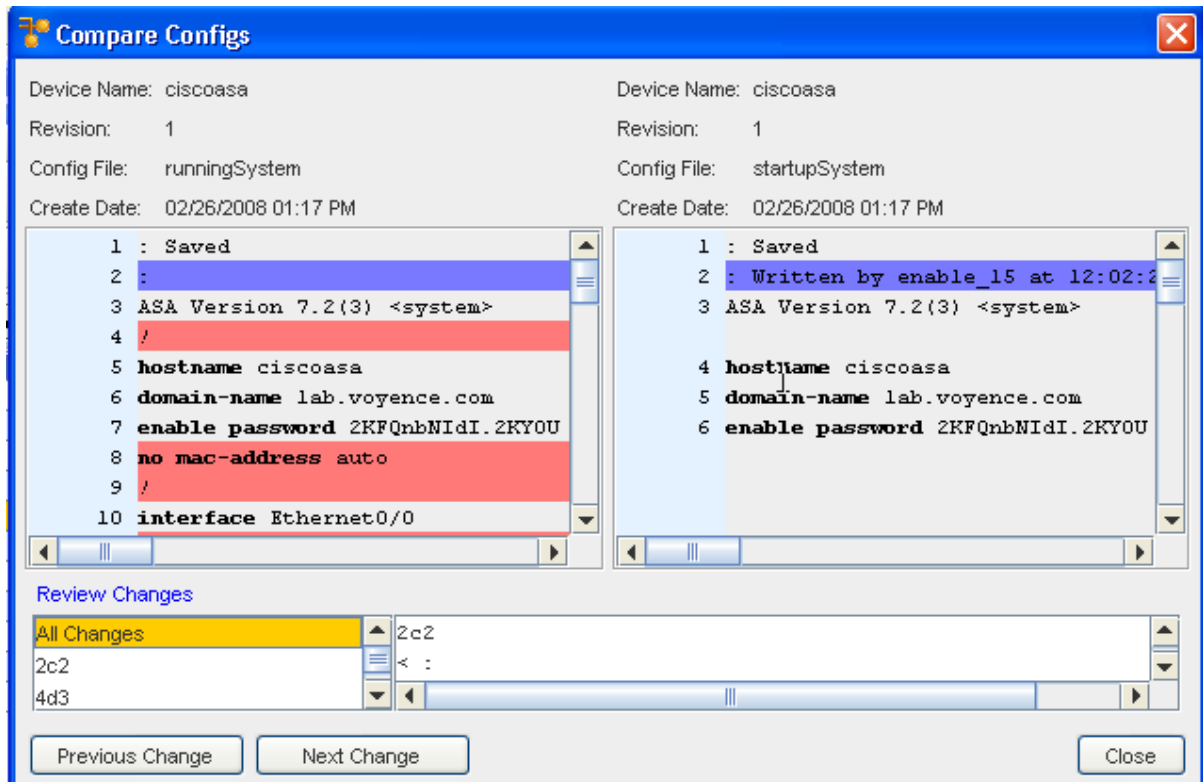


- Next, select a device from the list that has the "out-of-sync" icon in the **State** column, and right-click that device.
- At the Compare Out of Sync Files option, you can select one of two options. Select either the **runningAdmin / startupAdmin**, or the **runningSystem / startupSystem** option.

If selecting the **runningAdmin / startupAdmin**, the Compare Configs window shows the following comparison, for example.



If selecting **runningSystem** / **startupSystem** the Compare Configs windows shows the following, for example.



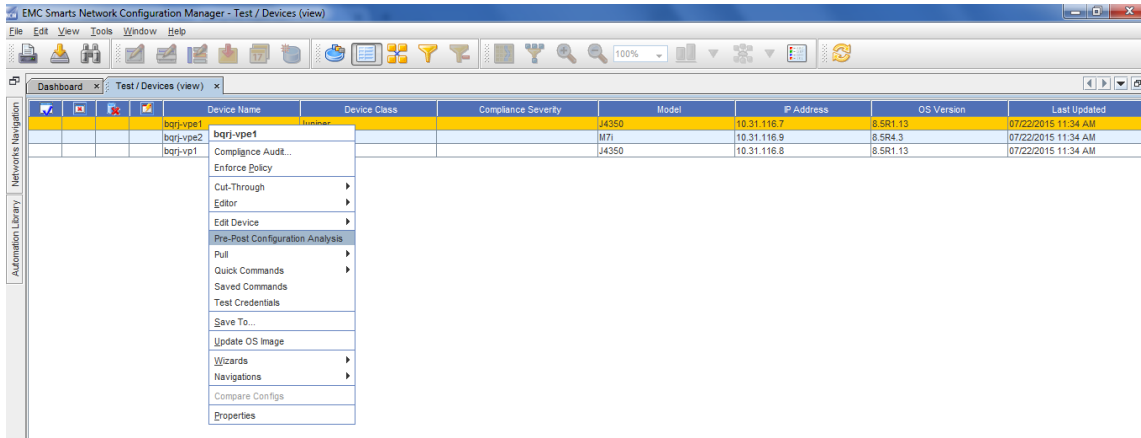


- 4 Select the **Previous Change**, to see the last change (it is displayed in the Review Changes section). You can also click **Next Change** to see the very next change listed in the **Review Changes** section.
- 5 Click **Close** when you have viewed the comparisons.

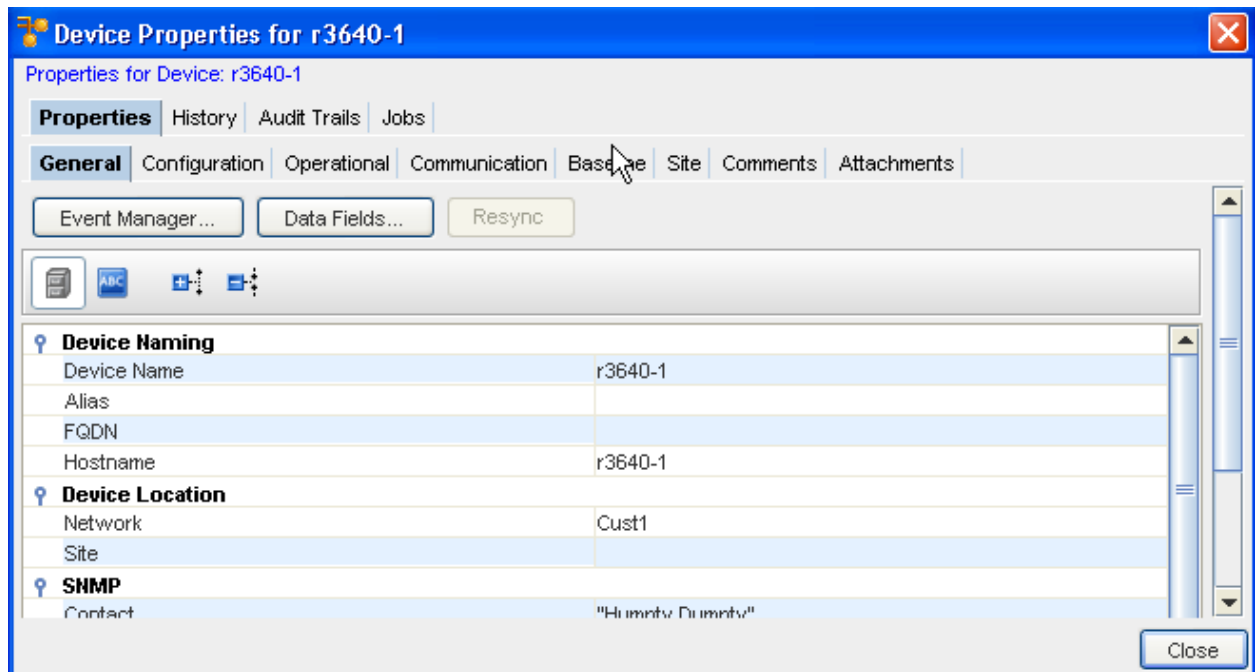
## Properties

From the Devices View you can quickly go to the **Properties** for any selected device.

- 1 From the Devices view, select a **device** , then right-click to see the menu options.



- 2 Once **Properties** is selected, you can now view all the device properties information contained within the General tab.



For more information on Device Properties, go to [Device Properties Tabs](#) .

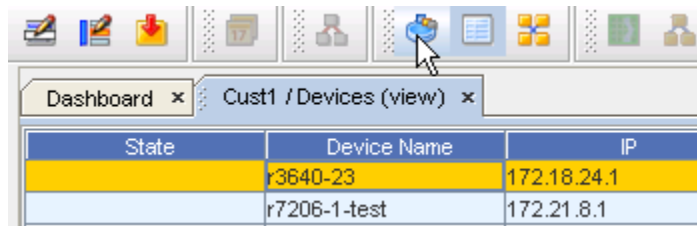
## Device Properties

### Device Properties Tabs

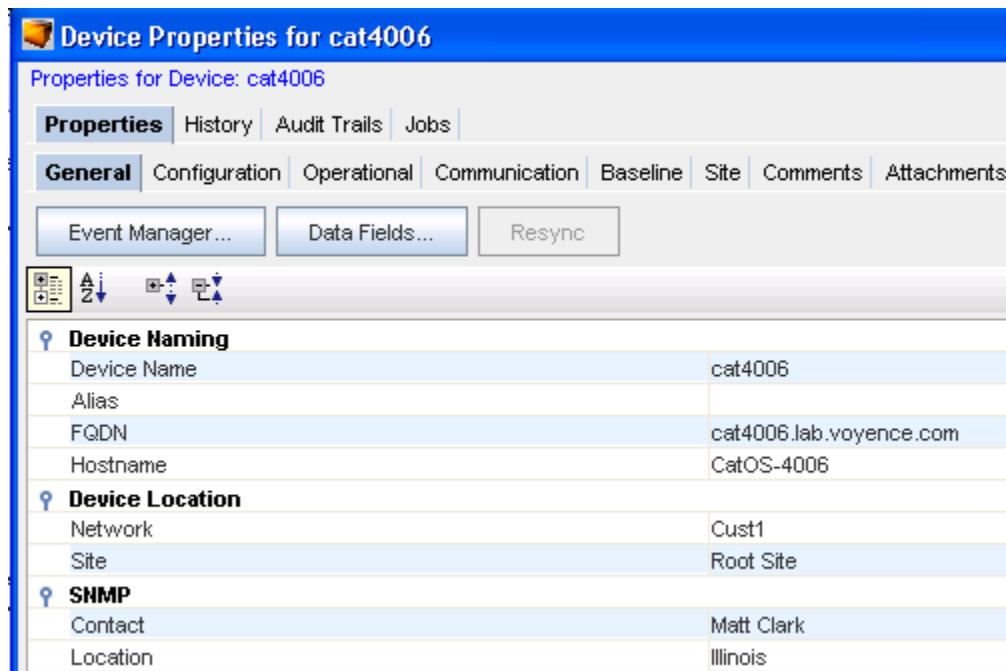
**Device Properties** contain some of the same information as do the right-click Device Properties options, however, the information is displayed differently, and may include additional information. Instead of being listed in the right-click menu, the Device Properties are displayed in tabs at the lower section of the Devices View window.

 Not all of the tabs are selectable at any one time .

This window can be displayed by selecting the **Properties** icon of the tool bar.



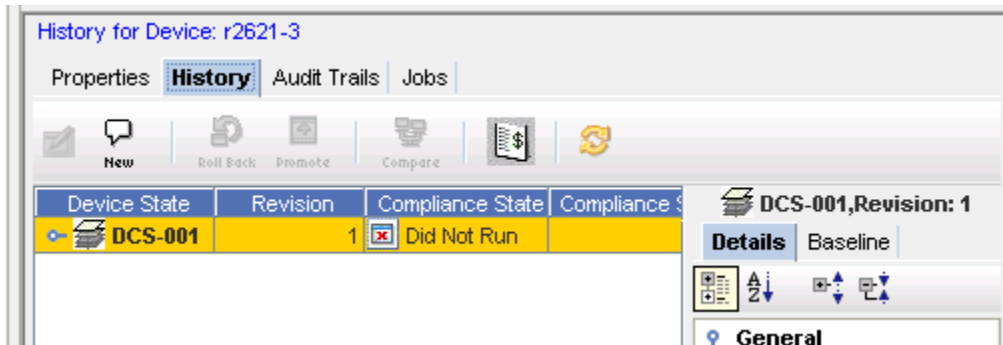
**Note** The properties information changes relative to the device selected in the current view.



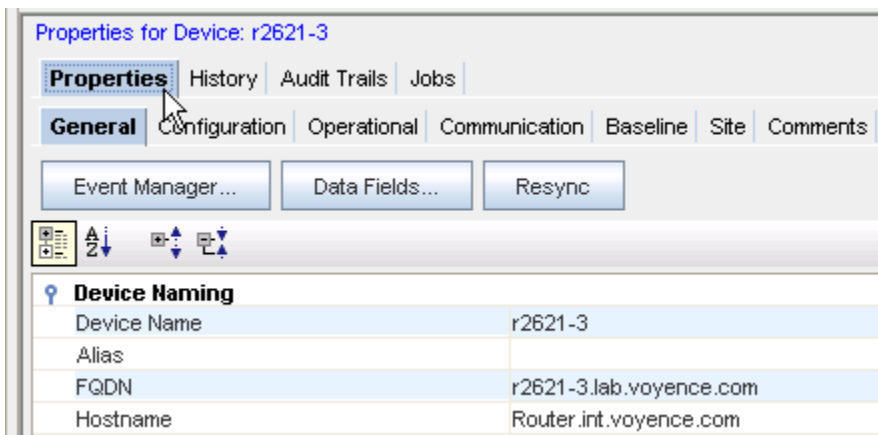
The first tab ( **Properties**) displays with **History**, **Audit Trails** , and **Jobs** tabs available.

Once Properties is accessed, the **General tab** is displayed. You can select any tab, in any order, to view information. When working with only those tabs at the Properties level (History, Audit Trails, and Jobs), the other tabs located beneath the Properties (Configuration, Operational, and so on) close.

For example, When you are viewing the **History** tab, the only tabs now available are **Audit Trails** and **Jobs**.



To once again view all tabs, click the **Properties** tab again.



Tabs contained within the Properties view are also the location where various tasks can be completed, such as in the History tab, where you can select **two or more revisions**, and then compare the revisions to view the changes made in each revision.

This table details the content of each tab within the Properties view.

<a href="#">The General Tab Overview</a>	Contains specific device information, including name, location, Device Properties, Server Location, and more
<a href="#">History Tab Overview</a>	Contains the history of tasks that have been completed on this device, including revisions. It is also where Rollback and Audits can be selected, and Data Fields can be added.
<a href="#">Working with Audit Trails</a>	Details the state of the device in reference to compliance, and when the compliance audit test was run
<a href="#">Working with Jobs</a>	Lists any jobs that have been scheduled for that device
<a href="#">Configuration Tab Overview</a>	Lists any running configurations, any previous configs, the config status, and more
<a href="#">Operational Units Tab Overview</a>	Contains a list of the data that was pulled for the device
<a href="#">Communication Tab Overview</a>	Contains all the In-Band, Out-of-Band, Cut-through communications, and allows you to update credentials
<a href="#">Baseline Tab Overview</a>	Allows you to review the network baseline config that affects the device

<a href="#">History Tab Overview</a>	Allows you to review the history on the config file
<a href="#">Site Tab Overview</a>	If the device has been assigned to a site, the site information displays on the Site tab.
<a href="#">Comments Tab Overview</a>	Allows you to enter device specific comments
<a href="#">Attachments Tab Overview</a>	Allows you to associate an external file to the network

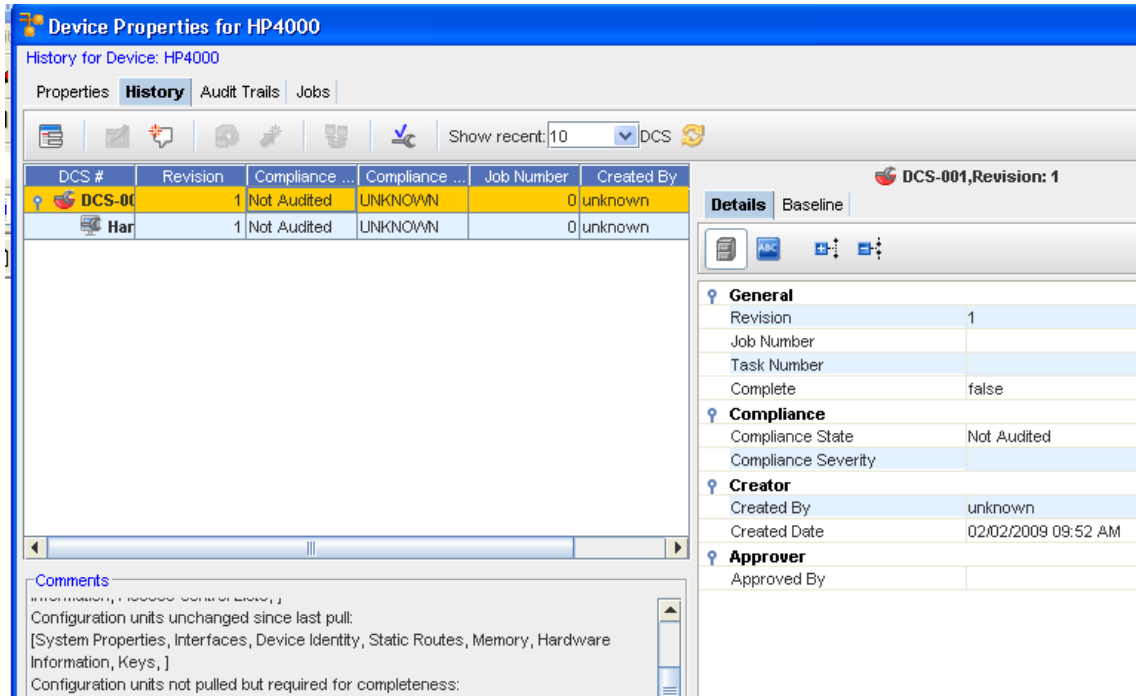
## The History Tab

### History Tab Overview

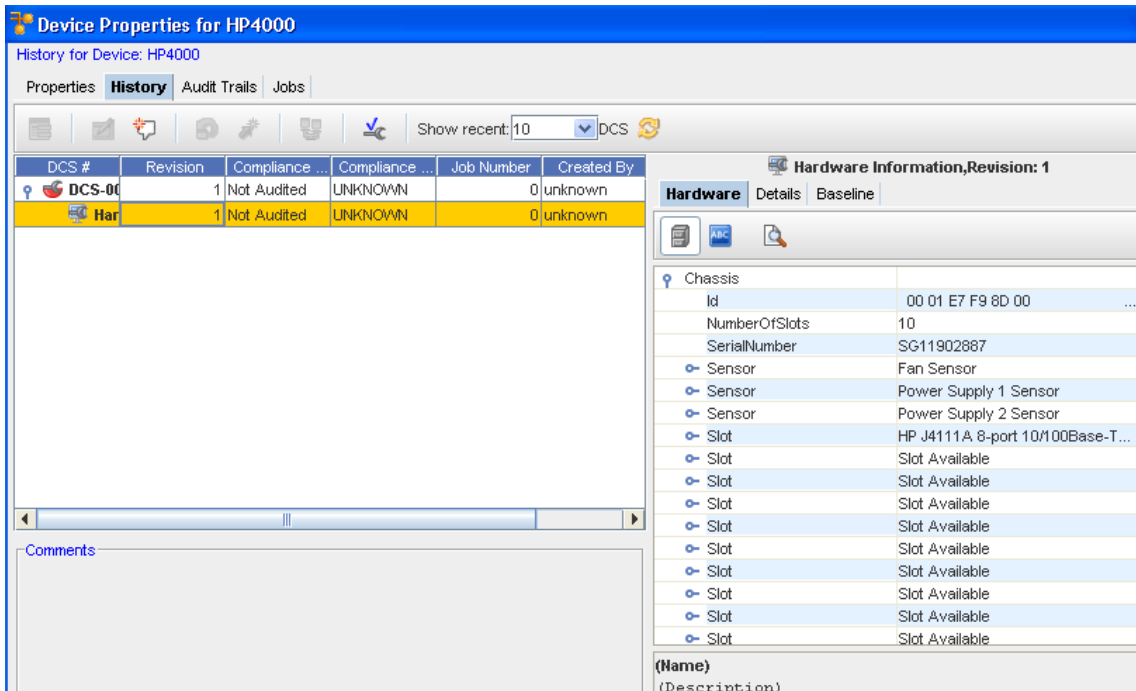
The **History** tab displays an actual history of that device. The History tab Allows you to:

- Review the device's history and past events
- Access the Config editor
- View or Update existing Data Fields
- Create a new Revision Comment, and review all previously added comments
- Review the Baseline and Config details
- Rollback to a previous configuration revision
- Promote a Configuration
- Compare one or more configurations
- Audit the configuration - allowing you to select the Standard, and then run a Compliance Audit. You can multi-select revisions and audit against a Standard to find historical compliance (when the device has gone out of compliance).
- Refresh the view after changes
- View the hardware details (when **Hardware** is selected from the Device State column)

You can also Audit the **Device Properties** feature.

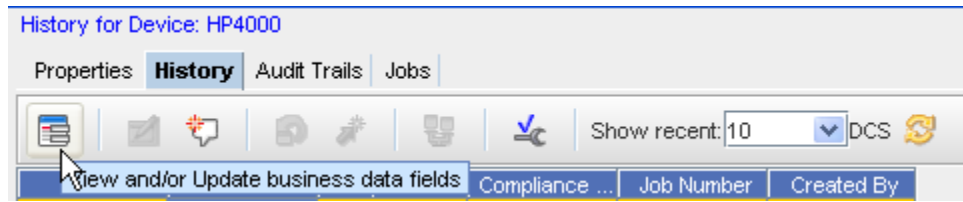


You can review the **Hardware**, the **Details**, and the **Baseline** of the current config.



- **Comments** on the Configuration can be viewed as well.
- Note that you can view ... the Device State Configurations by selection the drop-down beside the **Show Recent** option.

**History Tab Tool Bar**

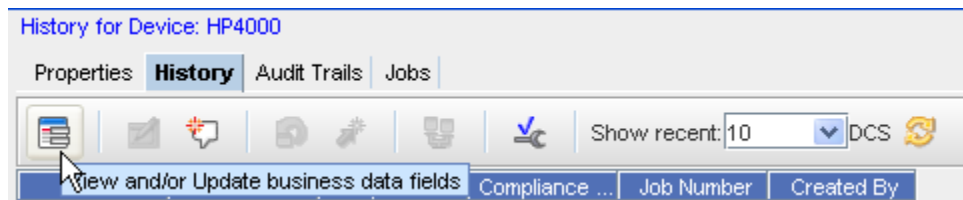


When viewing the History tab, note that the tool bar offers various options to complete tasks. For example:

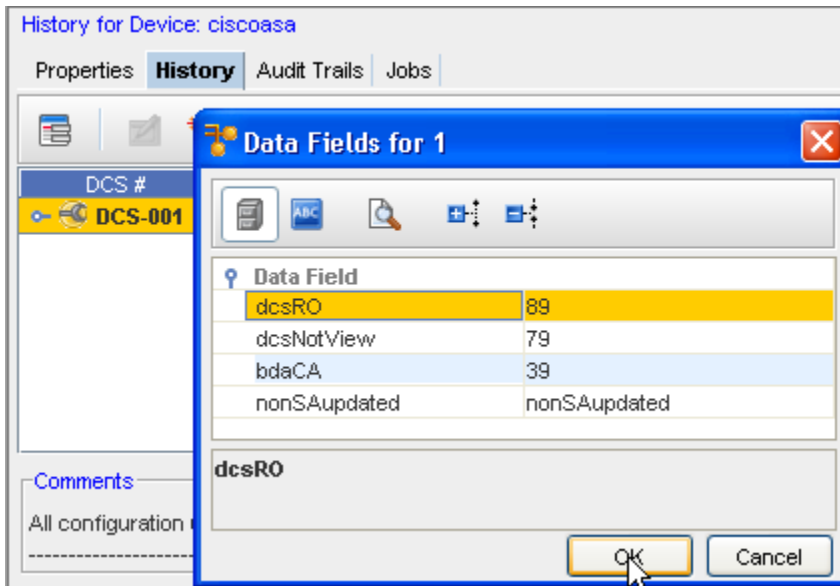
- View and/or Update Business Data Fields
- Access the Configuration Editor
- Create a new Comment
- Roll Back to Baseline
- Set the Current Revision as the Baseline
- Compare Device Revision Configs
- Run the Compliance Audit
- Refresh the view

#### Viewing or Updating a Data Field from the History or Interfaces tab

**Note** Data Fields are used to create attributes, and to assign values to devices.



- 1 From the **Devices View**, select to show the Device **properties** of a single device. Once the Properties tabs are displayed, click on the **History** tab (or the **Interfaces** tab).
- 2 Select the **View/Add Data Fields** icon to open the Data Fields window where you can select to add any of the available fields. If needed, expand the Data Fields listing, then select the appropriate option from the list.



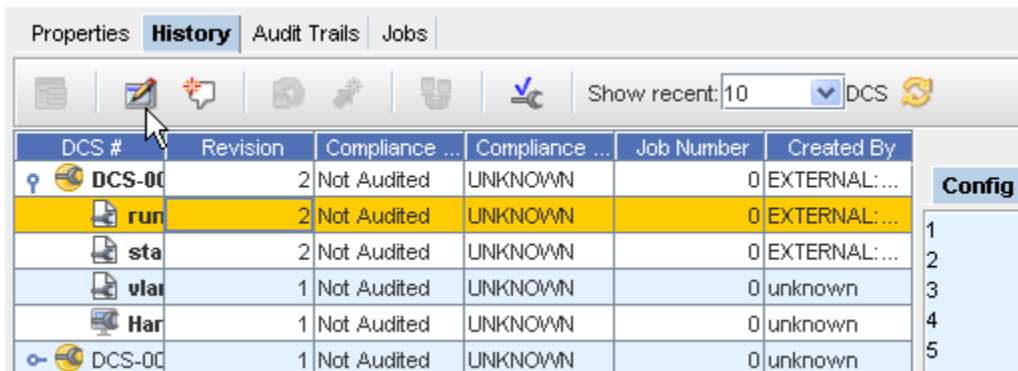
3 Click **Ok**.

**Note** You must have System Administration privileges to work with the Device Data Fields. You must also have View Permissions to view the data fields information.

### Changing the Config file

To make changes to the Config file,

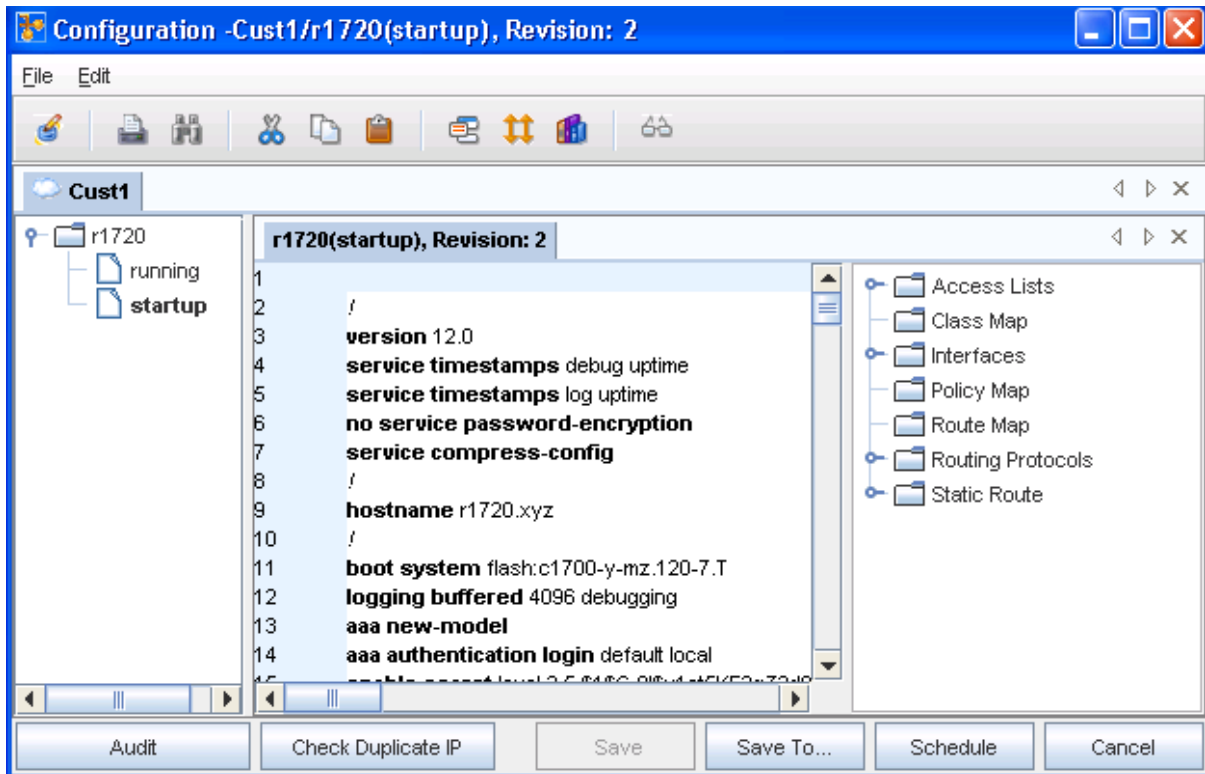
1 In the **History** tab, select a running config , and then click the **Config Editor** icon.



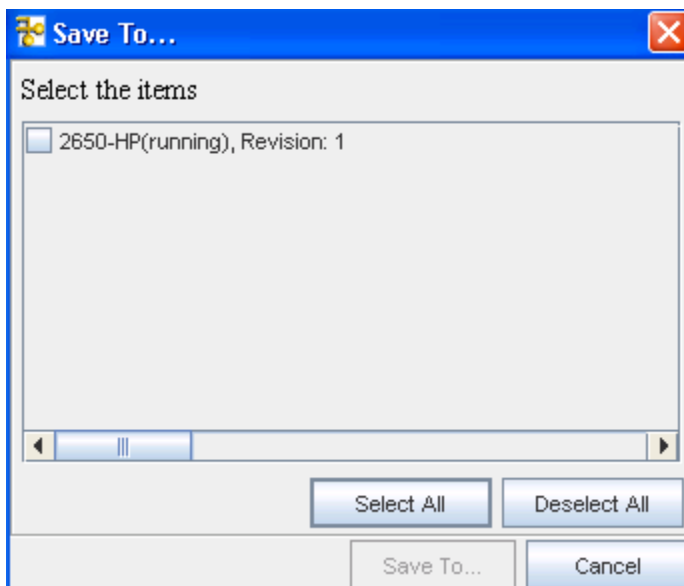
The Config Editor window opens.

2 Make any needed revisions to the information.

3 Click **Preview** to preview your changes, and then click **Save To...** to save your changes.

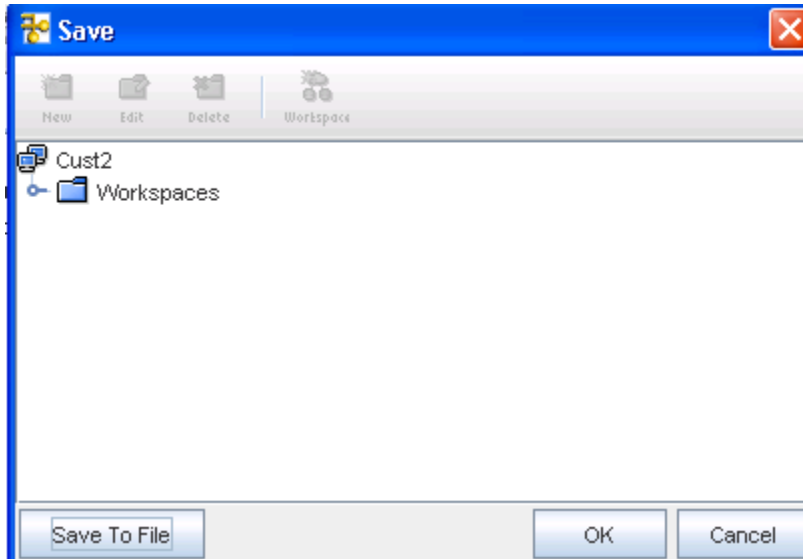


- 4 From there, in the **Save To..** window (shown below), you can select the items to save by clicking in the check box beside each device, or by using the **Select All** bar. then clicking **Save To....**



- 5 Now, use the **Save** window to determine where you want to save this.



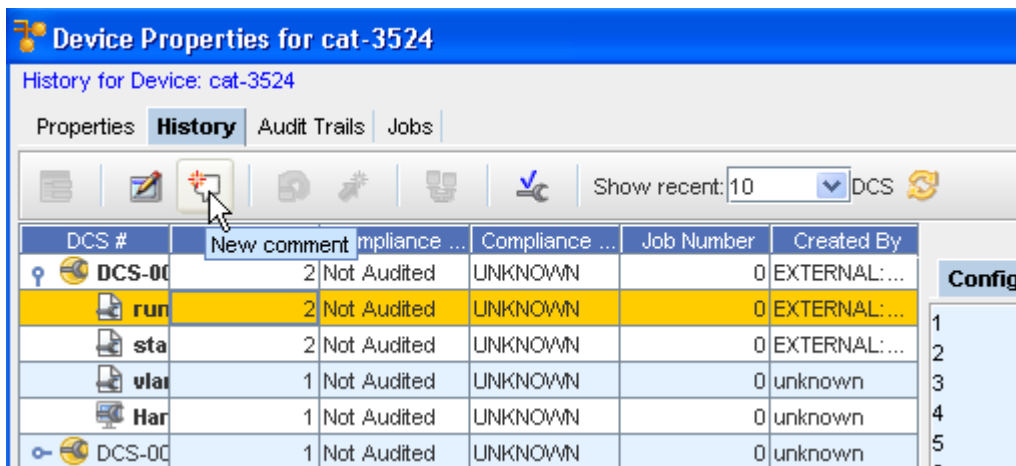


6 Click **Ok** when you have made your save location selection.

### Adding Revision Comments

To add revision comments,

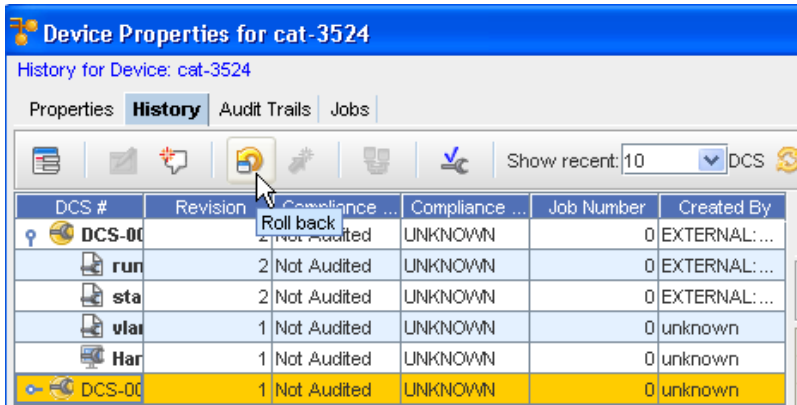
1 In the **History** tab, click the **New** icon to see the Revision Comments window for that device.



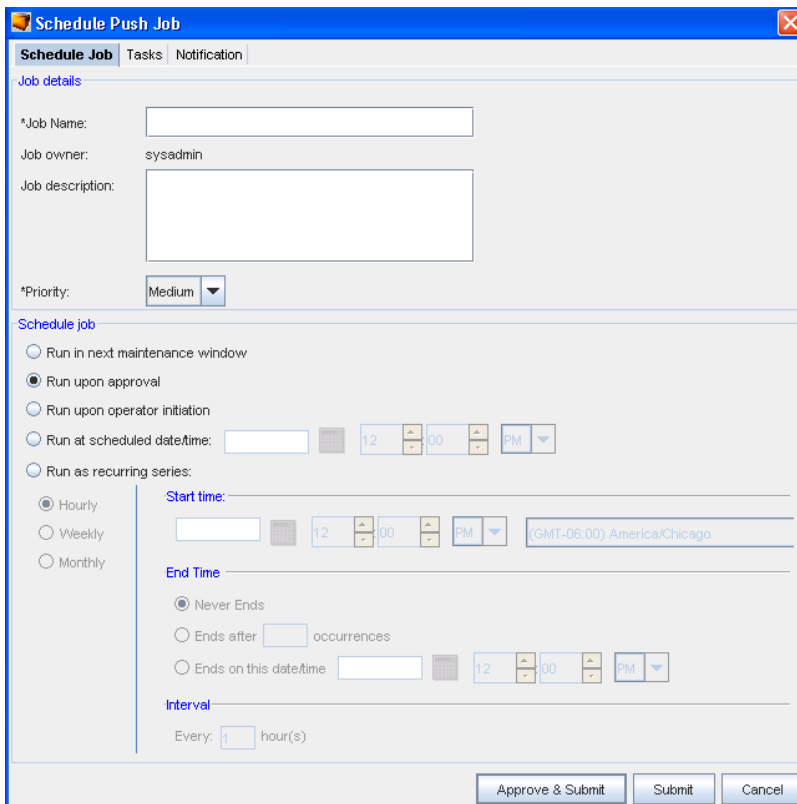
2 Enter any **new comments** in the Add Revision Comments window, then click **OK**. Your latest comments are now added to the top of the comments window.

### Rolling Back to Baseline option

1 From the **History** tab, select a revision, then select the **Roll Back** icon. This will roll the device back to the previous configuration level, prior to the latest configuration changes.



The Schedule Push Job window then displays.



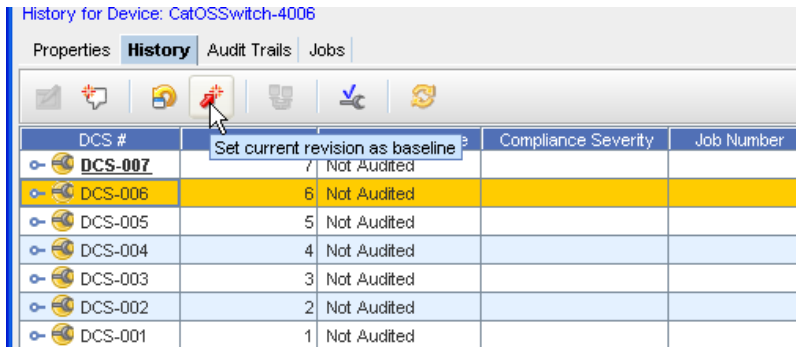
- 2 For information on using this window, go to [Scheduling a Run Time](#).

### Set the Current Revision as the Baseline

**Important** A Baseline must have already been set for the Network.

- 1 From the **History** tab in the Device Properties, you can access the **Set Current Revision to Baseline** icon to set the baseline to the current configuration version.
- 2 After selecting a Device from the Devices View, then selecting the **Properties** icon, you can then access the **History** tab.

- 3 If there is more than one revision shown (in the **Revision** column) you can promote the latest revision. For example, if you have two revisions shown; a number 1 and a number 2, then you can surmise that changes to the baseline have been made, and you need to promote the latest baseline revision (2).



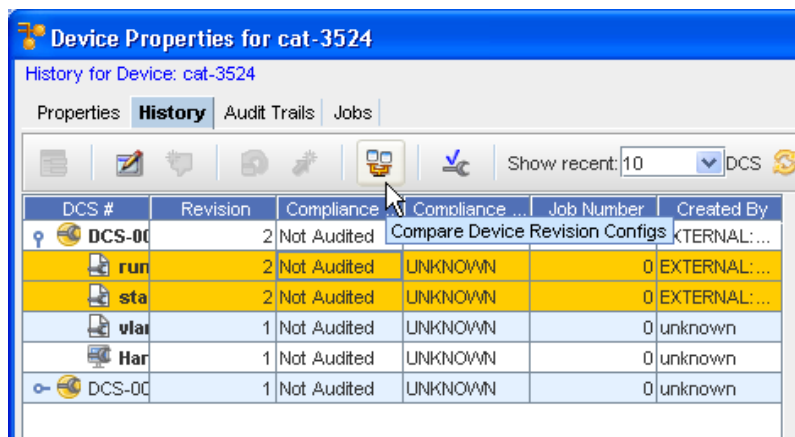
- 4 Select the **latest revision**, then click the **Set Current Revision to Baseline** icon to set the current configuration version. This will then be the current baseline configuration for the Device.

### Comparing Configs

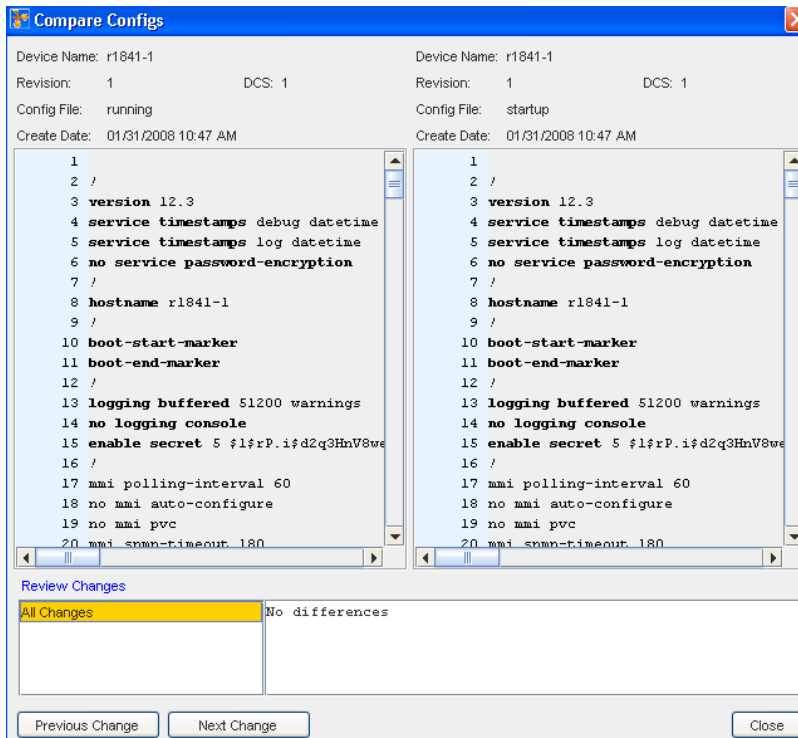
This feature allows you to compare two configuration file revisions. In the Compare Configs view, each configuration displays in its own window, and is not editable. When viewing the changes, red indicates lines deleted, blue indicates lines modified, and green indicates where lines have been added.

To Compare Configs,

From the **History tab**, you can compare any two revisions that you select.



- 1 Select (highlight) the **two revisions** you want to compare (holding down the Shift key, and then clicking the revision).
- 2 Now, select the **Compare** icon (as shown above). The Compare Configs window opens.



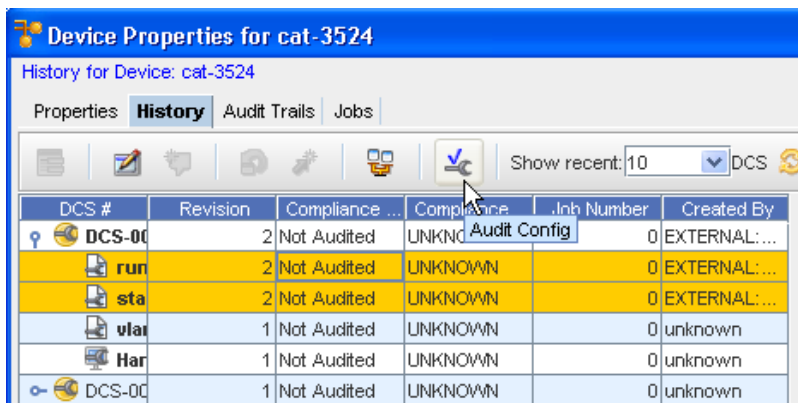
- 3 Review the previous changes by accessing the **Previous Change** button, then continue reviewing all the subsequent changes using the **Next Change** button.
- 4 Click **Close** when you have reviewed the Config comparison information.

### Running a Compliance Audit



You can see which of the configurations are **Compliant or Non-Compliant** .

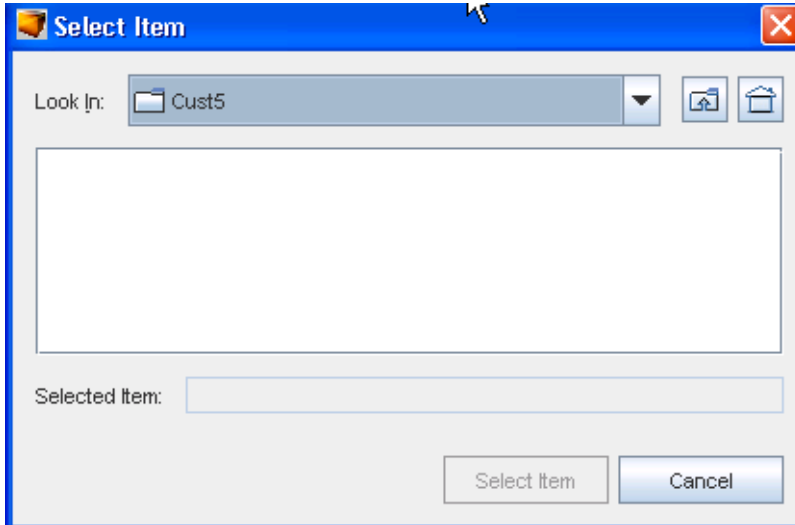
To complete an Audit,

- 1 From the **History tab**,select a Revision, then select the **Audit Config** icon.

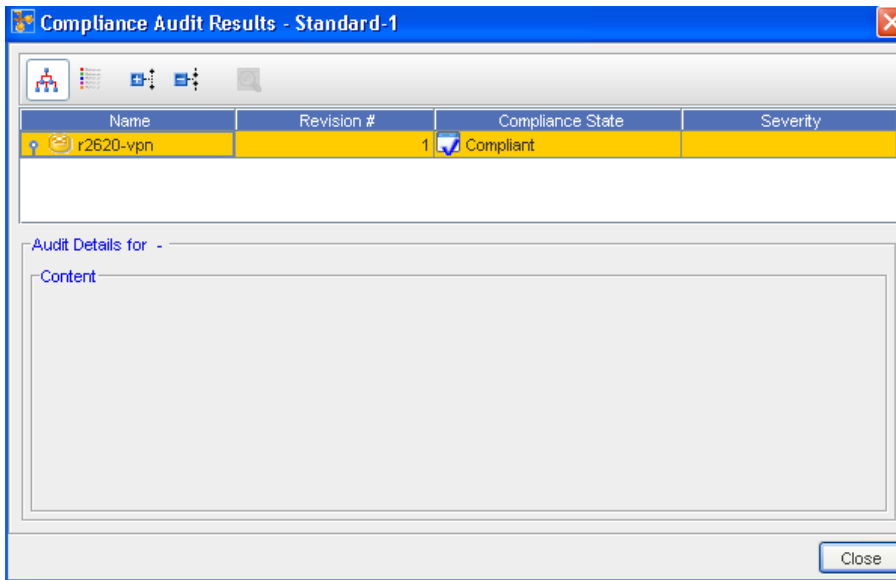


- From the Select Item window, click the drop-down arrow.

**Note** You can use the two icons   (Up one Level and Home) to expand or contract the listing contents).



- Make your selection from the list, then **select** the Item.
- At the Compliance Audit Results window, your results are displayed.



**Note** **Green** is Compliant, and **red** designates Non-Compliant.

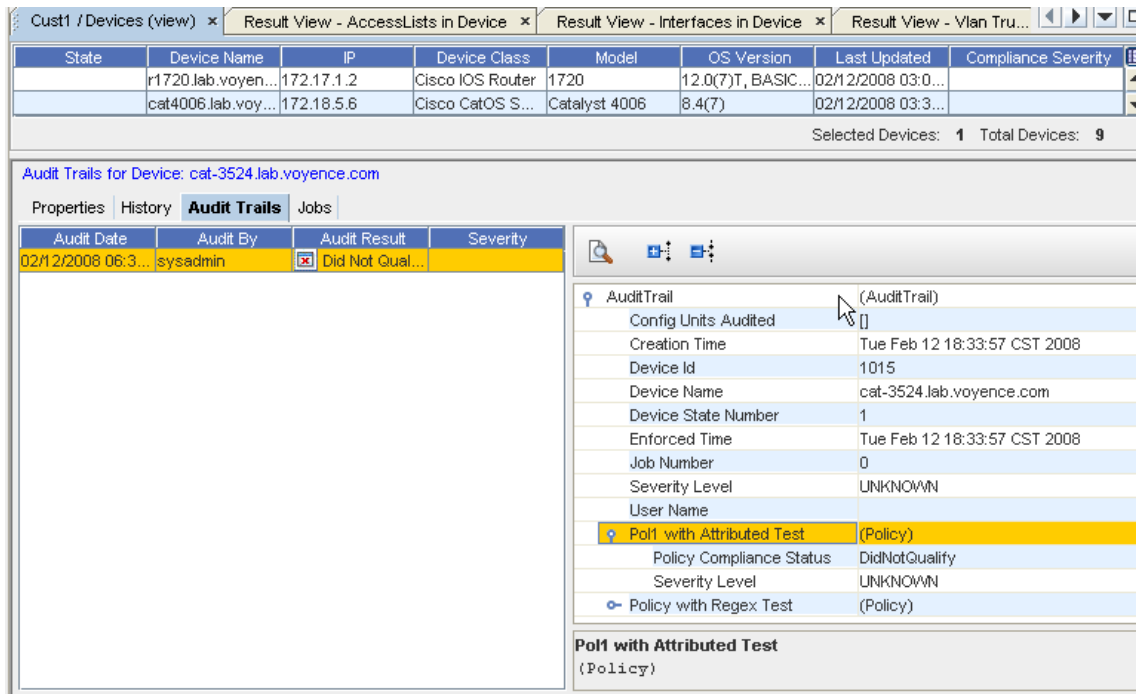
- Click **Close** when you have reviewed the audit results.

### The Audit Trails Tab

#### Working with Audit Trails

In the **Properties** tabbed view, you can access the **Audit Trails** of any device.

Once the Audit Trails are accessed, information pertaining to any audits for that device are listed. Information contained within this tab is **read only**.



To see detailed information, click on the items listed in the right, and expand the topics.

Within the Audit Trail information you can use the following:



- Show/Hide the Description area
- Expand or Collapse the Audit Trail items

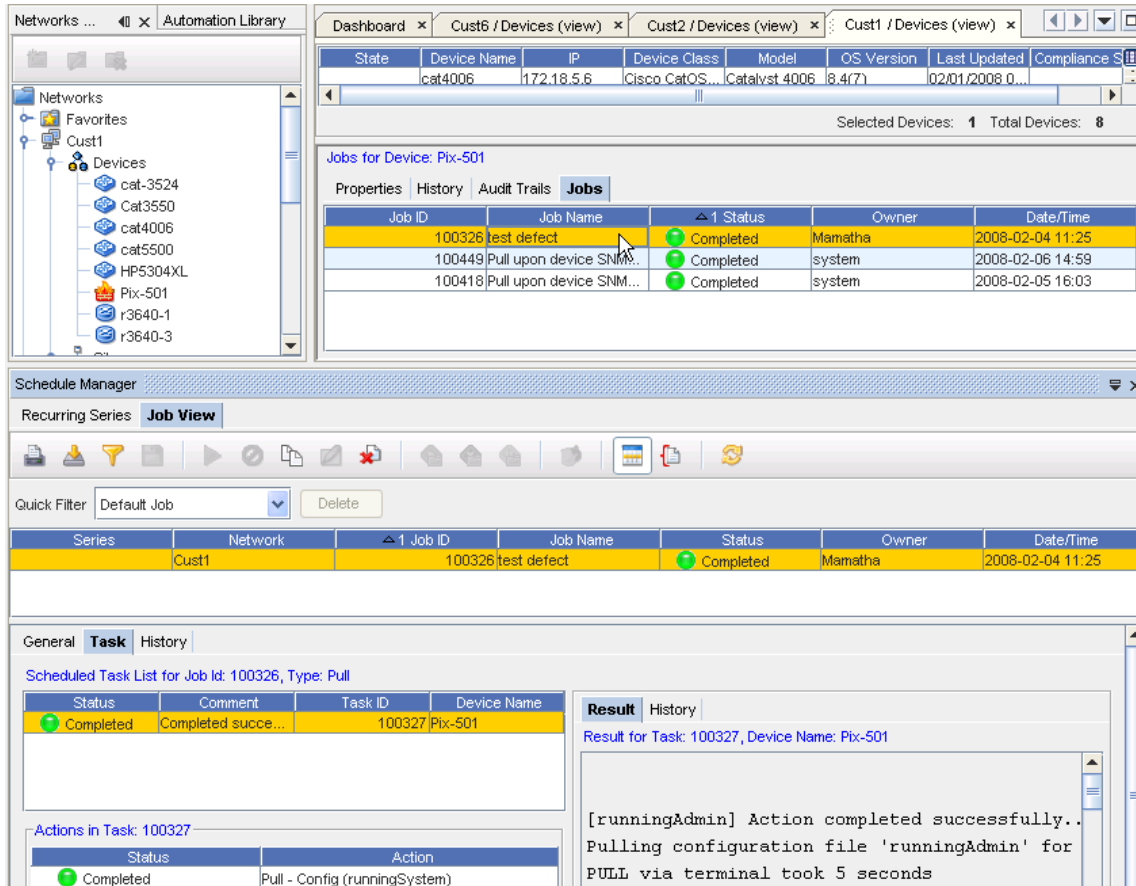
## The Jobs Tab

### Working with Jobs

From the **Properties** tabbed section, you can view any jobs that have been run against any device. By first selecting a device, then selecting the **Jobs** tab in Properties you can retrieve job information. This information is **read only**.

Make sure to click within any **column heading** to see if more columns headings are available for display, and thus more job information is available.

While reviewing the job information on any specific device, clicking on any actual job information in any column will open the **Schedule manager** .



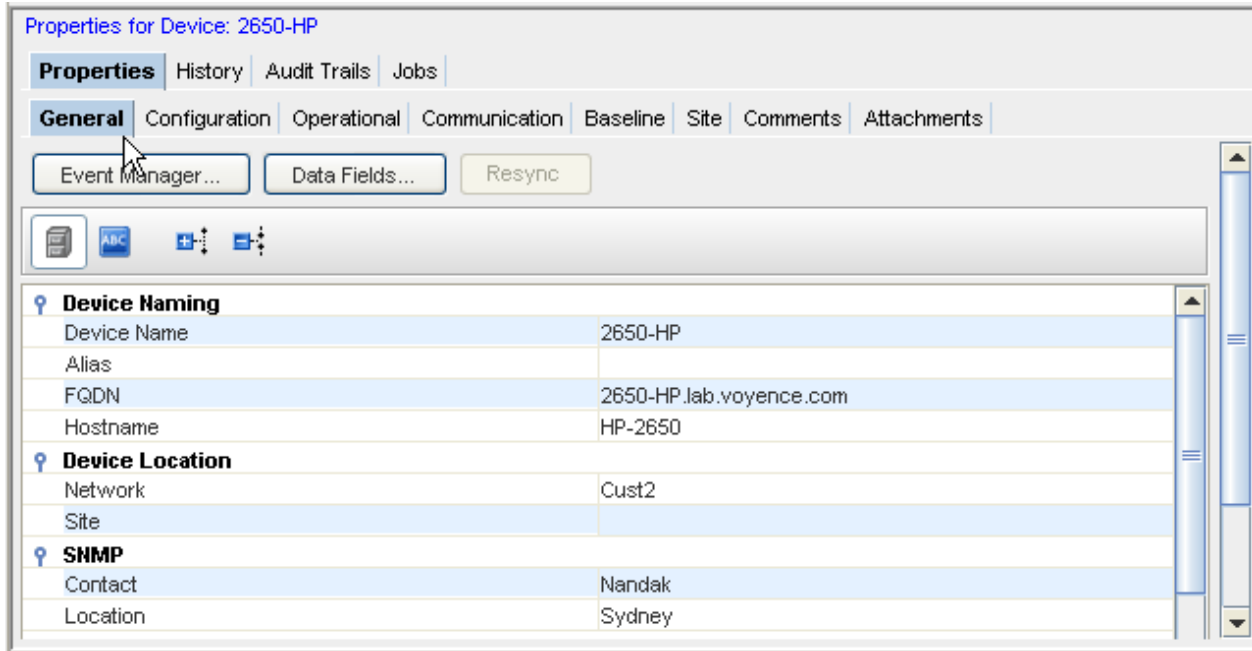
For more information, go to [Schedule Manager Overview](#)

## The General Tab

### The General Tab Overview

This window can be displayed by selecting the **Properties** icon in the menu bar, or from **Properties** when displaying the Devices view. The General tab contains specific Device information.

**Note** To expand the properties window, **drag and drop** the line separating the listing from the Properties tabs. This allows you to display more device properties information.



### Using the General Tab

You can access the [Event Manager Overview](#) from the General tab. Notice the Event Manager opens to display logs of event information and activity.

From this tab, you can also access **Data Fields** . This allows you to view extra Metadata attributes (data fields). The attributes are set up using Public API's, or from System Administration, as described in [Adding a Data Field](#).

You can also use this tab to [Resync Device Configurations](#) devices. This designates if the current running configuration is different than the start-up configuration. You can use the **Resync** button to bring your device's configuration back into sync with the database. This is only displayed if you actually have some devices that are currently out-of-sync.

### Task bar



These tasks can be completed within the General tab.

Icon	Task
	Categorize
	Sort Alphabetically
	Expand the listing
	Collapse the listing



### **Information included within this tab,**

Following are the sections of information contained within this tab.

#### **Device Naming**

This includes:

- Device Name
- Alias
- Fully Qualified Device Name (FQDN)
- Hostname

#### **Device Location**

This section of the General tab displays the device location.

- Network
- Site

#### **SNMP**

This section gives SNMP information.

- Contact
- Location

#### **Device Properties**

This includes:

- Device ID
- State
- Type
- Vendor
- Model
- Operating System
- Serial Number
- and All column headings you selected from the Devices View. See [Displaying Column Headings in the Devices View](#) for more information.

#### **Server Information**

This section details the server information.

- Name
- Type

Data Fields

## Resync Device Configurations

While viewing the Devices in either the Table or Diagram view, you are alerted (by the out-of-sync icon in the **State** column) that you have devices that are out-of-sync.

This indicates that the running configuration for a specific device is not "in sync" with the saved device configuration, and should be brought back into sync to preserve the running configuration when the application is rebooted.

There are three ways to get the device back "into sync":


- Using the **Resync** button provided in the **General tab** of Device Properties
- Using the **Schedule Manager** to complete a config pull
- Using the option in the **Devices View** right-click menu

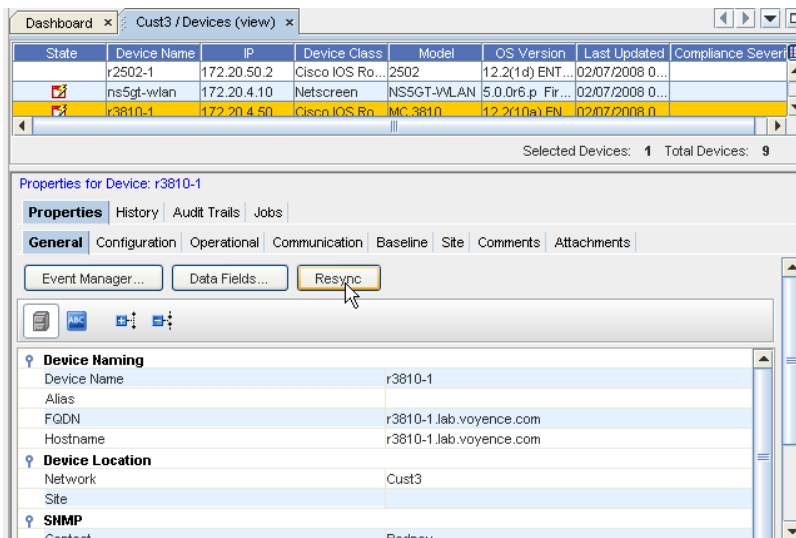
---

**Important** Make sure you refresh the Devices view after each resync is completed .

---

Using the Resync button,

- 1 To bring a single device, or **multiple devices** configuration back into "sync", display the devices using the Table layout.
- 2 From the Navigation tree, display the listing of devices to determine if you have any devices out of sync, as indicated by the icon  in the **State** column.
- 3 Next, select that single device, or select multiple devices from the list, then click the **Properties** icon on the menu bar.

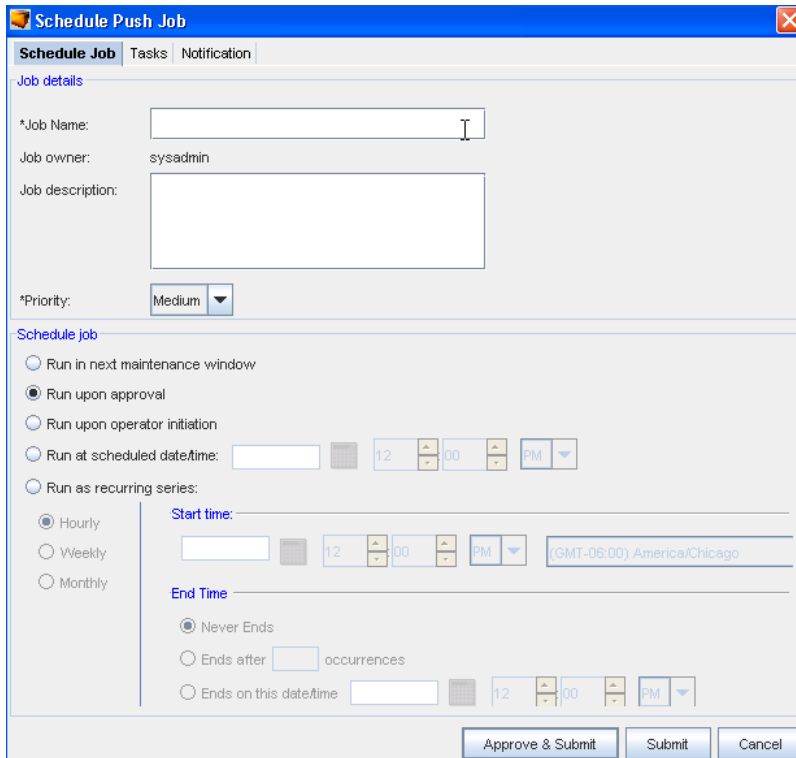




---

**Note** This Resync button is only available if there are any "out-of-sync devices" in the Device list.

---

- With the Device Properties displayed, go to the **General** tab. With the device selected, click the **Resync** button. The **Schedule Push Job** window opens, where you complete the information needed for the push job.



- See [Schedule Push Job](#) for details on how to complete this action, including how to work with each tab.
- After the application completes a Config pull (to bring the device configuration into sync) **select the Refresh icon**  to refresh your Devices view.

---

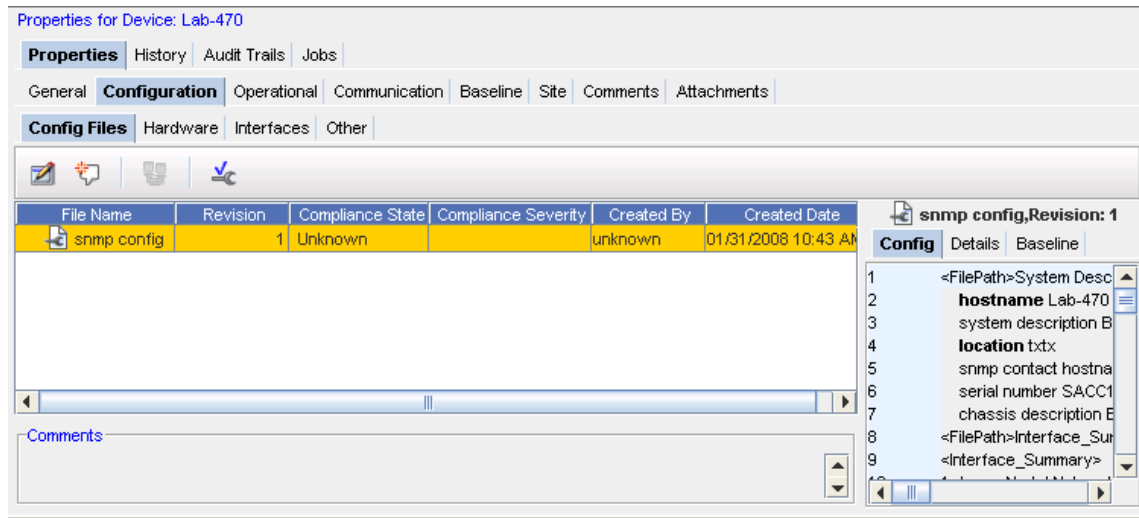
**Note** The device is no longer in the "out-of-sync" state in the Devices View. This indicates that the device's running configuration is now identical to the start-up configuration .

---

## The Configuration Tab

### Configuration Tab Overview

From the Devices View, when Properties is selected from the tool bar, the **Configuration** tab is available.



From this tab you can access:

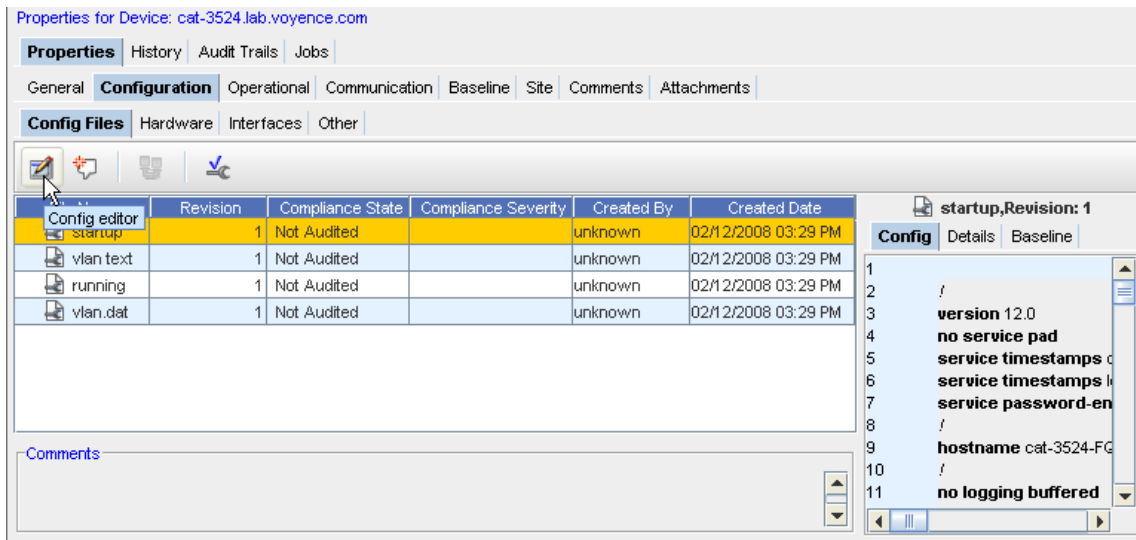
- Config Files
- Hardware
- Interfaces
- Other

### Config Files

#### Accessing and working with Config Files

To make changes to the Config file,

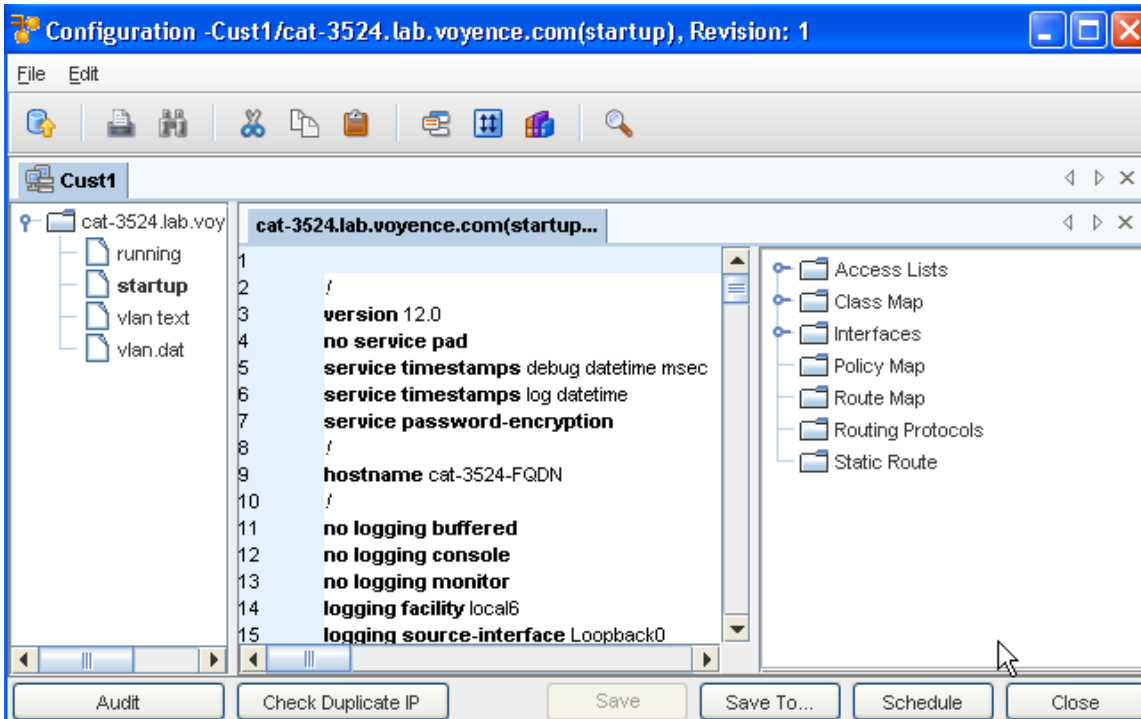
- 1 In the **Config Files** tab in the **Configuration** section of the **Device Properties**, select a running config, and then click the **Config Editor** icon.



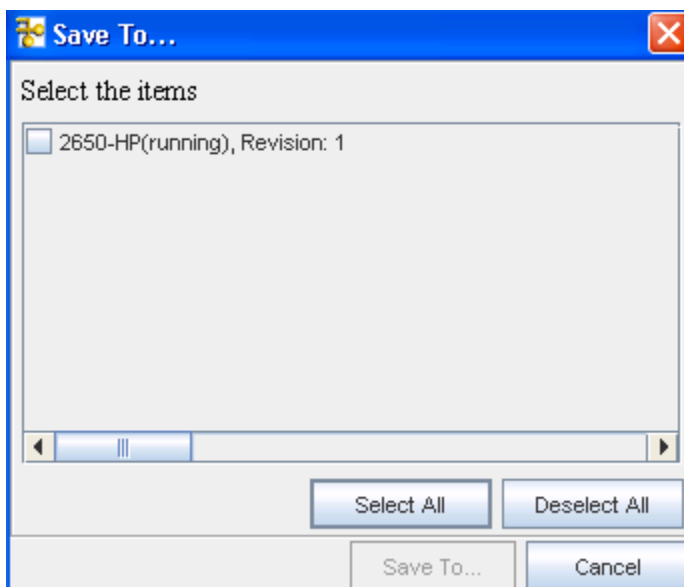
The Config Editor window opens.

- 2 Make any needed revisions to the information.

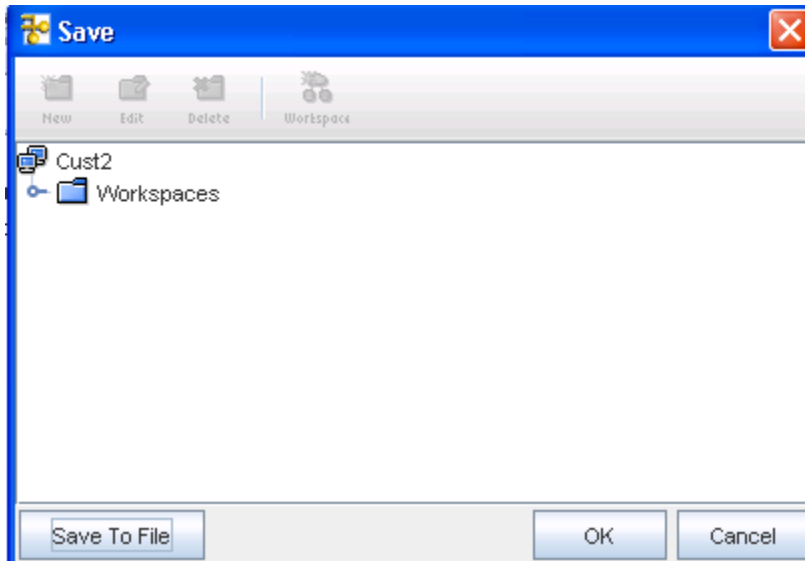
- Click **Preview**  to preview your changes, and then click **Save To...**, to save your changes.



- From there, in the **Save To..** window (shown below), you can select the items to save by clicking in the check box beside each device, or by using the **Select All** bar., then clicking **Save To....**



- Now, use the **Save** window to determine where you want to save this.

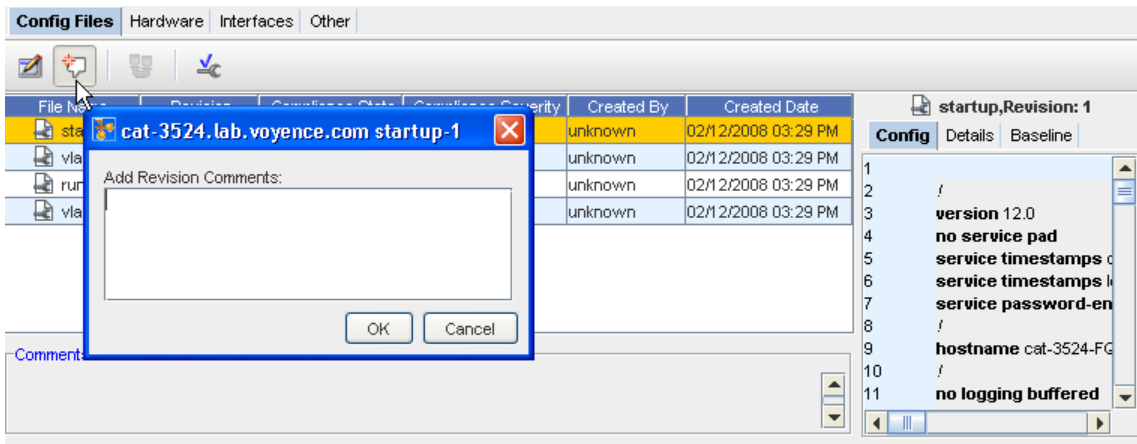


6 Click **Ok** when you have Saved your config.

### Adding a New Comment

To add revision comments,

1 In the **Configuration** tab, click the **New** icon to see the Revision Comments window for that device.



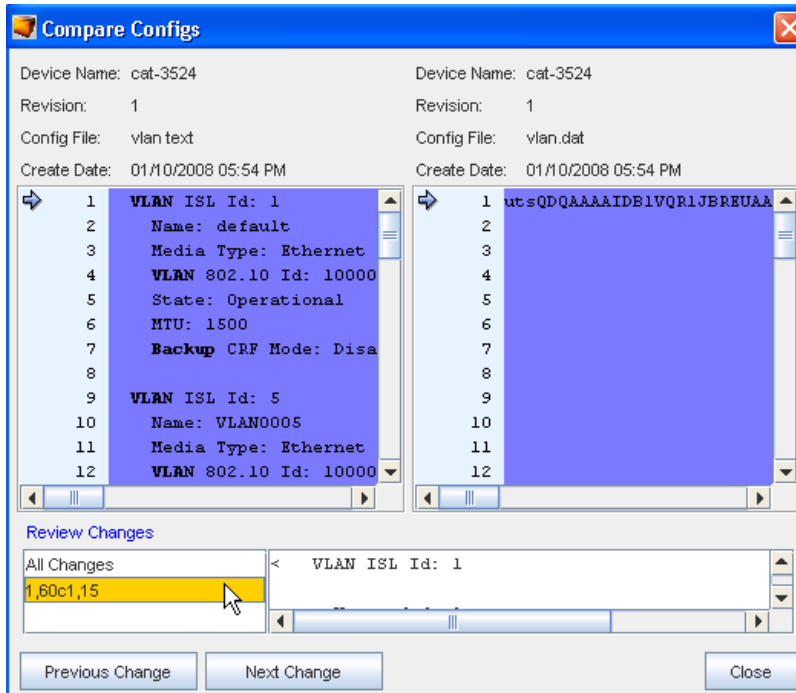
2 Enter any new comments in the Add Revision Comments window, then click **OK**. Your latest comments are now added to the top of the comments window.

### Comparing Device Revision Configs

1 From the **Baseline** tab, select two revisions , then click the **Compare Device Revisions** icon



. At the Compare Configs window, you can compare the difference in configurations.



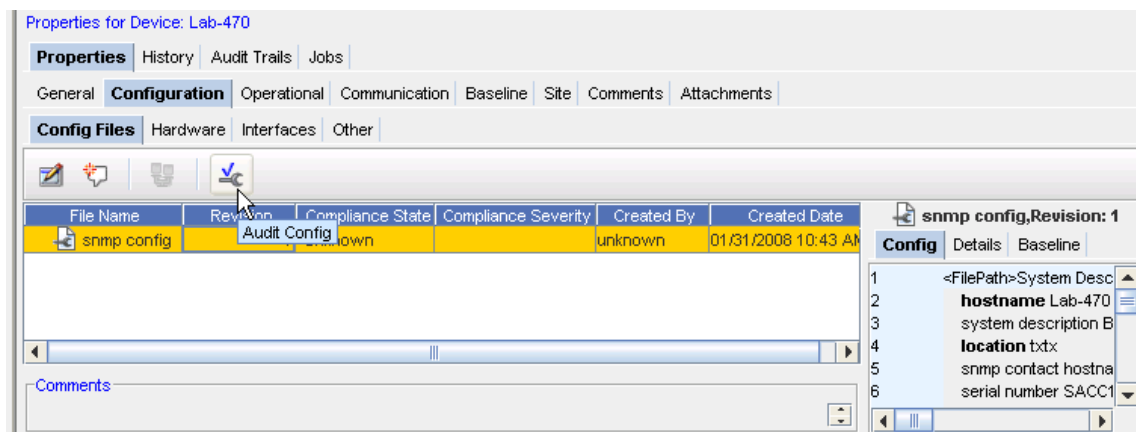
- 2 You can also select to view **Previous** and **Next** changes, or click within the **Review Changes** window.
- 3 Click **Close** when you have completed your review of this information.

### Audit Configuration



You can see which of the configurations are **Compliant** or **Non-Compliant** by the icons displayed in the Compliance State column.

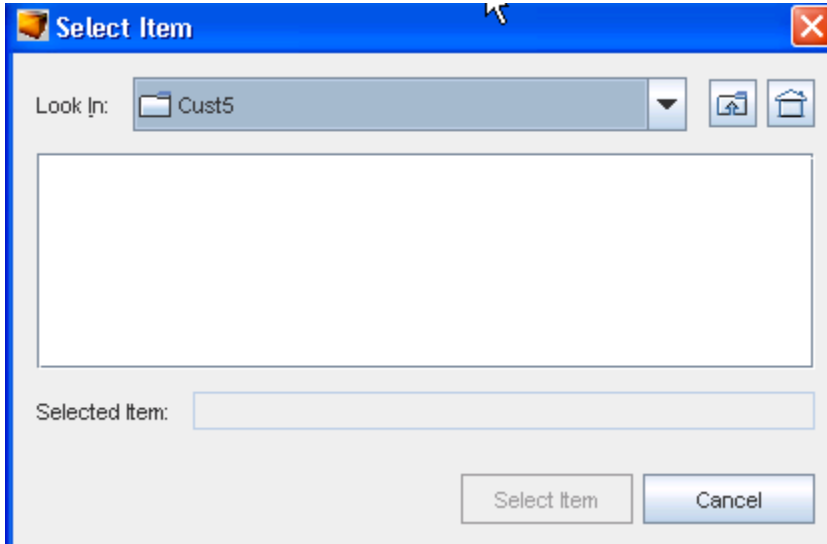
To complete an Audit,

- 1 From the **Configuration** tab,select a Revision, then select the **Audit Config** icon.

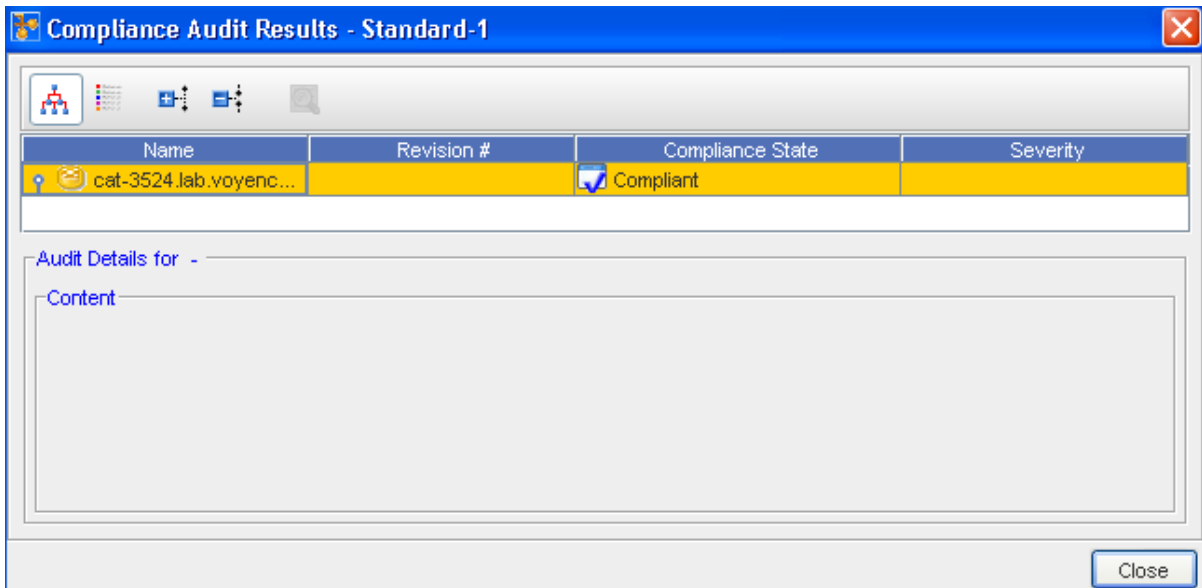


- From the Select Item window, click the drop-down arrow.

**Note** You can use the two icons   (Up one Level and Home) to expand or contract the listing contents.



- Make your selection from the list, then **select** the Item.
- At the Compliance Audit Results window, your results are displayed.



**Note** **Green** is Compliant, and **red** designates Non-Compliant.

- Click **Close** when you have reviewed the audit results.

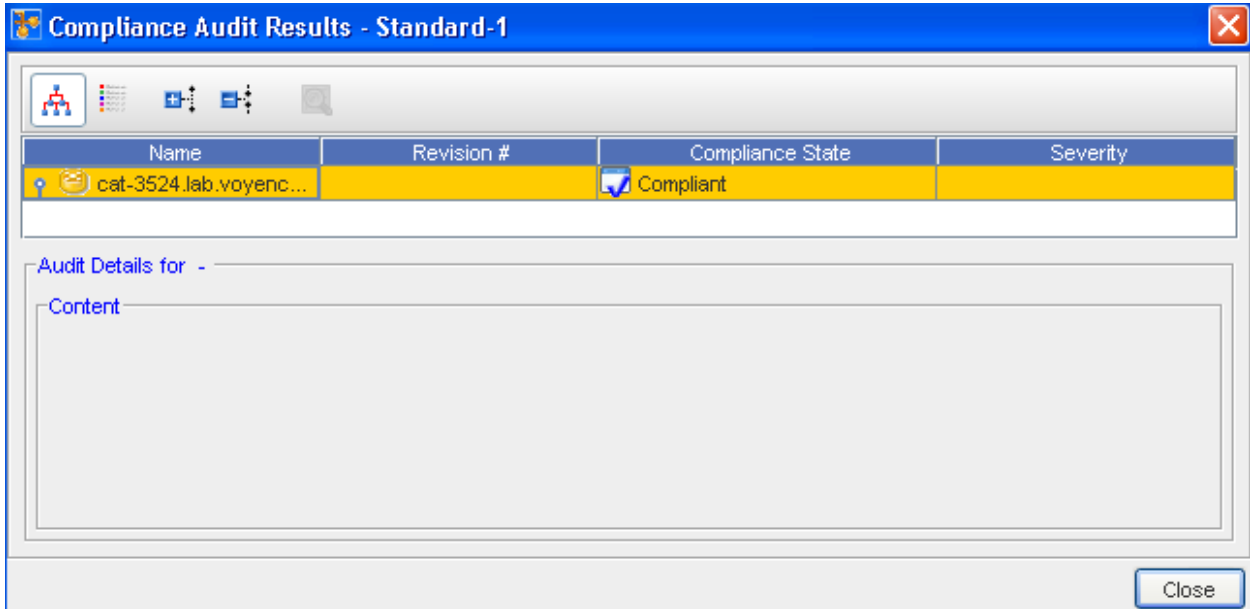
See [Audit Compliance Window](#) for additional information.

#### **Audit Compliance Window**

- To work within the **Audit Compliance Results** window, first select the device from the listing.



2 Next, use the icons to view or hide information, or to rearrange the order of devices.



Move your cursor over the icons to view the various options.


You can see the Compliance State.

## Hardware

### Hardware Information

The **Hardware** information can be viewed from within the Configuration tab when Device Properties are displayed.



- You can Categorize or put in Alphabetical order
- You can also select to Show  or Hide the hardware description (located at the bottom of the form).

The screenshot shows the Network Configuration Manager interface with the **Hardware** tab selected. Under **Physical Hardware**, the **Memory** and **File System** sections are visible. A table displays the following information:

Chassis	Cisco Catalyst c2950 switch with 24 10/100 BaseT...
Description	Cisco Catalyst c2950 switch with 24 10/100 BaseT...
FirmwareVersion	12.1(22)EA4
HardwareVersion	B0
Model	WS-C2950-24
Revision	12.1(22)EA4
SerialNumber	FAB0530W1LX
Memory	
Port	10/100BaseTXFast Ethernet
Port	10/100BaseTXFast Ethernet
Port	10/100BaseTXFast Ethernet
Port	10/100BaseTXFast Ethernet

Below the table, the **SerialNumber** FAB0530W1LX is displayed in a separate box.

Note that you can access both Memory and File System information.

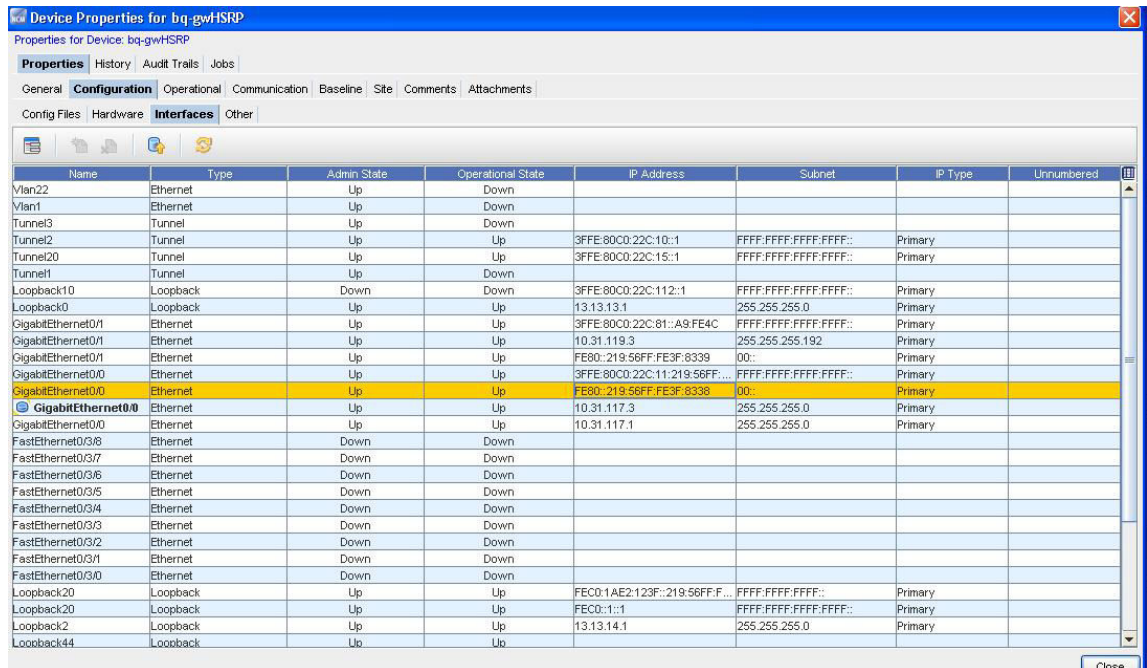
- 1 Click **Memory** or File **System** (under the **Physical Hardware** heading).
- 2 Click **Close** when you have viewed the Device OS information.

## Interfaces

### Interfaces tab (within Configuration)

The **Interfaces** tab provides a listing of all the **physical and logical** interfaces that are configured on the selected device, including their status. The Management interface is the Interface IP used to manage the device in Network Configuration Manager. Management Interfaces can be changed from this tab.

This information can be displayed by selecting the **Properties** icon, and from the **Configuration** tab from the Device Properties.



The **Interfaces** tab provides a listing of all interfaces that are defined in the config file. This tab details the interfaces information, including Name, Type, Admin State, IP Address, Subnet Mask, Tags, and DNS Interfaces.

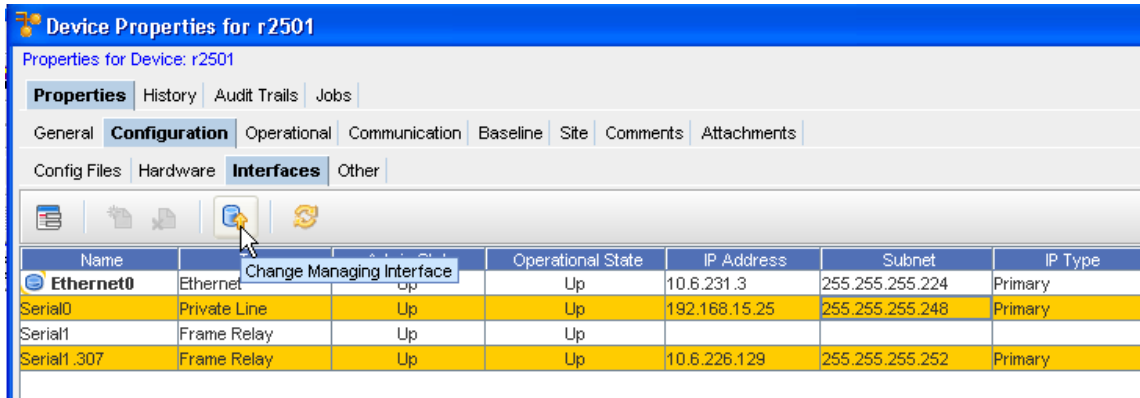
The Interfaces tab also allows you to [Viewing or Updating a Data Field from the History or Interfaces tab](#) for a specific interface.

**Note** Notice that the **Add** and **Delete**, as well as the **Change Managing Interface** icons are grayed out. You cannot add, delete, or change the managing interface anywhere but **within a Workspace**.

To manage the Interfaces, see [How to Managing Interfaces](#)

To change the managing interface,

- 1 Select an **IP Address** from the list that you want to change to the current managing interface . When you select another IP Address from the list of addresses, the **Change Managing Interface** icon is enabled.
- 2 Click the **Change Managing Interface** icon.



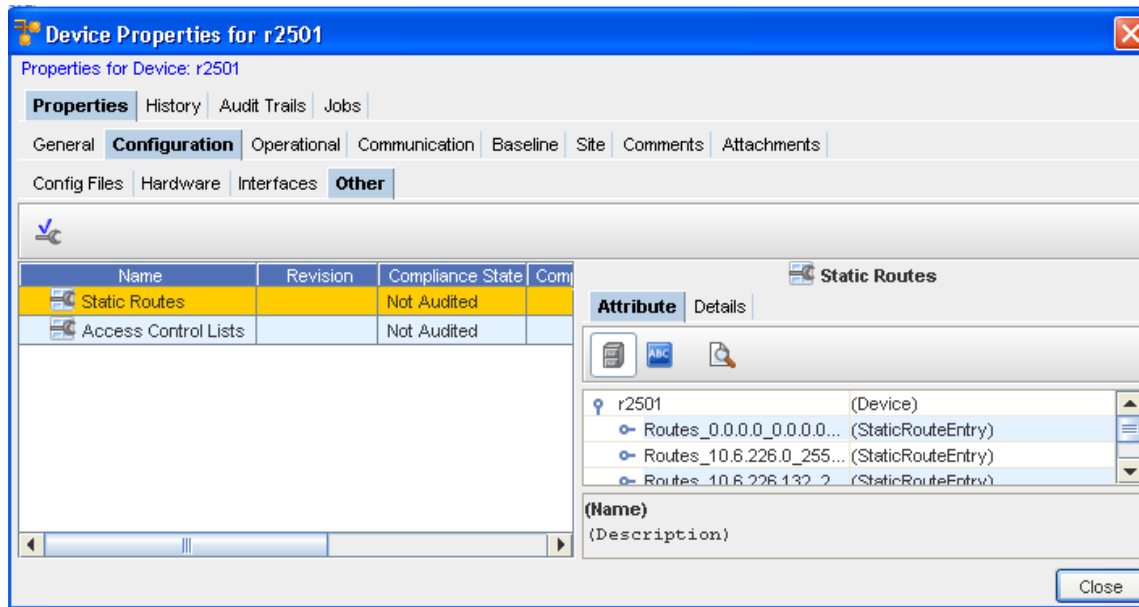
- 3 At the confirmation message, click **Yes**.
- 4 Click **Close** to close this window.

**Note** When you change the IP Address, a Config Pull and a Spec Pull are automatically scheduled, and a notification is sent to you if a Warning or Failed state occurs.

## Other

### Other Overview

This section is designated to store additional information that may not have a specific category. For example, information included here does not fit categorically into the Hardware or Interfaces informational classes.



In this instance, the "other" information consists of Statics Routes.

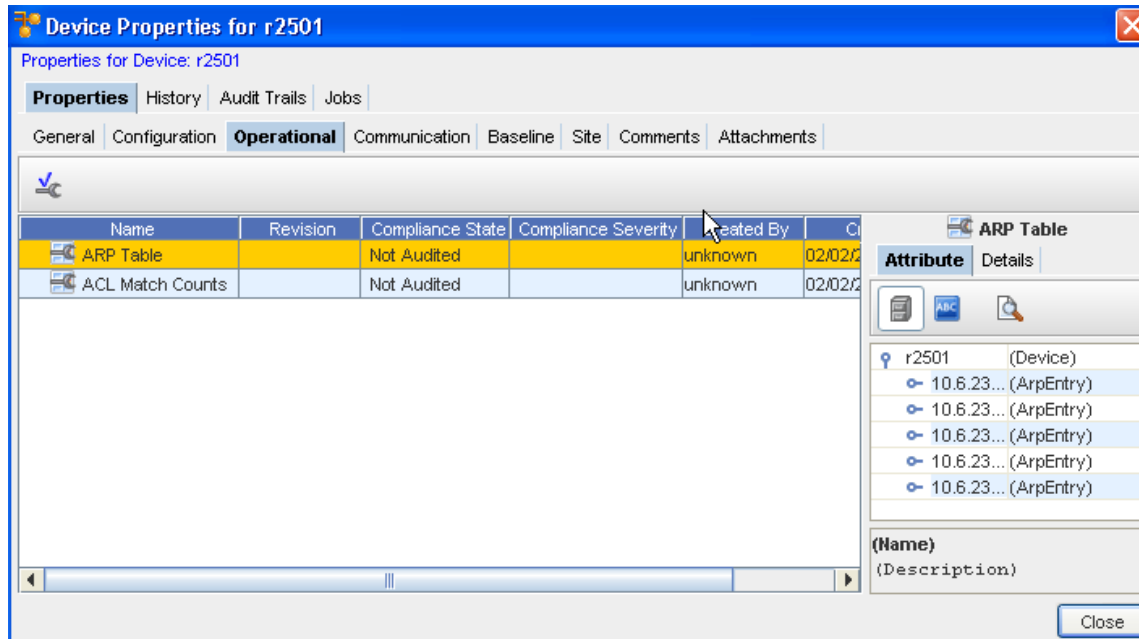
## Operational Units

### Operational Units Tab Overview

This displays a generic table listing of all configuration units that are not marked as "revisionable", and mostly contains the attributed units.

Typically, these operational units are not expected to be used for **rollback**. Note that there are configuration units that are revisionable, but yet not available for rollback. For instance, Hardware and Diagnostic Results.

Viewing this tab allows you to view additional information on the table, by clicking the **Attribute** and **Details** tabs.



The only task that can be completed from this tab is an **Audit** on the Config. See [Running a Compliance Audit](#) for more information and procedures to complete this task.

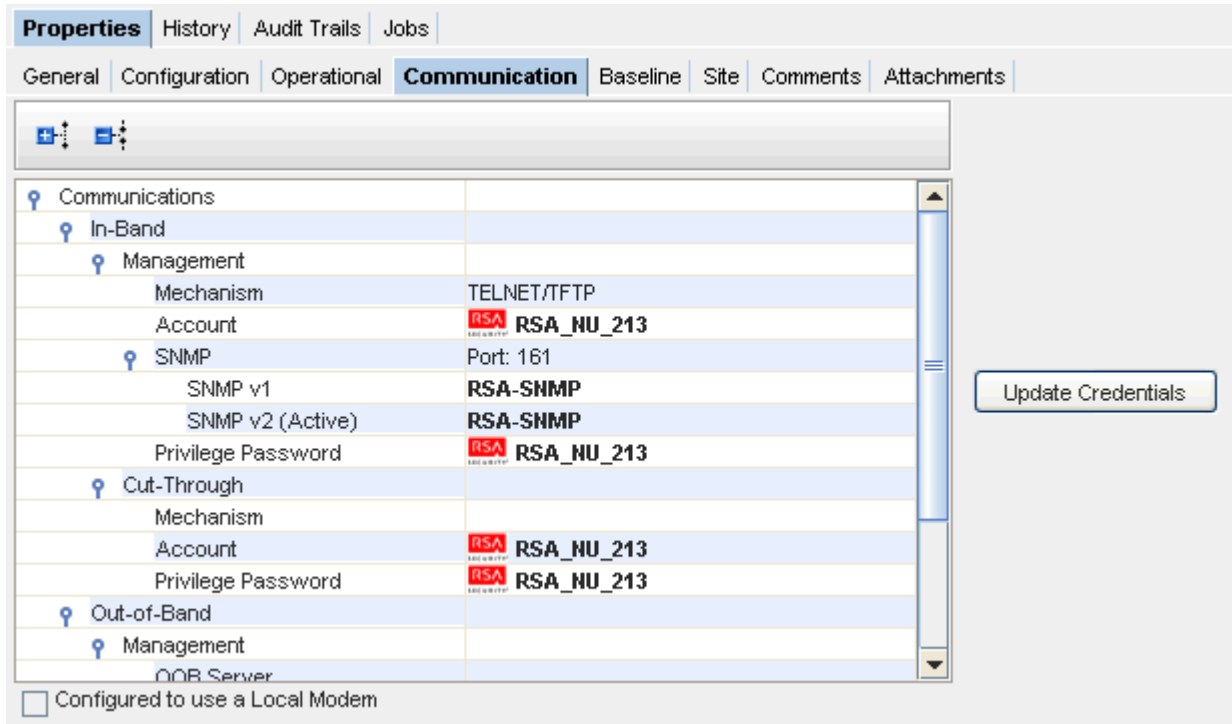
## The Communications Tab

### Communication Tab Overview

This tab can be displayed by selecting the **Properties** in the menu bar when you are in a Devices View or in a Workspace.

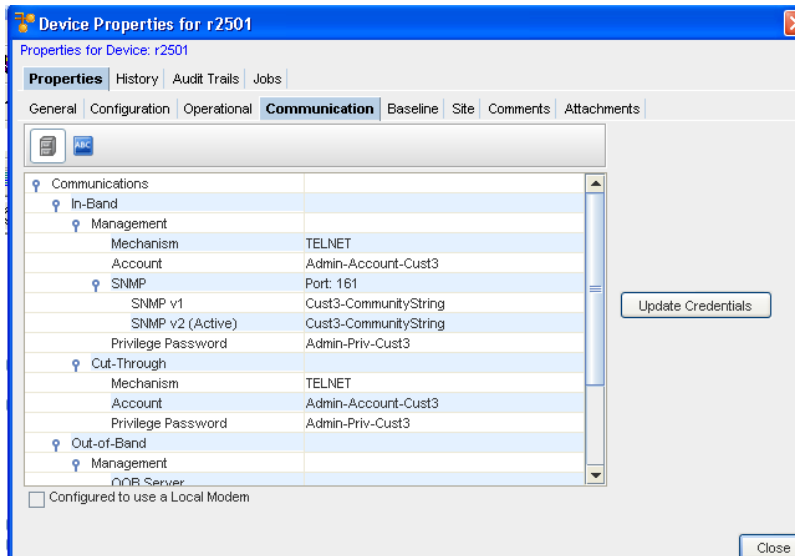
From this tab you can view your In-Band and Out-of-Band Communications, Management, Account, SNMP and Cut-Throughs. You can also **Update Credentials**.

The Communication tab allows you to manage the mechanisms for SNMP, Telnet, Telnet.TFTP, and both In-band and Out-of-Band communications with the device.



**Note** The **Configured to use a Local Modem** check box is only available if you have previously enabled a local modem.

### Editing In-Band Communications



To Edit In-Band,

- 1 Click the **Update Credentials** bar to get to the Update Credentials window.
- 2 Select the **In-Band** tab.

- In the **Management** section, you can select from the options in the following drop-down lists:
  - Mechanism
  - Account Credential
  - Privilege Password
- In the **SNMP Credentials** section, you can select from the options for SNMP Credentials:
  - SNMP Port - or no change
  - SNMP v1, v2, or v3, and select these to be Active
- In the **Cut-Through** section, you can select from the options in the following drop-down lists:
  - Mechanism
  - Account Credential (this can either be **User Prompted** or **User Account**).
  - Privilege Password
- When you have made selections for both Management and Cut-Through, you can then click **Schedule** to push your changes to the devices, or click **Save Only** to update the database associations only.

---

**Note** You can click **Cancel** to leave this window and cancel any selections.

---

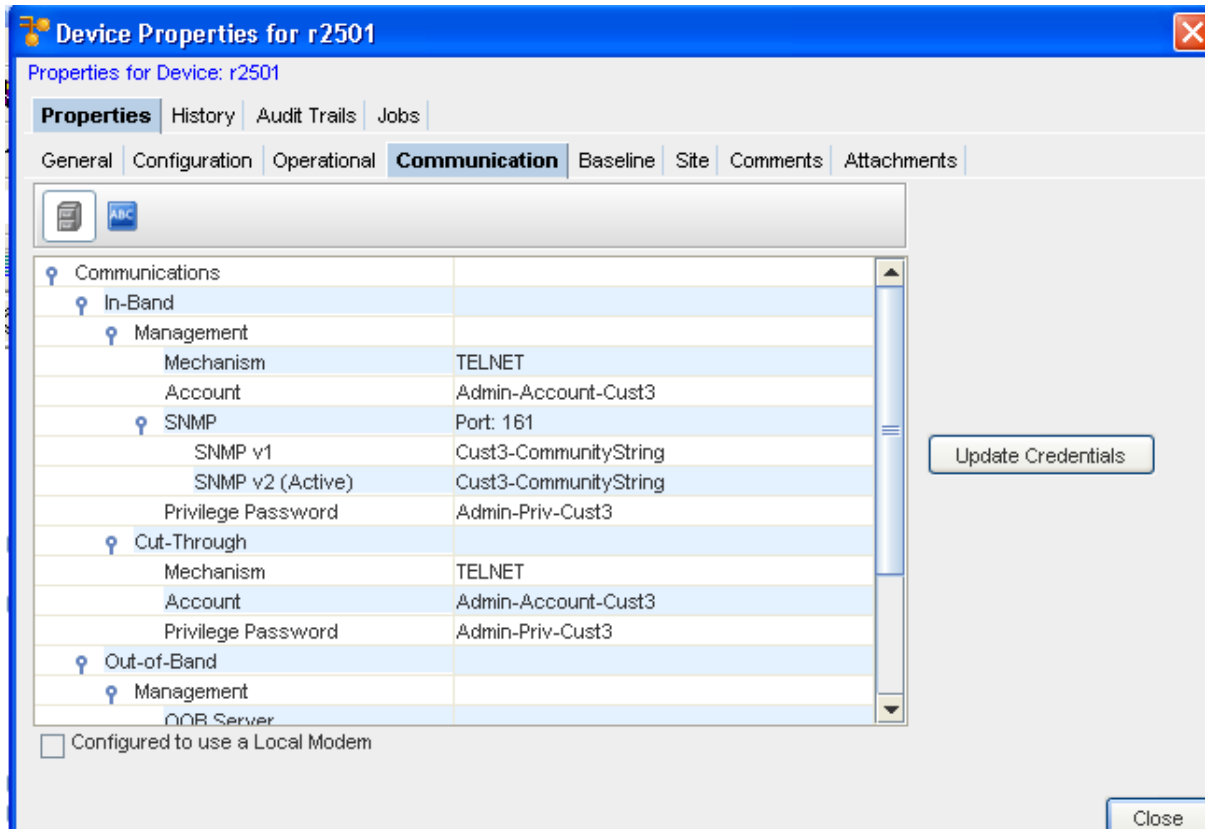
**See:** [Edit Out-of-Band](#)

## Managing Device Communications

Setting credentials at the device level allows you to override the network and system credentials to which other devices in your network respond.

To set credentials at the device level,

- 1 With a workspace displayed, select a **device**, then right-click to go to **Properties**.
- 2 With the Properties window displayed, select the **Communications** tab.



- 3 Select the **Update Credentials** button, then click the **In-Band** tab.



Update Credentials

Click "Schedule" to push your changes to the device(s).  
Click "Save Only" to only update the database associations.

**In-Band** Out-of-Band

In-Band Communications

**Management**

Mechanism: No Change

Account Credential: No Change

Privilege Password: No Change

**SNMP Credentials**

SNMP Port:   No Change

SNMP v1: No Change  Active

SNMP v2: No Change  Active

SNMP v3: No Change  Active

**Cut-Through**

Mechanism: No Change

Account Credential: No Change

Privilege Password: No Change

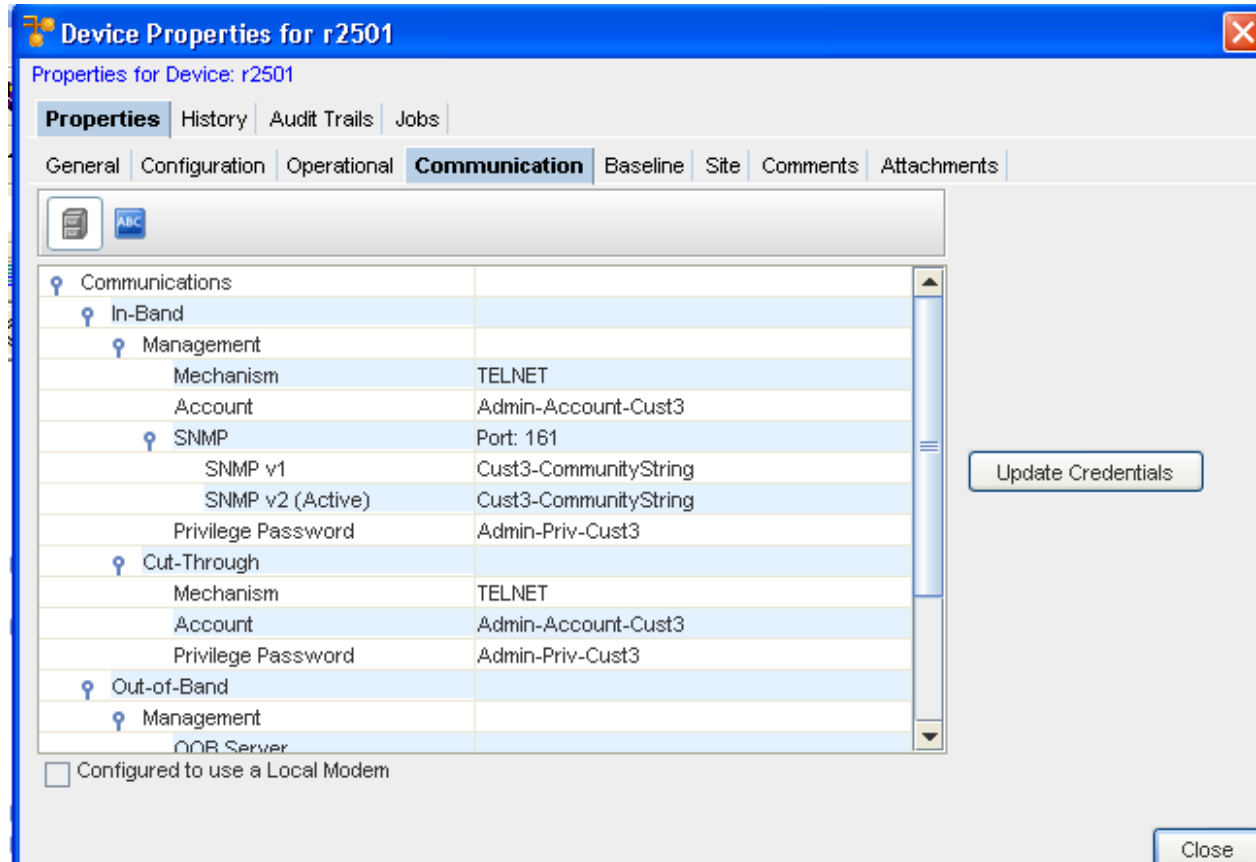
Schedule Save Only Cancel

- 4 Make your needed changes within each section of this window, then click **Ok**.

### Managing and Viewing Privilege Password Levels

Privilege Password levels associated with Devices determines the level of access and activity a user can have pertaining to any one device. Users are limited to the device tasks they can complete, based on their Privilege level.

- 1 From a table view of the Devices, click **Properties**, and go to the **Communications** tab.
- 2 In the information section, you can view all Privilege Passwords associated with this device.
- 3 You can use the **Expand** and **Collapse** icons to display information. You can also select [Updating Credentials](#) to make changes to the current credentials.



**Note** Multi-level can have **more than one** Privilege Password per device. Single-Level can have **only one** Privilege Password per device.

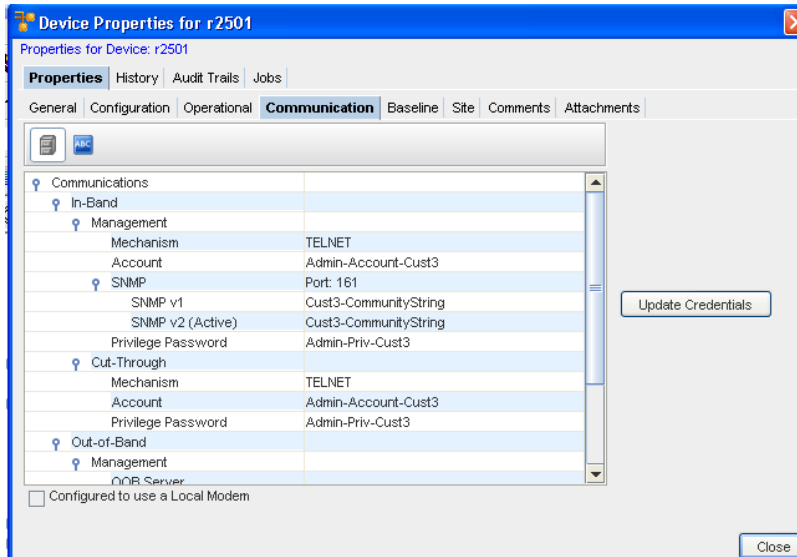
### Updating Credentials

**Important** You will only be allowed to Update Credentials using the **Update Credentials** bar on this **Communication** tab if you have previously been granted the appropriate permissions from your System Administrator. If the Update Credentials bar is grayed out, you do not have the appropriate permission.

**Note** You can also use the **Override** button on the **Schedule Manager** menu bar to get to the Update Credentials windows.

Updating Credentials on Multi-Levels includes the following process.

- 1 From the devices view, select the **devices** that support levels.
- 2 Select **Communications** from the Device Properties tab.
- 3 Select **Update Credentials**.



At the In-Band tab,

- 1 At the Update Credential window, you can select either In-Band or Out-of-Band tabs.

---

**Note** You have the option of selecting to **Schedule** to push your changes to the devices.

---

Click "Schedule" to push your changes to the device(s).  
Click "Save Only" to only update the database associations.

**In-Band** Out-of-Band

**In-Band Communications**

**Management**

Mechanism: No Change

Account Credential: No Change

Privilege Password: No Change

**SNMP Credentials**

SNMP Port:   No Change

SNMP v1: No Change  Active

SNMP v2: No Change  Active

SNMP v3: No Change  Active

**Cut-Through**

Mechanism: No Change

Account Credential: No Change

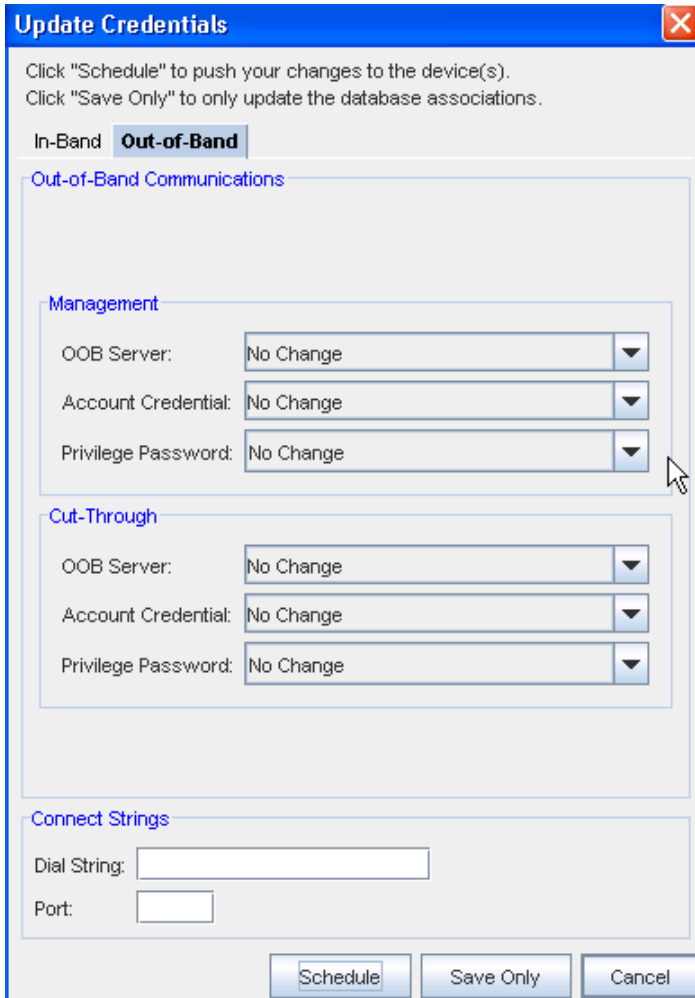
Privilege Password: No Change

Schedule Save Only Cancel

- 2 In-Band tab, make the selections from the drop-down arrows in the **Management** section:
  - Mechanism
  - Account Credential
  - Privilege Password
- 3 Make the selections from the drop-down arrows in the **SNMP Credentials** section:
  - SNMP Port
  - SNMP v1, v2, or v3, and select these to be Active
- 4 Make the selections from the drop-down arrows in the **Cut-Through** section:
  - Mechanism
  - Account Credential (this can either be **User Prompted** or **User Account**).
  - Privilege Password
- 5 Select to Schedule, Save Only, or Cancel the information you have selected from this window.

At the Out-of-Band tab,

- 1 At the Update Credential window, you can select either In-Band or **Out-of-Band** tabs.



- 2 At the Out-of-Band tab, make the selections from the drop-down arrows in the Management section:
  - Out-of-Band (OOB) Server
  - Account Credentials
  - Privilege Password
- 3 From the **Cut-Through** section, make your selections from the:
  - Out-of-Band Server
  - Account Credential
  - Privilege Password
- 4 At the **Connect String** section:
  - Enter a Dial string

- Enter a Port Number
- 5 When you have made selections for the Management, and Cut-Through sections, and entered the needed information in the Connect String section, you can then click **Schedule** to push your changes to the devices, or click **Save Only** to update the database associations only.

---

**Note** You have the option of selecting to **Schedule** to push your changes to the devices.

---

## The Baseline Tab

### Baseline Tab Overview

When a Network is baselined, the current revision for all devices in that Network are tagged. A baseline allows you to create a production state for all device in the Network, providing a quick mechanism to rollback any device configuration to its defined production revision.

Baselines are created in Network properties. A Network rollback to any baseline can be executed from Network properties.

---

**Important** A Baseline must have already been set for the Network.

---

The Baseline tab allows you to review the **network baseline config** that affects the device.

This tab can be displayed by selecting the **Properties** in the menu bar when you are in the Device's View.

The screenshot displays the 'Properties for Device: HP4000' window with the 'Baseline' tab selected. The main area contains a table with the following data:

DCS #	Revision	Compliance State	Compliance Severity	Created By	Created Date
No B...		Not Audited			
<b>Current</b>	1	Not Audited		unknown	03/23/2009 11:3

Below the table is a 'Comments' section with the text: 'Configuration units not pulled but required for completeness: [running, ]'. On the right side, a 'Details' panel shows the following information:

- Current DCS, Revision: 1**
- General**
  - Revision: 1
  - Job Num...: 0
  - Task Num...: 0
  - Complete: False
- Compliance**
  - Compliance State: Not Audited
- Creator**
  - Created By: unknown

- From this tab you can add **comments**
- **Roll back to the** previous device settings

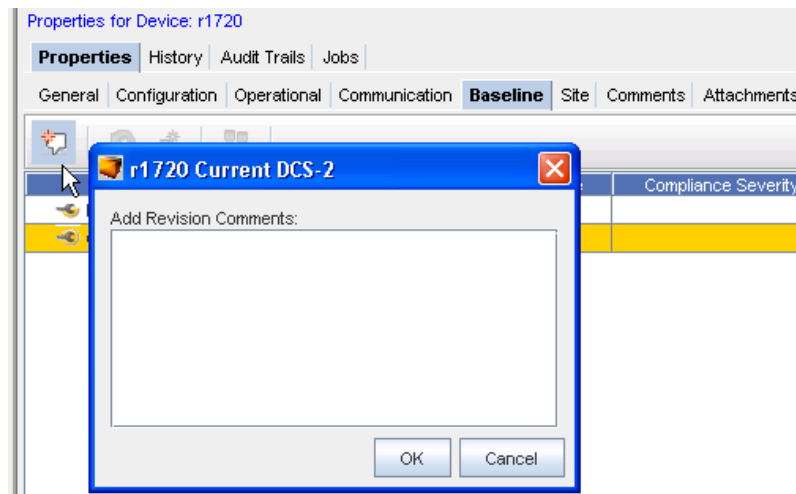
- **Set the current revision** as the baseline
- **Compare** revisions
- View the compliance state

### Adding Baseline Revision Comments

While in the Baseline tab, you can add additional comments to the current baseline.

- 1 Select from the **Device Configuration State Number** from the listing ( **DCS#**), then click the **Add Revision** icon.
- 2 At the Add Revision Comments: section, enter any comments you may have on this current state.
- 3 Click **Ok** when you are completed.

Your comments are now at the top of the Comments listing.




### Rolling back to Baseline

**Important** A Baseline must have already been set for the Network.

From the **Baseline** tab in the Device Properties, you can access the **Roll Back** icon. This allows you to rollback to the previous device settings.

To Roll back to the Baseline,

From this window, you can roll back to the baseline - back to the beginning.

- 1 Click the **Roll Back** icon  to display the Schedule Push Job window.
- 2 From here, you can make any need revisions to the **Job Details**, **Schedule Job Details** , and revisions to **Tasks** and **Notification** if needed. For more information, go to [Using the Scheduler](#).

- 3 After making your revisions, or adding additional information, click **Submit**. This starts your job in the process, with your revisions.

---

**Note** Each device packaged in Network Configuration Manager defines its own Roll back procedure. For example, for Cisco Devices, this is to push the content to the Start Config. Doing this will not affect the running config of the device. Also, the device must be rebooted for it to take affect.

---


### Setting the Current Revision to Baseline

---


**Important** A Baseline must have already been set for the Network.

---

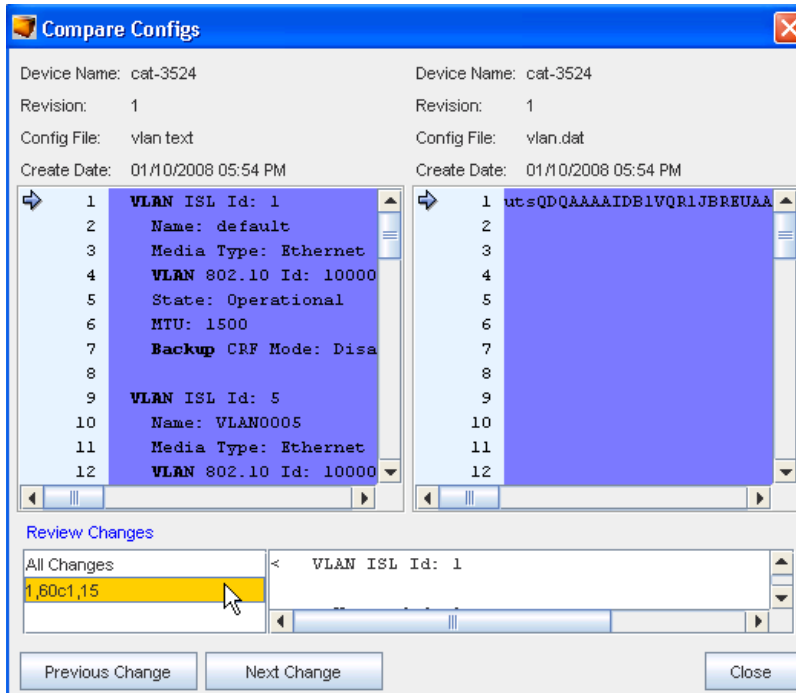
- 1 From the Baseline tab in the Device Properties, you can access the **Set Current Revision to Baseline** icon to set the baseline to the current configuration version.
- 2 After selecting a Device from the Devices View, then selecting the **Properties** icon, you can then access the **Baseline** tab.
- 3 If there is more than one revision shown (in the **Revision** column) you can promote the latest revision. For example, if you have two revisions shown; a number 1 and a number 2, then you can surmise that changes to the baseline have been made, and you need to promote the latest baseline revision (2).
- 4 Select the latest revision.

- 5 Click the Set Current Revision to Baseline icon  to set the current configuration version. This will then be the current baseline configuration for the Device.

### Comparing Device Revision Configs

- 1 From the **Baseline** tab, select two revisions , then click the **Compare Device Revisions** icon  . At the Compare Configs window, you can compare the difference in configurations.





- 2 You can also select to view **Previous** and **Next** changes, or click within the **Review Changes** window.
- 3 Click **Close** when you have completed your review of this information.

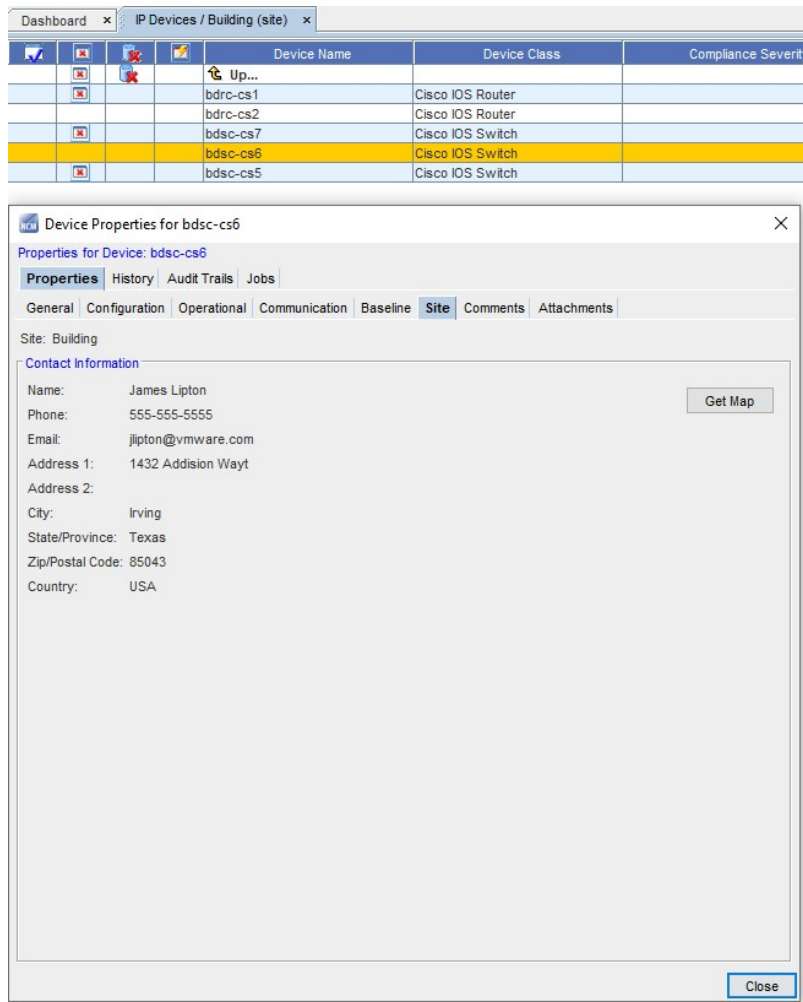
## The Site Tab

### Site Tab Overview

When a device is placed in a hierarchical Site structure, location and contact information can be entered that will be inherited by any devices within that Site. When address information is available for the device, clicking the Get Map option will display a **MapQuest map** of the Site.

This window can be displayed by selecting the **Properties** icon in the Devices View tool bar.

- The site information displays when the **Site** tab is selected.
- The **Site** tab allows you to review the Site information, if a device has already been assigned to a site.



**Note** When the contact information is displayed, you can click **Get Map** to go to the "map finding" feature for directions to that specific Site. For example, you may be directed to the MapQuest link.

See [Adding Site Information](#) for more details.

### Adding Site Information

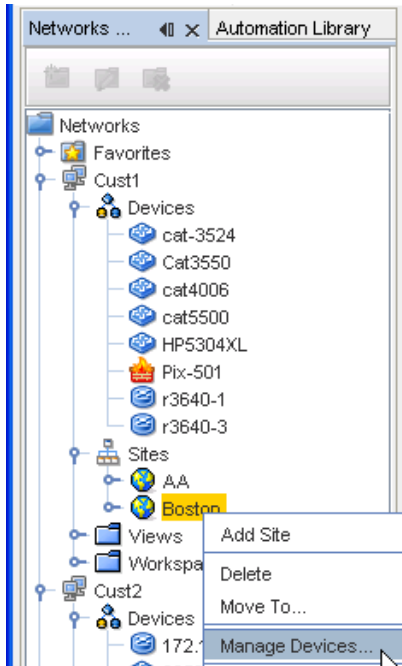
To add Site information,

- 1 Select **Site**, then right-click to select **Add Site** from the Navigation pane.

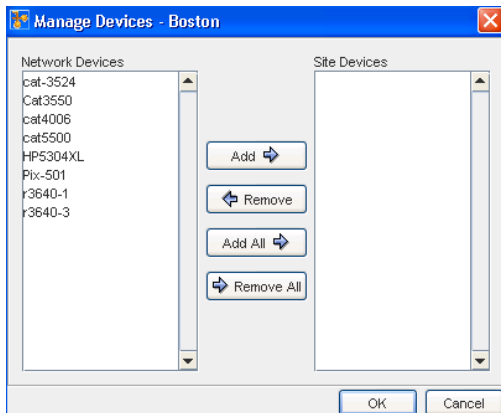
The screenshot shows a 'New Site' dialog box with the following fields and controls:

- \*Name:** A text input field.
- \*Type:** A dropdown menu showing 'Geograp...' and a globe icon.
- Description:** A text area with a vertical scrollbar.
- Override:** An unchecked checkbox.
- Contact Information:** Text input fields for 'Contact Name:', 'Contact Phone:', and 'Contact Email:'.
- Address Information:** Text input fields for 'Address 1:', 'Address 2:', 'City:', 'State/Province:', 'Zip/Postal Code:', and 'Country:'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

- 2 At the New Site window, enter the information needed.
- 3 Click **Ok** when you have entered all the information you want visible in the Site tab of the Devices Properties.
- 4 Now, from the Navigation pane, select the site you just created, then right-click to select **Manage Devices**.



- From the Manage Devices window, select the devices you want to add to the Site. Use the **Add** or **Add All** arrows.



- Click **Ok** when you have completed moving devices into the Site Devices pane.

## The Comments Tab

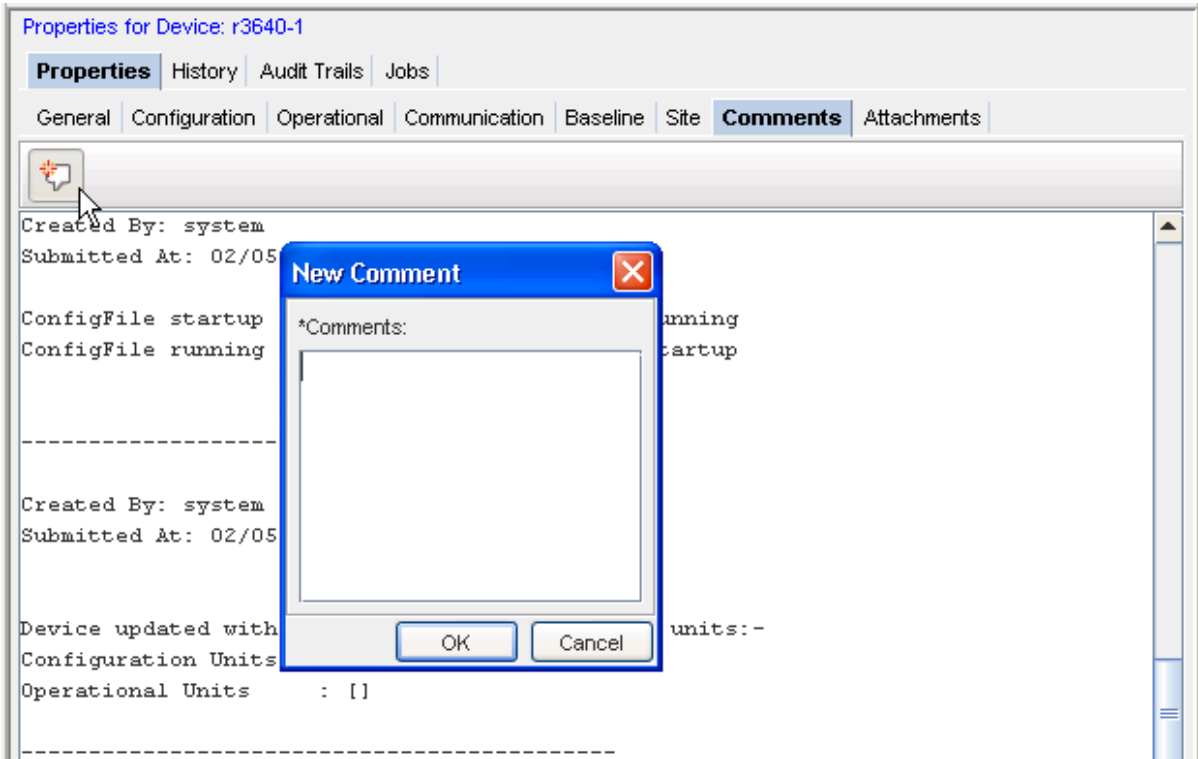
### Comments Tab Overview

The Comments tab allows you to enter device-specific comments. This tab can be displayed by selecting the **Properties** icon in the menu bar. From this tab you can add new comments.

To add a new comment,

- With the Device Properties displayed, select a **device** from the Devices View.
- In the Comments tab, click the **New** icon. The New Comments window opens.

- 3 Enter your comments, then click **Ok** to add this new comment. Each comment is recorded in this section by the date the comment was entered.

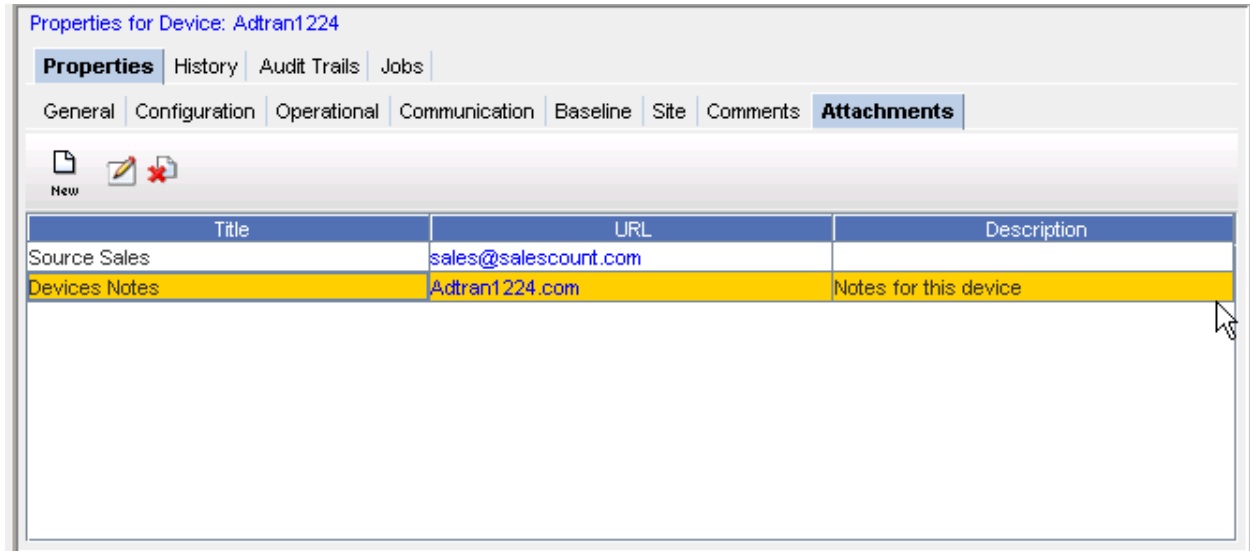


- 4 Click **Cancel** to close this window without saving your comments.

## The Attachments Tab

### Attachments Tab Overview

The Attachments tab allows you to associate an external file to the network.



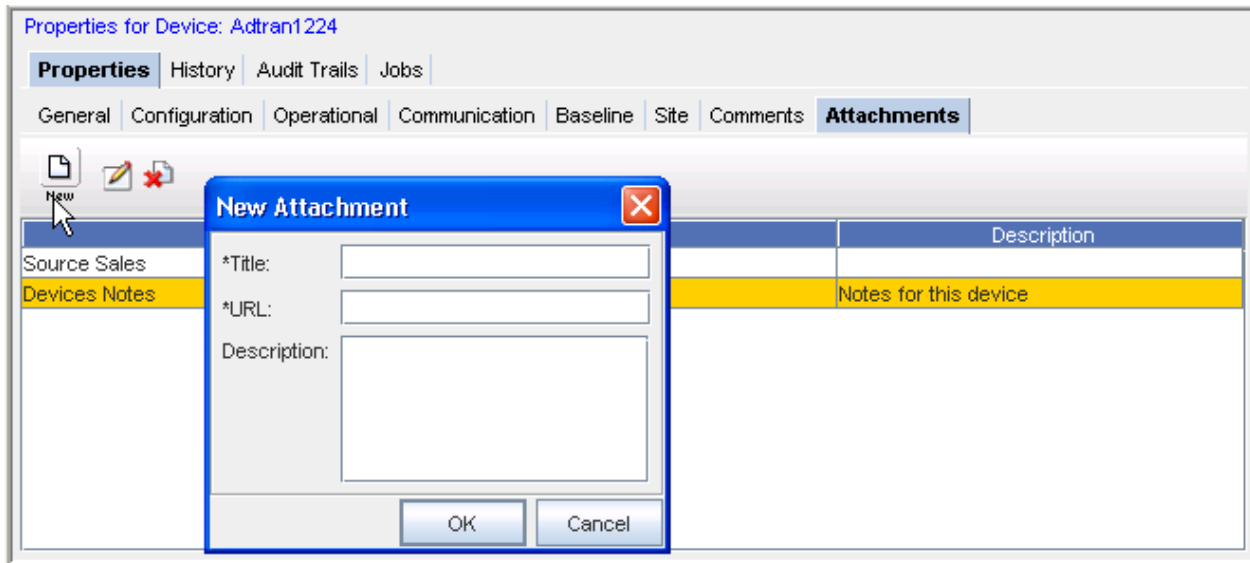
This tab can be displayed by selecting the **Properties** icon in the menu bar when you are in a Workspace or Devices view.

From this tab you can:

- [Adding an Attachment](#)
- [Editing an Attachment](#)
- [The Dashboard](#)

### Adding an Attachment

To add an attachment,



To add an attachment,

- 1 On the Attachments tab, click the **New** icon. The New Attachments dialog window opens.

- 2 Enter a **title** for the attachment.
- 3 Enter a **URL**. Remember the document must be saved in a format that will open in a browser.
- 4 If needed, enter a **Description**.
- 5 Click **OK**. The New Attachments window closes.
- 6 For each new attachment, repeat **steps 1-5**.

**Note** The Edit and Delete icons are only active when one or more attachments have been created.

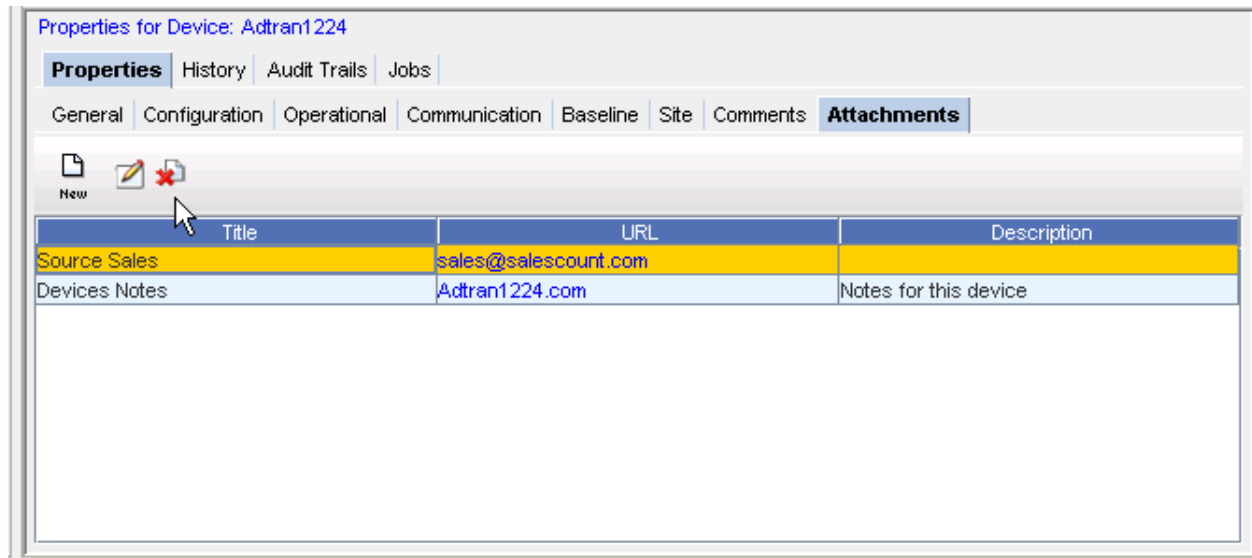
### Editing an Attachment

To edit an existing attachment,

- 1 First, select an **attachment** from the listing of attachments.
- 2 On the Attachments tab, click the **Edit** icon. The Edit Attachments dialog window opens. The Title, URL and Description fields can all be edited.
- 3 Make any changes as needed.
- 4 Click **OK**. The Edit Attachments window closes.

The attachment row updates with the edited details.

### Deleting an Attachment



To delete an attachment,

When deleting an attachment, the actual document that you are referring to is not deleted. You are removing its **linked reference** from Network Configuration Manager.

- 1 First, select an **attachment** from the listing of attachments.

- 2 On the Attachments tab, click the **Delete** icon. The Confirm dialog window opens asking, "Are you sure?".
- 3 To delete, click **Yes**.
- 4 Click **OK**. The Confirm window closes.

The Attachment tab refreshes.

## Working with Global Device Search

### Global Device Search Overview

The **Global Device Search** feature allows you to search through your network at the Global level, and locate devices using powerful filtering capabilities . You can search for Device Class and Network, narrowing your search to produce faster search results.

A new API "executeGlobalDeviceSearch" is introduced which allows you to search a specified IP address in all networks including all device classes. It provides two instances of the "ResourceIdentityInfo" object. One provides the device information and the other provides the network information where the device belongs. You can access this API either through a web service call or through J2EE.

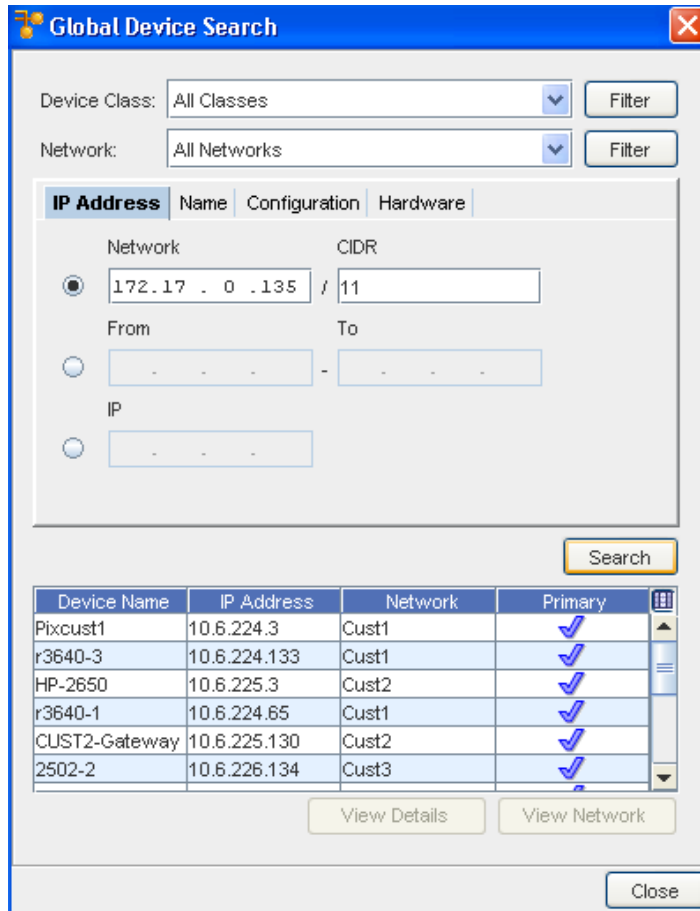
- 1 To begin your search, access the Global **Device Search** window by clicking **Tools** on the menu bar, then selecting **Global Device Search** .



- 2 With the Global Device Search window displayed, continue with your search by selecting and entering Search criteria.



- 3 Click **Search** when you have completed the search criteria. The Search Results display in the bottom of the Global Device Search window.



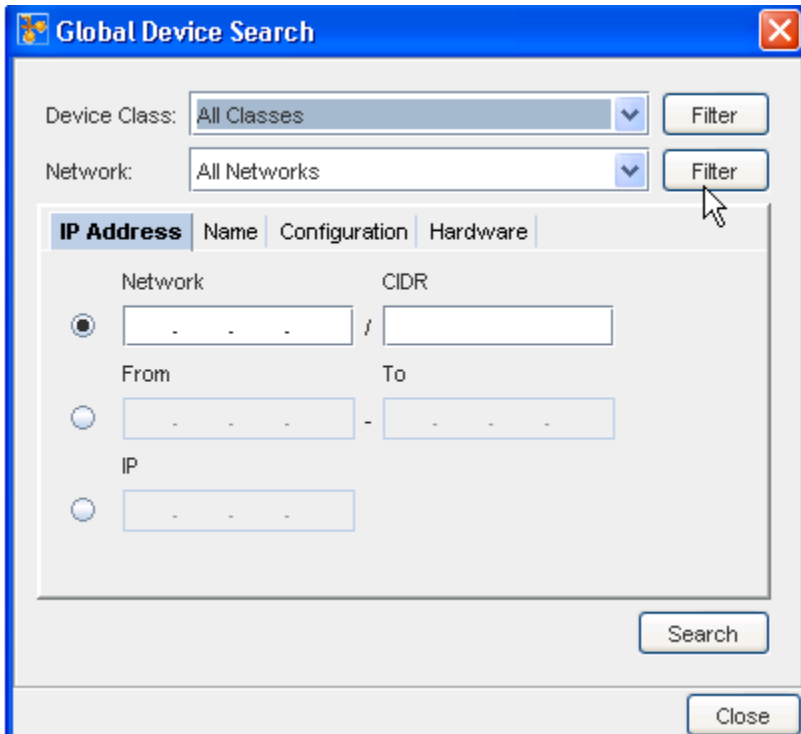
## Using the IP Address Tab (within Global Device Search)

The **Global Device Search** feature allows you to search through your network at the Global level. You can search for Device Class and Network, narrowing your search to produce faster search results.

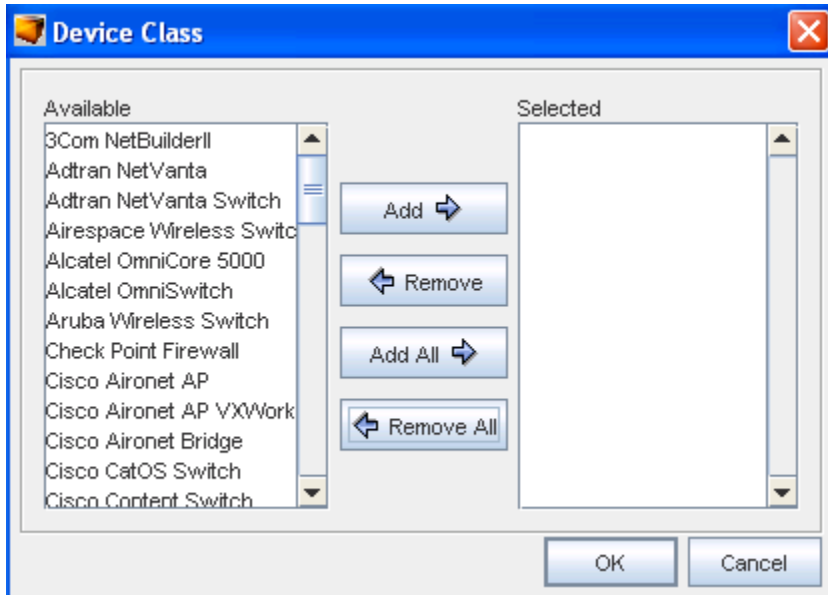
- 1 From the Network Configuration Manager launch page, access the **Global Device Search** option from the **Tools** menu bar.

Tools Window Help	
Networks Navigation	F6
<b>Dashboard</b>	<b>F8</b>
Automation Library	F3
Schedule Manager	F7
QS Inventory	F9
Event Manager	F11
Data Field Manager	
Metadata	F12
System Administration	F4
EMC M&R	
Change Audit	Ctrl-U
Global Device Search	Ctrl-S
Single Device Auto Discovery	
Template Merge	
Change Password	
Change RSA Tokens PIN	

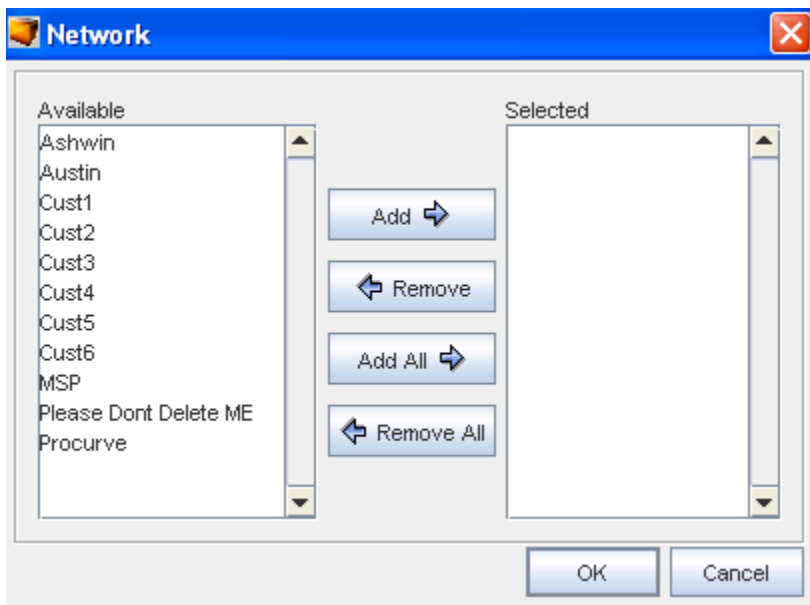
The Search window is now open. Note that the **IP Address** tab is active.



- 2 To search for **All Device Classes** and All Networks , keep these defaults, then click the **Search** Button.
- 3 To narrow your search to only one Device Class or one Network, click the drop-down arrow, and select from the list of Device Classes (or Networks) displayed.
- 4 To select to search for more than one Device Class ( **but not all**), click the corresponding **Filter** button to see the list of Available Device Classes.



- 5 Make your selections by highlighting the appropriate devices in the **Available** pane.
- 6 After making your selections from the Available pane, use **Add** (or Add All) to move your selections into the **Selected** pane.
- 7 Once your selections are moved into the Selected pane, click **OK**.
- 8 The Search window now shows Multiple Classes...in the Device Class search field. This indicates that you have selected more than one, but not All of the available device classes for your search.
- 9 Repeat the selection process with the **Network** search field to narrow your Network search criteria. To select to search for more than one Network ( **but not all**), click the corresponding **Filter** button to see the list of Available Device Classes (or Available Networks).



- 10 Make your selections by highlighting the appropriate Networks in the **Available** pane.
- 11 After making your selections from the Available pane, use **Add** (or Add All) to move your selections into the **Selected** pane.
- 12 Once your selections are moved into the Selected pane, click **OK**.
- 13 To continue defining your search criteria, and to narrow your search, you must select one of

The screenshot shows a dialog box with four tabs: **IP Address**, **Name**, **Configuration**, and **Hardware**. The **IP Address** tab is active. It contains three radio buttons and their corresponding input fields:

- Network:** A radio button (selected) next to a field containing "172.17.0.2" and a "CIDR" field containing "12".
- From/To:** A radio button next to two fields labeled "From" and "To", each containing a dash "-".
- IP:** A radio button next to a field containing a dash "-".

the following:

- Click the radio button in the **Network** field, and enter the Network location and the **CIDR** number.
- Click the radio button, then enter the **From** and **To** Network fields you want to search in.
- Click the IP radio button, and enter the **IP address** for your search.

- 14 Now, click **Search**. Search Results are shown in the bottom of the Search window.

### Available Device Classes

### Available Networks

The screenshot shows the **Global Device Search** window. At the top, there are two dropdown menus: "Device Class" (set to "Multiple Classes...") and "Network" (set to "All Networks"). Each dropdown has a "Filter" button to its right. Below these are the same search criteria tabs as in the previous screenshot, with the **IP Address** tab selected. The "Network" radio button is selected, and the "From" and "To" radio buttons are unselected.

You can view if the device is associated with a Primary Network from this window.

You can click **View Network** or **View Details** for more information on the Search results.

## Global Search from the Name Tab

- 1 To search for **All Device Classes** and All Networks , keep these defaults, then click the **Search** Button.
- 2 To narrow your search to only one Device Class or one Network, click the drop-down arrow, and select from the list of Device Classes (or Networks) displayed.
- 3 To select to search for more than one Device Class ( **but not all**), click the corresponding **Filter** button to see the list of Available Device Classes.
- 4 Select the name type you are using; Device Name, Hostname, Fully Qualified Device Name (FQDN), or Alias.
- 5 Enter the **string** into the Search String field to narrow your search, then click **Search**.

---

**Note** You can use the following wild cards when entering search strings.

---

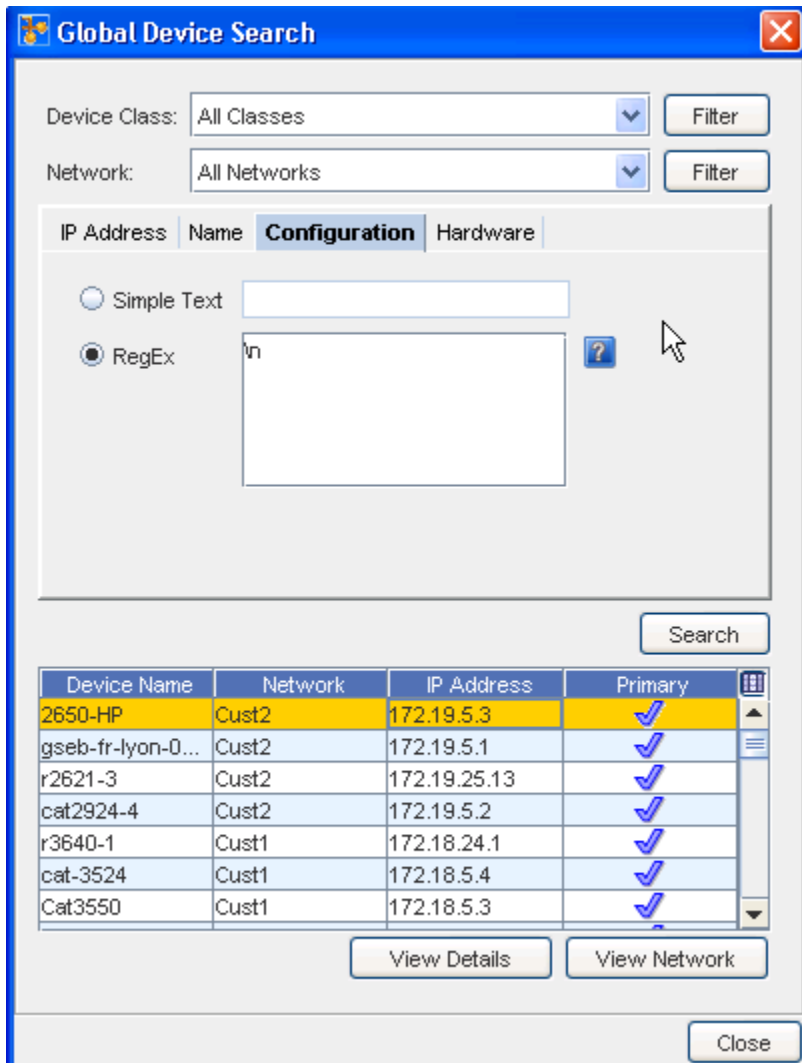
- An asterisk (\*) for sequences of characters
  - A question mark (?) for a single character
- 6 View your search results at the bottom of the screen.

You can also view the **Details** and the **Network** from this window.


[Global Device Search Overview](#)

## Global Search from the Configuration Tab

- 1 With the Configuration tab displayed, you can select the **Device Classes** drop-down arrow and make selections, or use the **Filter** button and make the Device Class selections.
- 2 You can also make selections for the **Network** in your device search by clicking the drop-down arrow and selecting from the list, or use the **Filter** button and move the Networks into the appropriate pane.



### 3 Select between **Simple Text** and **RegEx**.

- If using **Simple Text**, click within the radio button, then enter the text you want to use for a search criteria.
- Click within the **RegEx** radio button to view RegEx.
- Click the icon  to get more information on using RegEx, and enter the appropriate expression.

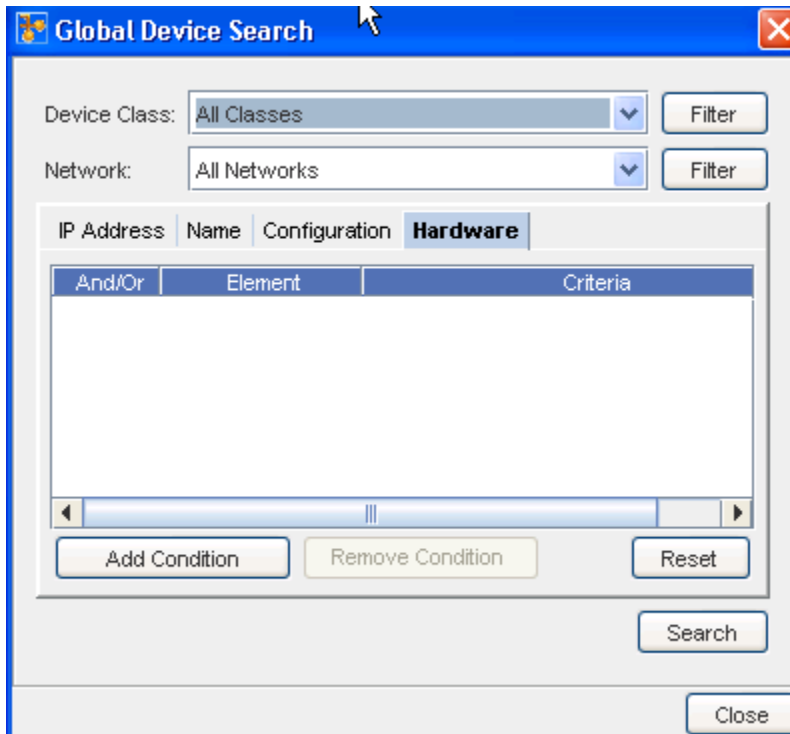
### 4 After entering your search criteria, click **Search**.

### 5 View your search results at the bottom of the screen.

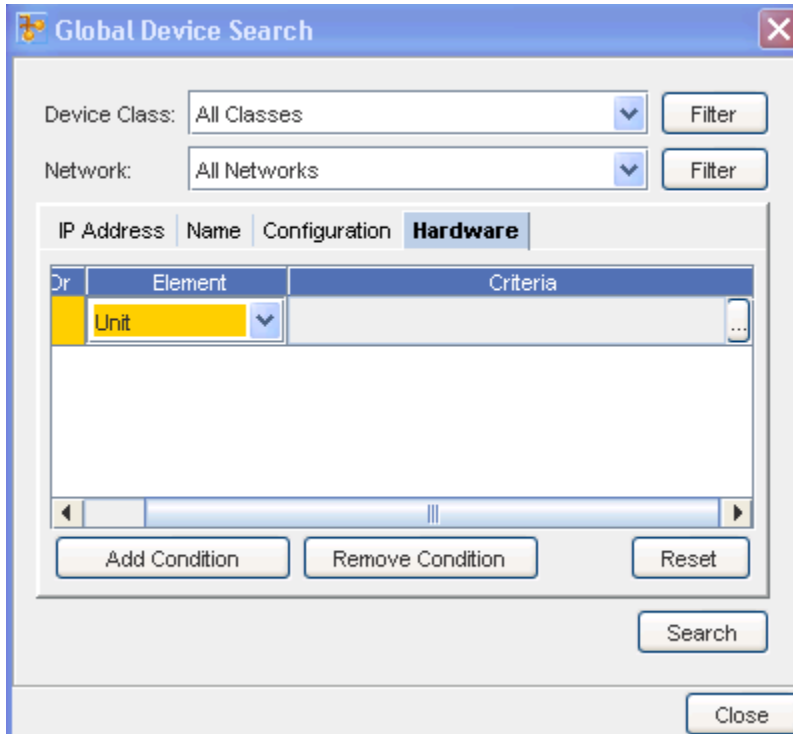
### 6 You can select a result, then click either **View Details** or **View Network** to get additional details.


## Global Search from the Hardware Tab

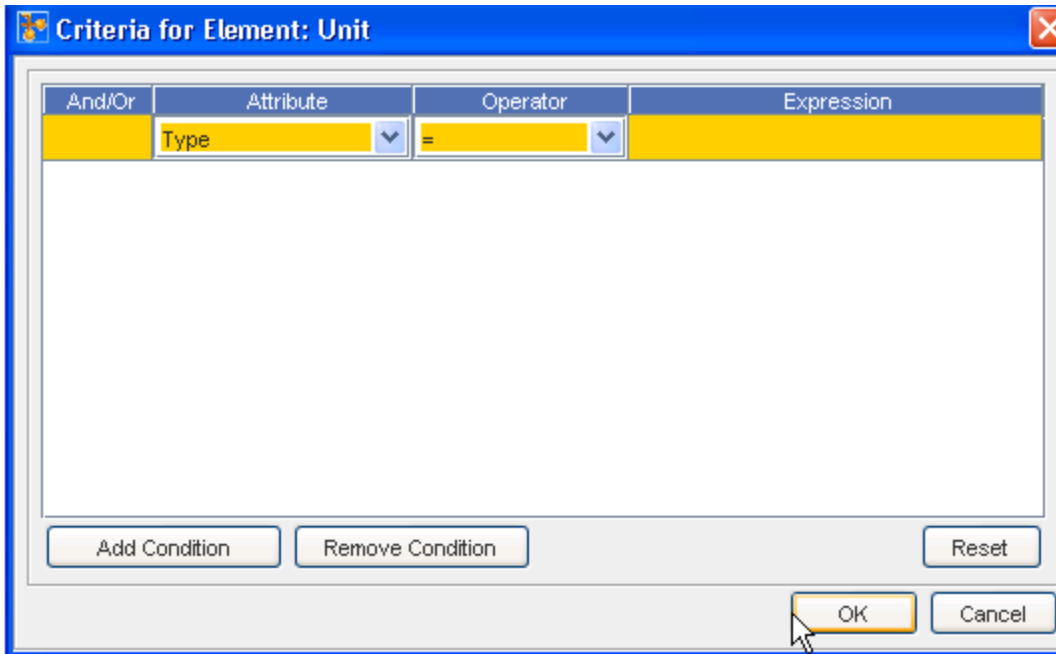
- 1 Click the drop-down arrow in **Device Class** to select a class from the listing, or click **Filter** to filter the listing of classes.
- 2 Click the **Network** drop-down arrow to see a listing of the networks to select from, or click **Filter** to further filter the listing of networks.



- 3 You can define your search criteria by adding conditions (or removing existing conditions). Click **Add Condition**, and select from the **Element** drop-down options.



- 4 Next, select the drop-down in the **Criteria** column  to go to the **Criteria for the Element** window you just selected.
- 5 Click the **Add Condition** button to activate the Criteria for Element window.





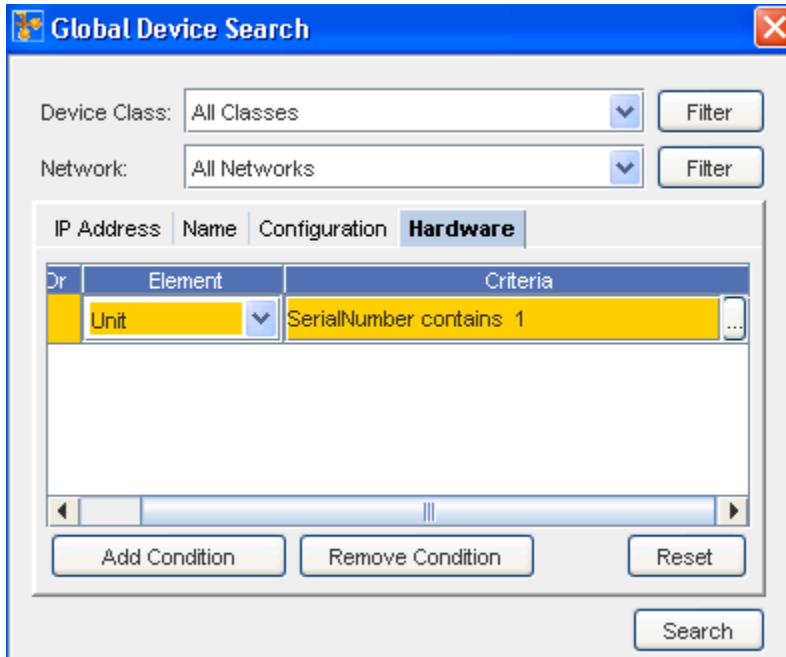
- 6 Make And/Or, Attribute, Operator, and Expression selections for your search. Note that you can also Remove any existing Conditions, if necessary.

---

**Note** To make changes to the criteria you have selected, click the **Reset** button to clear the fields, and begin again.

---

- 7 After making your selection on this window, click **OK**.
- 8 At the Hardware Tab window, click **Search**.



- 9 You can now view your search results at the bottom of the window. **View Details** and **View Network** information is also available from the tabs at the bottom of the window for any device listed in the Search results.

## Working with Sites

## Sites Overview

- Each network in Network Configuration Manager contains a single-site hierarchy construction, which is created at the same time as the network. However, there is no requirement to create and manage sites within each network. For example, there may be times that the construct of a geographical relationship for network devices is not beneficial to the management of the network.
- By default, devices are not assigned to a site, but they do display at the top of the site hierarchy, ready to be managed into a site structure (if needed).
- A Site is a physical view of network devices that can be segmented into a hierarchical structure representing the location of a device. There exists an explicit order to site relationships, determined by the site type. All networks contain the ability to create a site hierarchy for network devices. By default, all devices are available in the Devices tree branch.
- Site types allow you to segment devices based on geography, building, floor, room, and rack. Each site type can contain its own site. For example, a geography can contain a geography, and a room can contain a room.
- A site hierarchy contains the following site types. The site types are listed in the order of how they must be configured when creating a site hierarchy. It is not required to have each site type, but you must construct the site types accordingly.
- Navigating down a network site hierarchy is accomplished by selecting a site and opening it, and then repeating the process to open any other sites further down the hierarchy. Navigating up a site hierarchy is possible by selecting an Up Site icon on any site diagram that has a parent site.



**Geography** - for example, Country, State, City, Province. A geography can contain another geography, building, floor, room and/or rack



**Building** - for example, Headquarters, Street Location, or Complex Number. A building can contain a floor, room and/or rack



**Floor** - within the building, the floor on which devices reside. A floor can contain a room and/or rack



**Room** - on the floor, the exact room where the devices reside. A room can contain another room and/or rack

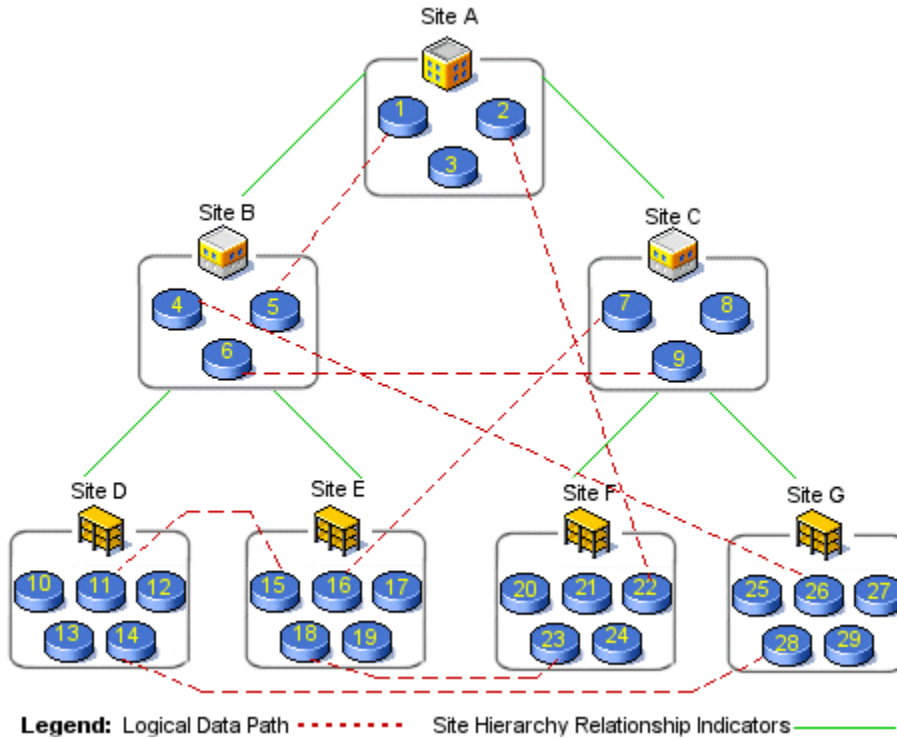


**Rack** - in the room, the rack on which the servers are located. A rack can contain another rack

A site hierarchy has no depth limitations or restrictions. For example, your corporate office may need to consist of a large network site hierarchy, including a geography containing multiple buildings, each containing multiple floors, each containing multiple rooms, and each in turn, containing multiple racks.

In this scenario you might locate all your devices at corporate within the rack site containers. However, within the same network it would be acceptable to have a single building container holding a few devices located at each small regional sales office.

Sites have parent/child hierarchy relationships. A physical representation of a site shows the relationships within the site hierarchy. A logical connection indicates the connection between devices and sites, regardless of the hierarchical layout.



The previous diagram shows a sample visualization for a possible network site hierarchy. In this hierarchy, there exists a root building site **A**.

- Site A contains two lower-order floor sites, **B** and **C**, and three devices.
- Site B also contains two sites, in this case, rack sites **D** and **E**, and three devices.
- Each rack site contains five devices.
- Assuming that all attribute information for each site is the same, and is not overridden at any site, attributes can be entered at site **A**, and then inherited at all other sites.

All site hierarchy is user-defined, and managed. It can not be shared between networks. Permissions to modify a site depend on the membership filters. See [Permissions and Site Security](#) for more information. Sites can not be seen in other views, as each view is unique. Sites can be viewed by other users who have access to the networks.

As each site hierarchy is created for each network, devices are added to sub-sites. All devices associated with the network resides within a site. **A device can reside in one site only.**

When devices are used that actually reside in another network, these devices have an "off-site" connector symbol to the outside network. This connection uses the off-site connector to indicate that the devices are not managed by the open network. You are not allowed to move a device that is not managed by the primary network, because the device can only be placed into the site hierarchy of its primary network.

The following are characteristics of sites:

- Each network has a single-site hierarchy.
- A site contains both sub-sites and devices.
- Sites can not be shared with other networks.
- Sites are recursive, and have no depth limit.
- Sites are user-managed, and are a physical representation of a network.
- Only users with adequate permissions can create and name sites.
- All information entered into a higher level site is propagated to the lower tier sites, such as, contact and address information. When inherited by sub-sites, this information can be overwritten.

Once you have created a site hierarchy for your network, you can define the layout when viewing the layout:

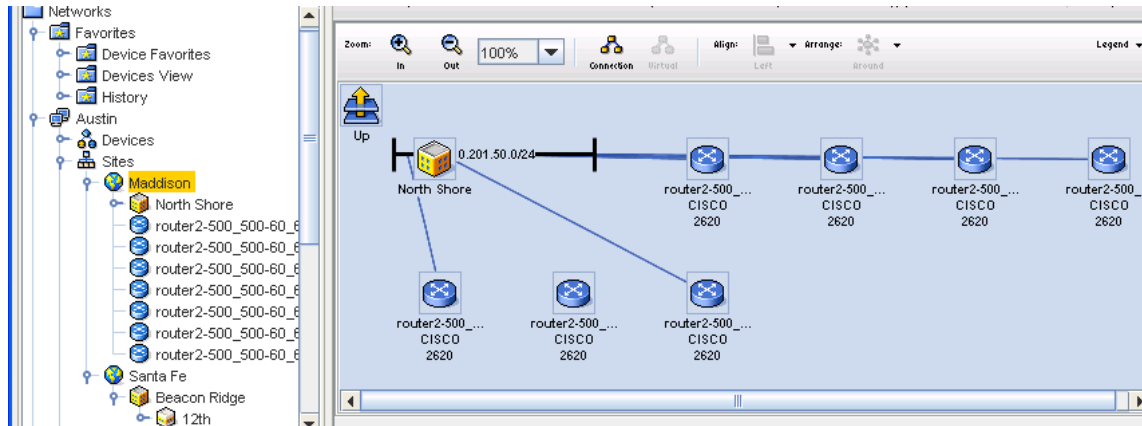
**Table** Shows the devices in a sorted table layout

**Diagram** This is the default view, and shows the devices using icon representation.

This is an example of the **Table** view.

Device Name	IP	Devic...	Model	OS Versi...	Devi...
<b>North Shore</b>					
router2-500_500-60_60-...	10.2...	Cisco ...	2620	12.1(8) E...	
router2-500_500-60_60-...	10.2...	Cisco ...	2620	12.1(8) E...	
router2-500_500-60_60-...	10.2...	Cisco ...	2620	12.1(8) E...	
router2-500_500-60_60-...	10.2...	Cisco ...	2620	12.1(8) E...	
router2-500_500-60_60-4	10.2...	Cisco ...	2620	12.1(8) E...	
router2-500_500-60_60-...	10.2...	Cisco ...	2620	12.1(8) E...	
router2-500_500-60_60-...	10.2...	Cisco ...	2620	12.1(8) E...	
Up...					

This is an example of the **Diagram** view.



- Sites Hierarchy and Logical Connections
- Sites Best Practices
- Permissions and Site Security
- Sites Filters
- Creating the Site Hierarchy
- Attributes
- Editing the Site Hierarchy
- Removing a Site Hierarchy level
- Right-click Features
- Right-click Features - Diagram View
- Assigning Devices to Sites
- Editing Device Associations to Sites
- The General Tab - Editing Site Properties
- The Sites Comments Tab
- The Attachments Tab
- Using Quick Commands
- Sites - Legends

## How Sites and Views Work

Network Configuration Manager offers a flexible and dynamic way to efficiently segment the management of devices in your network, through the use of Sites and Views. Sites and Views allows you to implement and manage device containers within your network that best reflects your management needs.

Sites	Allows you to segment device management physically, by a geographical location
Views	Allows you to segment your devices by technology type, vendor, departmental responsibility, or any other preferred logical segmentation

In this way, each user with the proper Network Configuration Manager network credentials can customize the way they organize and access devices in the network.

## Sites

Regardless of the number of networks you construct in your Network Configuration Manager environment, Sites and Views provide you with the ability to physically or logically segment the devices contained within each network. Sites, as the name indicates, reflects a physical, geographic segmentation of devices.

To track the physical location of managed devices for asset tracking, maintenance or repair purposes, or just work better with devices organized in a physical relationship, implement Sites within Network Configuration Manager.

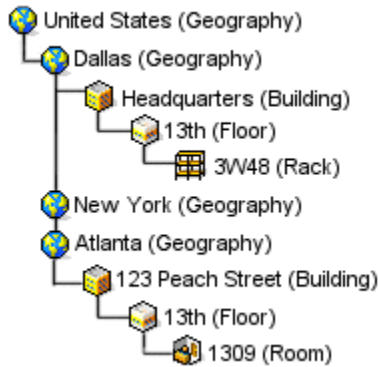
## Views

Views provide a logical segmentation of devices, meaning there is no need for a physical relationship to exist between devices within a View.

If you operate across geographical boundaries, and segment network management responsibilities by technology or vendor, you will find that Views will address the need for device organization. However, it's likely that a combination of both Sites and Views will be the **most effective** method for providing the flexibility to manage network environments.

### How Sites and View Work

- Sites are constructed in a hierarchy. As such, sites can contain other sites, as well as devices. There exists an explicit order to site relationships determined by the site type.
- By using the site Hierarchy, you can diagram the physical relationships devices have with one another. Sites provides a "snapshot" allowing you to focus on any part in the network. You can then segment the site to allocate devices into sub-sites. For example, the following is a site hierarchy, and the possible site type relationships.



- This example indicates that your devices are divided into four possible geographical locations: United States (Primary Site), Dallas (sub-site1), New York (sub-site2), and Atlanta (sub-site3).
- Within Dallas, the devices have been further segmented to the exact **rack location**, and in Atlanta, the devices have been segmented to the **room** where the devices are located. In this hierarchy, New York's relationships remain hidden.
- In the example, notice the duplication of the 13th floor being used. When naming sites, you cannot use duplicate names when the types are on the same level in the hierarchy. However, it is permissible to duplicate a name, when in separate site levels .
- Also, note that all site types were not used in either Dallas or Atlanta. In the Dallas site, a room has not been indicated. In Atlanta, a rack is not indicated. This is to emphasize the ability to create the site types that best reflect your locations.
- As each site is diagrammed, note that the physical layout of a site does affect the logical connections of devices.
- Views have no relationship to one another as they contain flat, and sometimes unrelated groupings of devices. As such, views have no relational hierarchy in a network. However, for organizational purposes, views are maintained in a folder structure within a network. In this way, for example, you could create a vendor folder named Cisco™, containing sub-folders for routers models, each of which would contain views holding routers sorted by connection type. For example, Frame, ATM, or Point-to-Point.
- Sites and Views are designed as public, or shared containers under each network. As such, any Network Configuration Manager user with **view access** to a network can access and see the sites and views created in that network. There is one default view created for all networks called the **All Devices** view. It is a view created to provide a single reference to all devices in a network.

---

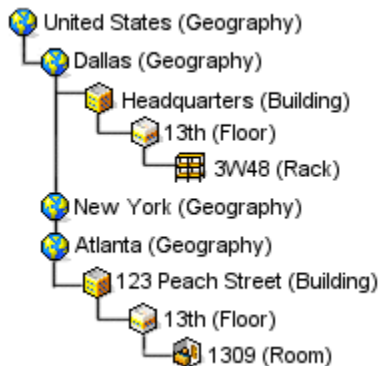
**Important** It is not recommended that you use the All Devices view for device management, especially for large networks, as system performance is proportional to the number of devices in a view. Opening up and operating in the All Devices view could cause slowed performance, and use considerable resources.

---

## Sites Best Practices

Best Practices are recommend methods of completing tasks or tips that should be used, based on a typical scenario.

- The Site hierarchy was constructed to provide your organization with an effective way to track the physical location of devices in your network. While it is acceptable to use the Site hierarchy for day-to-day network management, it is recommended that Views be used for managing devices, especially when a deep site structure is created. This will greatly speed the navigation to the devices you frequently manage.
- When creating networks and adding sites and views, construct the site hierarchy from the bottom up. Start with the **rack location**, and work backward. By creating the site in this manner you only have to move the devices that belong in each site type to their location, rather than moving all of them from the upper-most location downward.
- Hierarchical rules apply to the site hierarchy. For example, site names are unique at each level of the hierarchy. In the hierarchy graphic (shown below) when naming site types, there cannot be two New York locations under United States. There can, however, be duplicate floor names (such as 13th), as they reside under two different sub-site locations.



- When making changes to a site type, all set attribute values are lost and must be reset.

## Sites Hierarchy and Logical Connections

Sites and Views provide the ability to display connections between devices. Connection types are identified by different line styles in your View or Site. Connections can be displayed in two formats:

Physically This displays clouds for certain WAN technologies, giving a layer-2 visualization of your network.

Logically This provides layer-3 visualization.

Because of the hierarchy of sites and the association rules of devices in views, this is where the similarity of connections ends between the two.



## Views

Views are flat in nature, having no relation to other views. Connections in Views are visible only between devices within that view.

Since a required relationship between any device in a view is not needed, you could create a view in which there are no connection associations between any of the devices.

A good example of this would be a view containing all firewall devices in an enterprise. Each firewall could be providing outbound access from the enterprise, and have no actual direct connectivity to each other. In this view, the diagram would display an icon for each device, but there would be no connections.

## Sites

Sites, because of their hierarchical relationship and physical nature, have a complex connection construct. This is due to the three-dimensional effect created by the site hierarchy when in a site diagram.

Before explaining the concept of connections in sites, it is important to remember that ALL connections in Network Configuration Manager are ultimately device-to-device. Also, connector lines in a diagram can represent a single connection, or at times, a group of connections conveniently associated by a connection type.

Imagine a site diagram containing three devices and two other sites. The two sites would be considered children, or sub-sites, of the current site, as they are 'down' the hierarchy chain. In this imagined diagram, it is possible that two of the visible devices could have connections (for example, Ethernet, or Frame Relay) between them, which would create a device-to-device connector.

One of the devices could have a connection to a device contained in one of the sub-sites, which would require a device-to-site connector. It is also possible that a device contained in the first sub-site could be directly connected to a device in the second sub-site.

In the current view, the diagram would construct a site-to-site connector. Consider also that the devices in the sub-sites may not live at the top of that site level, but be nested in other sub-sites down the hierarchy. Regardless, the same connector would be constructed.

Finally, a device in the current diagram or contained in one of the sub-sites, could be directly connected to a device in a site, in a completely different branch of the site hierarchy, or 'up' the hierarchy. In both of these cases, the terminating device or site would not be visible in the current diagram. In this case, a device-to-off-site, or site-to-off-site connector would be constructed.

Within a site diagram, there are five connector relationships:

### Device-to-Site

Are connections between devices contained in the hierarchy.



### Device-to-Device

Shows connections from one device to another device.



**Device-to-Off-site**

Are connections to devices outside of the site hierarchy. These connections are identified by an off-site icon.

**Site-to-Site**

Shows connections from one site to another site.

**Site-to-Off-site**

Are connections to site levels within the site hierarchy. These connections are identified by an Off-site icon.



**Note** It will take implementing a network site hierarchy to see how the connectors are generated and to understand how the diagramming of connections works within sites. Also note, that the calculation of all the permutations of possible connectors is a tedious process.

Since it is assumed that once a site hierarchy is constructed, there will be few physical changes. The recalculation of connections in a site hierarchy is completed as a nightly batch process, at approximately 4:00 A.M.

This schedule can be changed, depending on the requirements of your network. As changes are made to networks during regular use, a flag is used to indicate that site diagrams are due for an update. When a site diagram is refreshed, it is transparent to the user. Depending on the number of devices, the refresh may be time consuming.

## Editing the Site Hierarchy

Once created, the site hierarchy can be edited as follows:

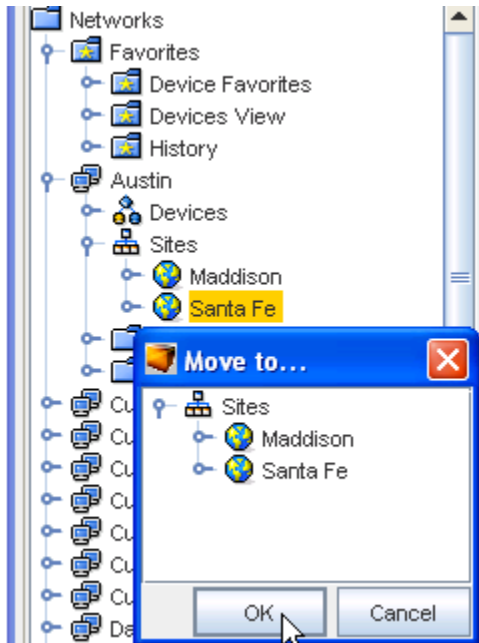
- [Removing a Site Hierarchy level](#)
- Devices can be moved to other site types
- [Sites Hierarchy and Logical Connections](#)
- Site Type properties can be edited

Once a site type has been removed from the site hierarchy, it cannot be retrieved. You must re-enter any information that has been deleted in error.

### Edit Site Hierarchy

To move the site hierarchy,

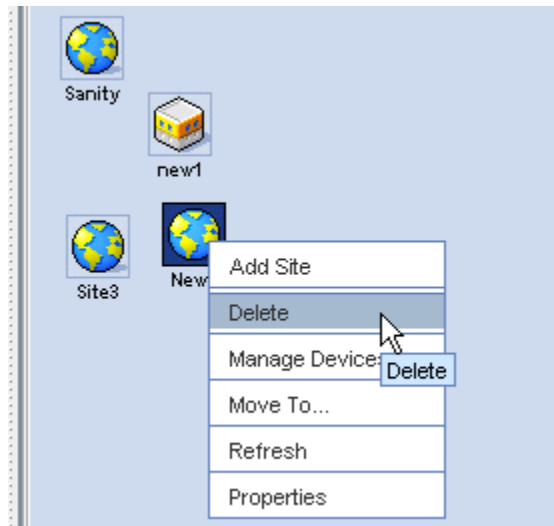
- 1 In the tree menu, expand the **Sites** branch.
- 2 Expand the tree menu, then right-click the appropriate **Site type**.



- 3 From the right-click options, select **Move To....**  
The Move To... window opens.
- 4 Navigate to the site location where the site is being moved.
- 5 Click **OK**. The Move To.... window closes.
- 6 If the window does not automatically refresh, right-click on **Sites**, then select **Refresh**.

## Removing a Site Hierarchy level

- 1 In the tree menu, expand the **Sites** branch.
- 2 Expand the tree menu, then right-click the appropriate **Site type**.
- 3 From the right-click options, select **Delete**.
- 4 The Confirm dialog window asks, "Are you sure?" To delete this single site, click **Yes**. If there are site levels within the site you are deleting, the following Confirm window opens.
- 5 To delete the site levels with the site you are deleting, click **Yes**.
- 6 If the window does not automatically refresh, right-click on **Sites**, then select **Refresh**.



## Permissions and Site Security

Authorizations for the protected device resources in a Site or View are taken from the authorizations granted at the **Network** or **Individual Device** level.

If you have been provided the access or permission (either at the network, or specifically on the device) to update that device and schedule changes for the device to the scheduler, you can complete this task from any Site or View that contains a representation of that device in the network.

To create a Site or View, or to modify its contents, you must be able to [Managing Network Access Permissions](#).

## Sites Filters

To further enhance the information presented within Sites and Views, display filters provide a mechanism for tailoring your display of the network. You can customize the display filters to limit the device types visible in a **Site** or **View** window. In the same way, connection technologies can be filtered between visible devices.

For example, you may have a Site that contains all the devices (72) in the 3rd floor communications closet at the Corporate location. Opening this Site visually displays all 72 routers and switches in that closet. However, at this time, you are only concerned with identifying the Frame Relay routers in the closet. A filter could be quickly constructed within the Site window to only display routers and frame relay connections, greatly speeding the identification of the devices you need.

In addition to displaying filters, Views provide the ability to create dynamic membership filters. Filters are identical to display filter types, but provide a way to automatically assign devices to a View, based on their type or technology.

Each time the view is opened the device membership list is updated with all eligible devices. For example, creating a View with a membership filter is an ideal way to always have a view of every firewall device in your network, which is updated anytime a new firewall is discovered in the network.

For details regarding the Sites window, see [Sites Overview](#) .

## Attributes

Each site type has its own attributes, but as an option, you are able to propagate information to sub-sites that can be inherited or overridden from parent sites. These attributes are used to identify the location of a site, and the devices or other sites contained within it.

In this way, devices and sites placed in a building site construct will inherit the physical address of that site. When changes are made to a higher level site, the overwritten details remains intact.

### Site Attributes include:

- Name
- Type
- Description
- Override (where you can override the initial contact names or description)
- Contact Name
- Contact Phone
- Contact Email
- Address 1
- Address 2
- City
- State/Province
- Zip/Postal Code
- Country

Dynamic inheritance in sites allows lower-order sites to have their site attributes updated when the same information is updated in the parent site. This dynamic inheritance can be overridden at any site.

When the override flag is set for a site, local attributes can be customized, and will not receive dynamic updates from the parent attributes. Un-setting the override flag for a site restores the attribute inheritance from the parent site.

## Creating the Site Hierarchy

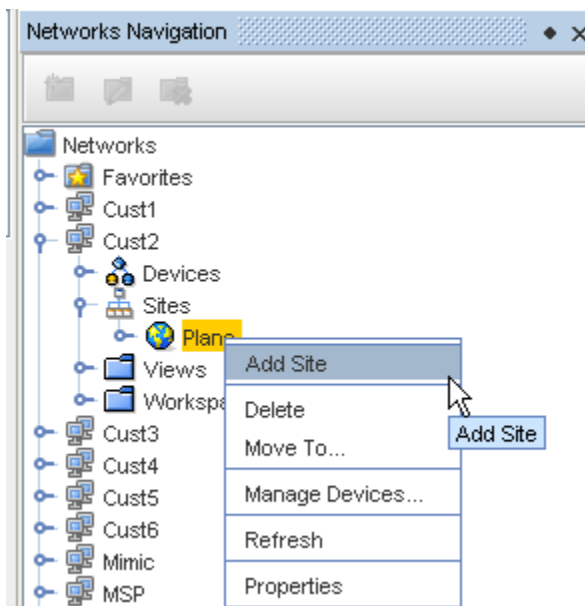
Contact information can be provided per Site, or inherited from a parent Site. Once the Site has been created, devices can be associated with the site. Devices associated with the network are listed under the **Devices** branch of the menu tree. The Sites branch remains empty until a site hierarchy is created.

**Important** When creating Sites, you must follow the nesting hierarchy in [Sites Best Practices For more information](#), see [How Sites and Views Work](#).

As you are creating the Site hierarchy, devices can be assigned as you go, or the Site hierarchy can be created, and then assigned to the devices within the hierarchy.

To add Site information,

- 1 Select **Site**, then right-click to select **Add Site** from the Navigation pane.




- 2 At the New Site window, enter the information needed.

**Note** You can select to Override existing Geography information with this new information if Building, Floor, Room or Rack is selected from the Type drop-down, and Override is checked.

**New Site**

\*Name:

\*Type: Geography 

Description:

Override

Contact Name:

Contact Phone:

Contact Email:

Address 1:

Address 2:

City:

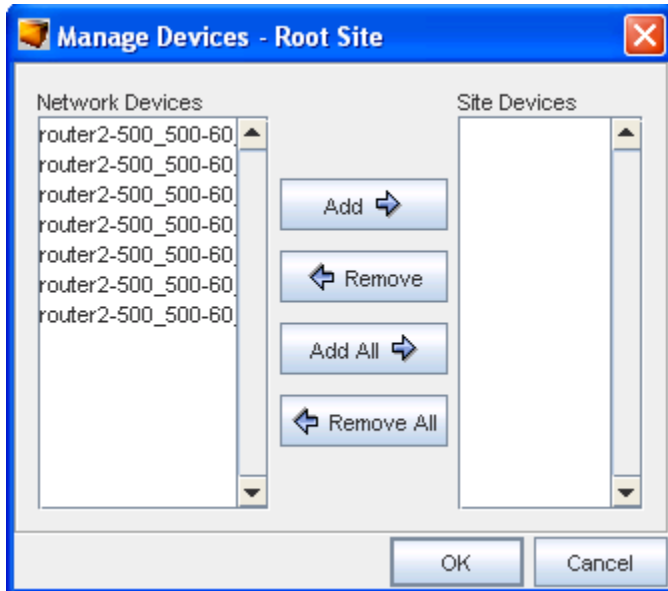
State/Province:

Zip/Postal Code:

Country:

OK Cancel

- 3 Click **Ok** when you have entered all the information you want visible in the **Site** tab (of the Devices Properties).
- 4 Now, from the Navigation pane, select the site you just created, then right-click to select **Manage Devices** from the Root Site.
- 5 From the Manage Devices - Root Site window, select the devices you want to add to the Site. Use the **Add** or **Add All** arrows.



6 Click **Ok** when you have completed moving devices into the **Site Devices** pane.

When Site types are added to the hierarchy, you need to categorize the networks devices. Once finished, [Assigning Devices to Sites](#) .

## The General Tab - Editing Site Properties

Site properties contain contact and location information for the Site. By default, Sites inherit the properties of the parent Site, unless the Override check box is selected. Devices in Sites inherit Site properties which are displayed in the Site tab of the Device Properties.

Comments and Attachments can be associated with a Site. Site objects also support Data Fields.

The (General) properties of a site are the details entered when the site hierarchy was created. Added to this information are two additional tabs:

- [The Comments Tab](#)
- [Attachments](#)

---

**Important** You must follow the nesting hierarchy [Sites Best Practices](#). For more information, see [How Sites and Views Work](#).

---

A site type can be edited in two ways:

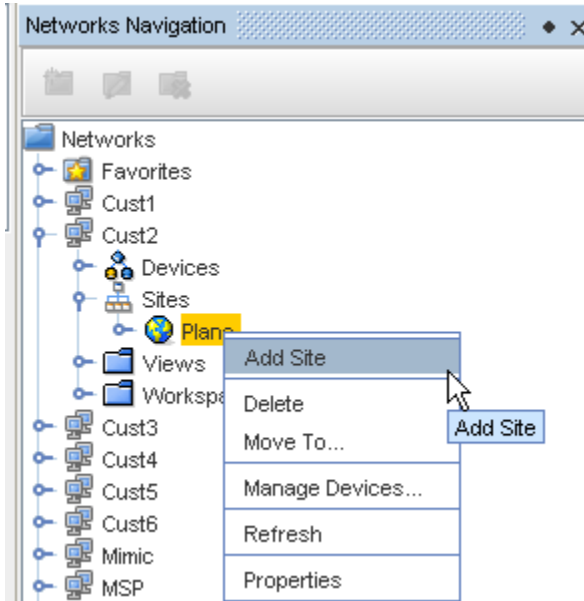
- [Editing the site type properties](#)
- [Editing Device Associations to Sites](#)

The ability to edit the site type properties allows you to modify the Name, Site Type, Description, and Override information, if needed. This information works hand-in-hand with the ability to edit the devices associated with the site type. Anytime that you edit the site type, you should review the devices associated to the modified site type.

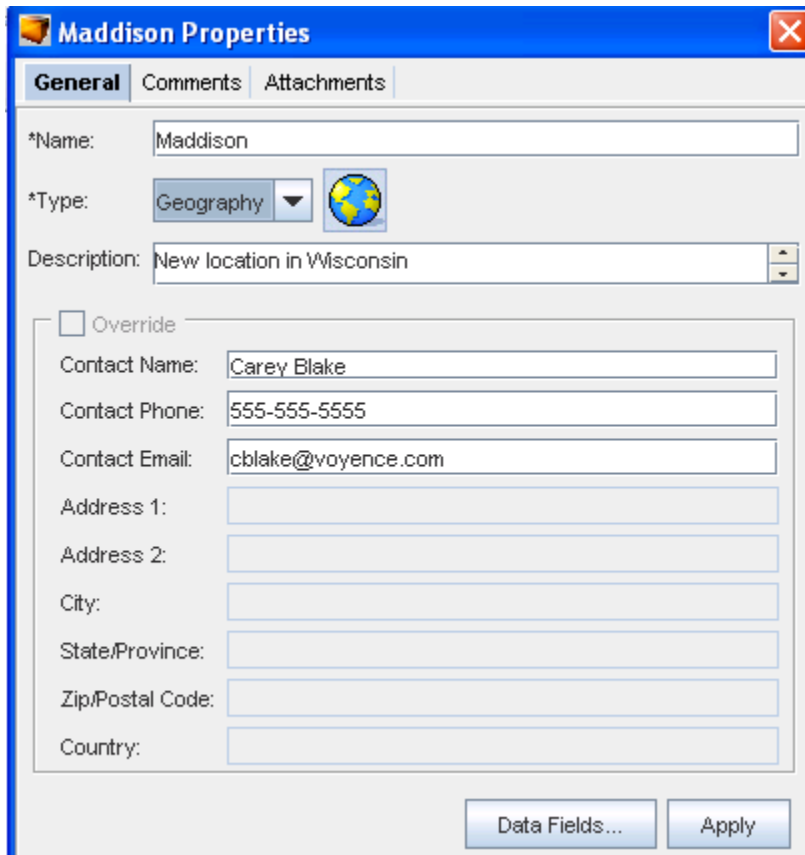


To edit a site types properties,

- 1 In the tree menu, open the **Sites** branch.
- 2 Expand the tree menu, then right-click the appropriate **Site**.



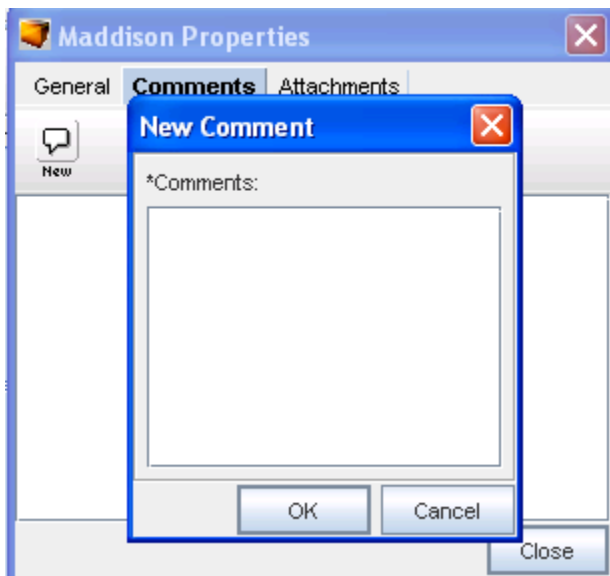
- 3 From the right-click options, select **Properties**. The [Site Name] Properties window opens.



- 4 All fields in the properties window can be edited. **Edit the information** as needed.
- 5 To enter contact information specific to this site (in the **Building, Floor, Room,** and **Rack** types - selected from the Type drop-down) check the **Override** box. The Contact field information window activates allowing you to add additional entries to the previously empty sections.
- 6 When finished, click **Apply**. The [Site Name] Properties window closes.

## The Sites Comments Tab

The **Comments** tab contains a running list of comments, related to the site.



The comments are logged as they are entered. Each comment identifies who created the comment, and when. A broken line indicates the end of each comment.

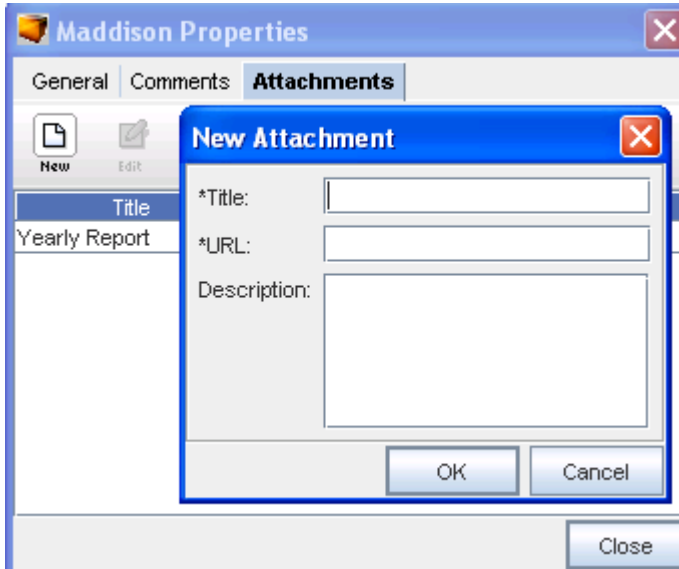
To create a new comment,

- 1 On the Comments tab, click the **New Comment icon**. The New Comments dialog window opens.
- 2 Enter your **comments**. The Enter key can be used to create paragraph breaks in the comments.
- 3 Click **OK**. The New Comments window closes. Each new comment is added to the top.
- 4 For each new comment, repeat **steps 1-3**.

## The Sites Attachments Tab

The **Attachments** tab allows you to associate an external file to the site. This can include worksheets, documents, or .html files. Any document that can be opened in a web browser can be mapped as an attachment.

Multiple attachments can be added to each site.

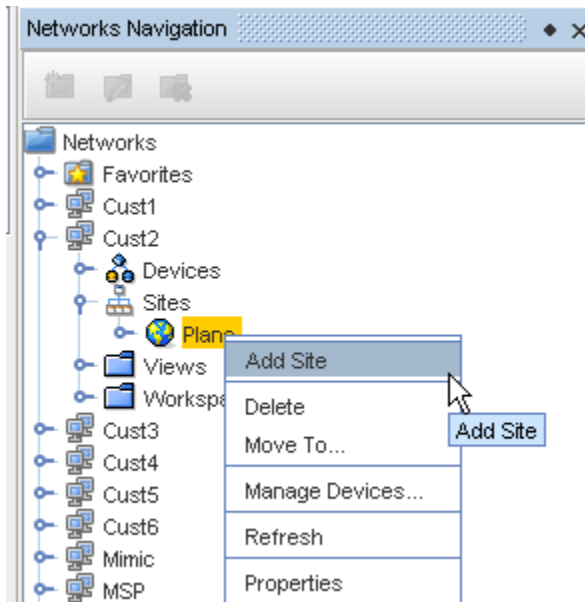


## Right-click Features

From the Navigation tree you can access other windows to work within sites, and you can complete tasks using the right-click feature.

To use the right-click features in Sites (in the Networks Navigation),

- 1 In the tree menu, right-click **Sites**.



- 2 You can complete the following using the right-click features:

- 3 **Add Site** - this opens the New Site window where you can designate a Site
- 4 **Delete** - this allows you to select a Site, then right-click and select Delete
- 5 **Move to** - this takes you to the Move To window where you can then move the Site within the Network
- 6 **Manage Devices** - this takes you to the Manage Devices window where you can add or remove devices
- 7 **Refresh** - this refreshes your Sites view
- 8 [The General Tab - Editing Site Properties](#) - this takes you to the Properties window where you can enter information pertaining to the Site

## Data Fields in Sites

You can select the appropriate Data Fields within Sites. Data Fields are used to create attributes, and to assign values to devices.

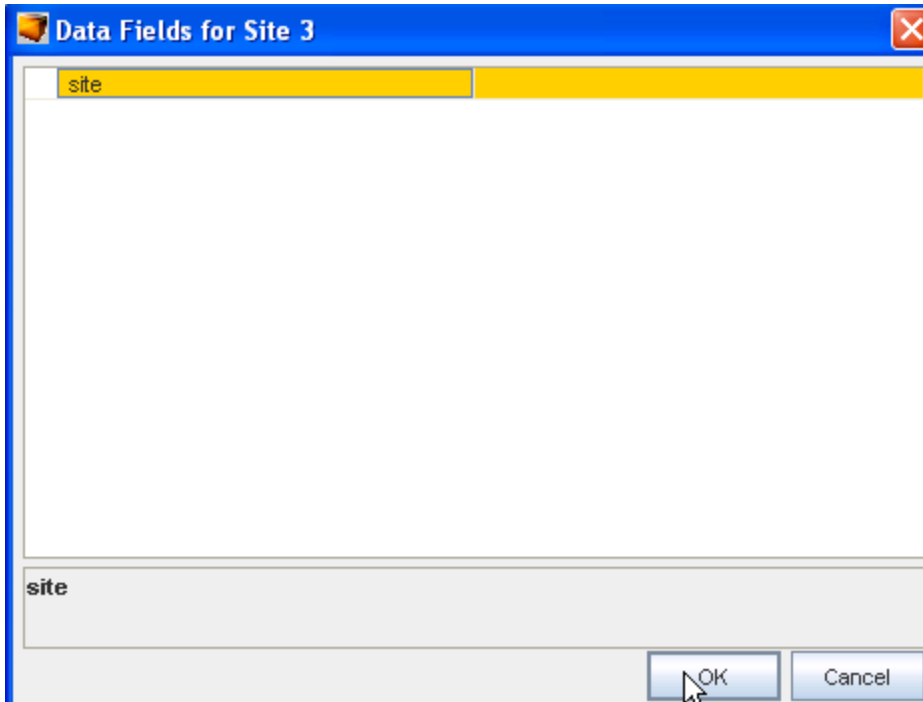
- 1 With the Site Properties window open, click the **Data Fields** selection.

The screenshot shows the 'Site 3 Properties' dialog box with the 'General' tab selected. The fields are as follows:

- \*Name:** Site 3
- \*Type:** Geography (with a globe icon)
- Description:** New site - associated to New Rack
- Override**
- Contact Name:** Jamie Dawson
- Contact Phone:** 555-555-5555
- Contact Email:** jamie@voynce.com
- Address 1:** (empty)
- Address 2:** (empty)
- City:** (empty)
- State/Province:** (empty)
- Zip/Postal Code:** (empty)
- Country:** (empty)

Buttons at the bottom: **Data Fields...**, **Apply**, and **Close**.

The available Data Fields will display in the Data Fields for [site name].

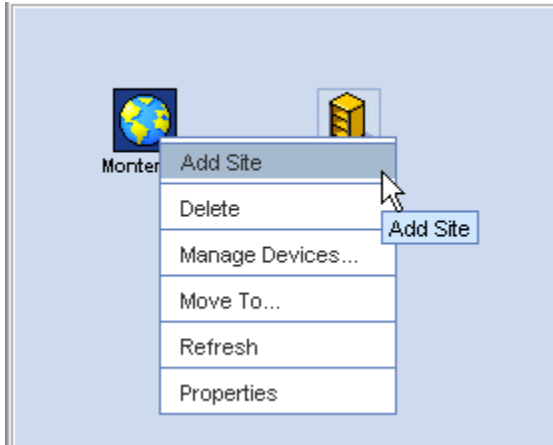


- 2 Select the data field, then click **OK**.

## Right-click Features - Diagram View

To use the right-click features in Sites (in the Sites table or Diagram View),

When you have Sites displayed in the diagram view, you can also use the right-click feature.

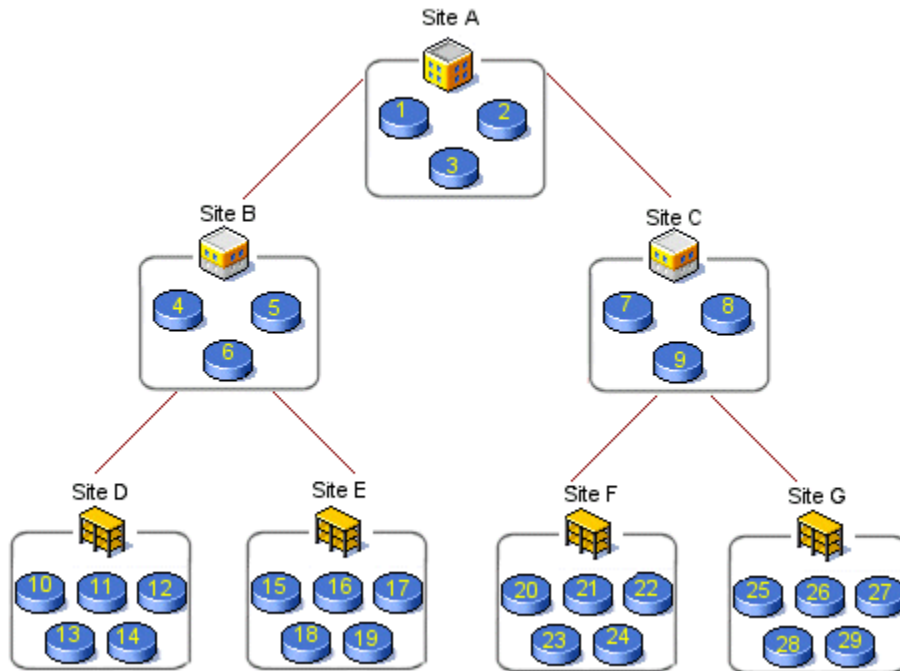


- 1 Right-click the **site** in the table or diagram format.
- 2 Select a **task** from the menu to work with.

## Assigning Devices to Sites

When creating a Site, you can develop a multi-tiered hierarchy that segments the network as deeply as needed. Each Site can contain not only devices, but also other sites .

In the following example, there are seven Sites. Each Site contains not only its own devices, but Sites **B** and **C** serve as both parent and child.



The above graphic indicates:

**Site A** - Site B and Site C and Devices 1,2,3

**Site B** - Site D and Site E and Devices 4,5,6

When creating a site hierarchy, you do not have to consider the devices associated within each Site. From a physical standpoint, Site A has a direct relationship to Site B.

The site hierarchy is a flexible structure. As you are creating the site hierarchy, devices can also be assigned, or the site hierarchy can be created, and then assigned the devices within the hierarchy.

**Note:** When creating a hierarchy for a large network, it is strongly recommended that you build the site hierarchy starting at the bottom-most tier.

To Manage Devices in Site Hierarchy,

- 1 Once the site Type is [Creating the Site Hierarchy](#), right-click on the **type name**.
- 2 In the right-click menu, select **Manage Devices**. The Manage Devices window opens. The list of network devices displays. Devices already associated with the site type are listed in the Site Devices column.
- 3 In the **Network Devices** column, select the devices that will be associated with the site type.

**Note:** A string of devices can be selected by holding down the Shift-key, while selecting the devices. Or, select multiple, non-sequential devices by holding the Ctrl key down, while selecting the devices.

- 4 Click **Add**. The selected devices move to the Site Devices column. Or, to move all devices to the **Site Device** column, click **Add All**.
- 5 To remove devices from the Site Devices column, select the devices to be moved.
- 6 Click **Remove**. The selected devices are moved from the Site Devices column into the Network Devices column. Or, to remove all devices from the Site Devices column, click **Remove All**. The devices that remain in the Site Devices Column are assigned to the site type.
- 7 When you are finished selecting devices to be managed under the current site type, click **OK**. The Managed Devices window closes.

---

**Note** If the tree menu does not immediately refresh to display the devices, right-click on the Site type, and select **Refresh**.

---

## Editing Device Associations to Sites

The location of network devices can change. This could be something as simple as moving a rack of devices to another room, or as complicated as relocating devices from one geographical location to another. Regardless of the level of difficulty, Network Configuration Manager handles the changes with ease.

A Site Type can be edited in two ways by:

- [The General Tab - Editing Site Properties](#)
- Editing the network devices associated with a site type

Assigning devices to a site type in the hierarchy function can be done, but you can also move devices from one site to another site using the drag and drop action.

There are three ways to move devices site-to-site:

- Using the same method used to [Assigning Devices to Sites](#) when it was created
- Dragging and dropping devices into sites
- Moving devices in the tree menu

To drag and drop devices in a site hierarchy,

---

**Note** The drag and drop feature works only in the diagram view.

---

- 1 Open the site type where the devices currently reside.
- 2 Double-click on the site **type**. The Network Configuration Manager [Network Name] > Site Type window opens. All devices and child site types display in the right pane.
- 3 **Click (and hold)** the devices to be moved.

In the table view, a string of devices can be selected by holding down the Shift key while selecting devices. Or, select multiple, non-sequential devices can be selected by holding the Ctrl key while selecting devices. In the diagram view, hold the Shift-key while making selections.

- 4 Drag the selected device to the **child site**. If the tree menu does not immediately refresh to display the devices, right-click on the site type, and select **Refresh**.

To move devices in the tree menu,

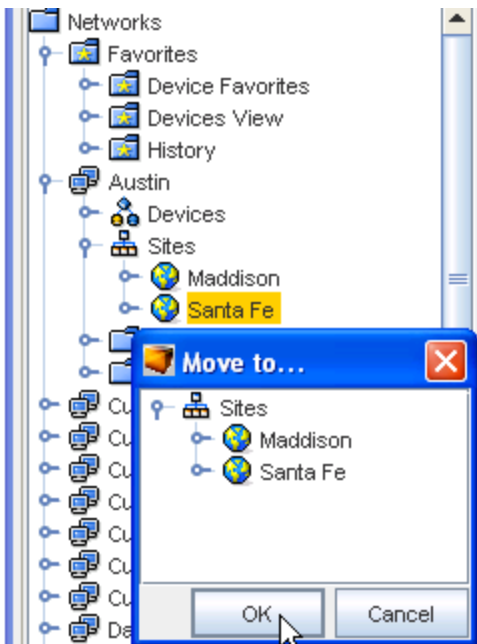
- 1 In the tree menu, select the **devices**.

---

**Note** A string of devices can be selected by holding down the Shift-key, while selecting devices. Or, select multiple, non-sequential devices can be selected by holding down the Ctrl key, while selecting the devices.

---

- 2 After all the devices are selected, right-click on one of the **selected devices** . The Move To... window opens.



- 3 Expand the Sites tree menu until the site where the devices will be moved is displayed.
- 4 Select the **Site**.
- 5 Click **OK**. The window closes. If the tree menu does not immediately refresh to display the devices, right-click on the site type and select **Refresh**.

## Symbolic Device Links in Sites



Due to the physical nature of Sites, devices may exist in only one network and one site. This is logical, considering that a switch or router can physically exist in only one rack, in one room, on one floor, in one building, and in one geography at any time. However, symbolic links for any device can be placed in other sites or networks. This allows connected neighboring devices (that may exist in other networks or sites) to be accessible in the local site, for management convenience.

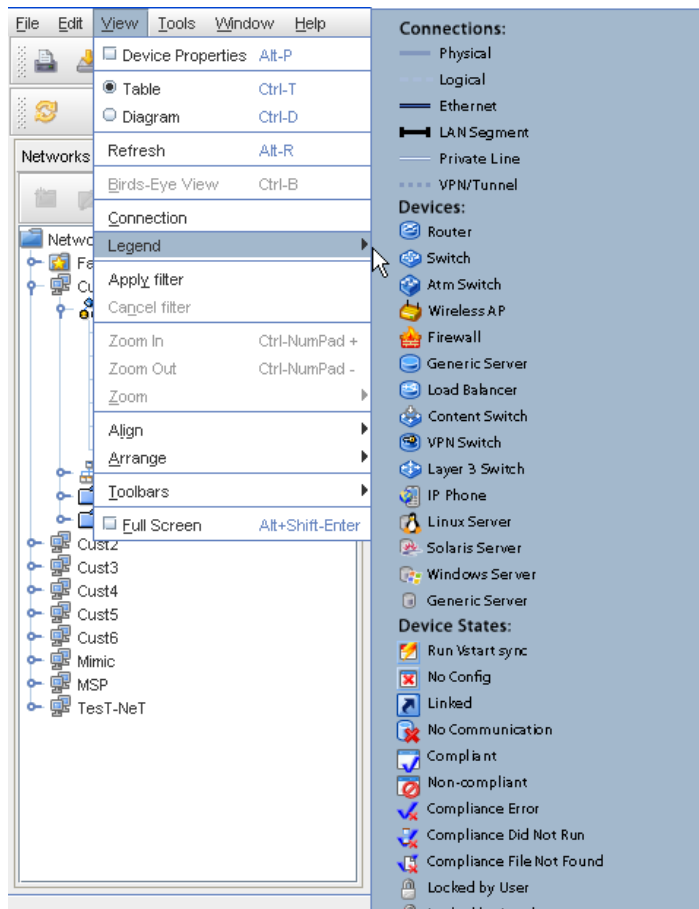
Security for managing symbolically-linked devices comes from the original device, or its primary network. Therefore, a user with no permissions to a device or its primary network, would visually see that device symbolically-linked in another network site, but they will not be able to view or manage that device.

See [Setting Network Permissions](#) for more information on device security.

## Sites - Legends

### Using the Legend

The Legend is part of the Diagram menu bar, and will only be available when using the Diagram layout to view your sites. Review the following legend information to discover the meaning of each icon when viewing your sites.



1 From the Menu bar, select **View**.

2 Next, select **Legend** from the options to view the legend details.

## Sites Property Tabs

### The General Tab - Editing Site Properties

Site properties contain contact and location information for the Site. By default, Sites inherit the properties of the parent Site, unless the Override check box is selected. Devices in Sites inherit Site properties which are displayed in the Site tab of the Device Properties.

Comments and Attachments can be associated with a Site. Site objects also support Data Fields.

The (General) properties of a site are the details entered when the site hierarchy was created. Added to this information are two additional tabs:

- [The Comments Tab](#)
- Attachments

---

**Important** You must follow the nesting hierarchy [Sites Best Practices](#). For more information, see [How Sites and Views Work](#).

---

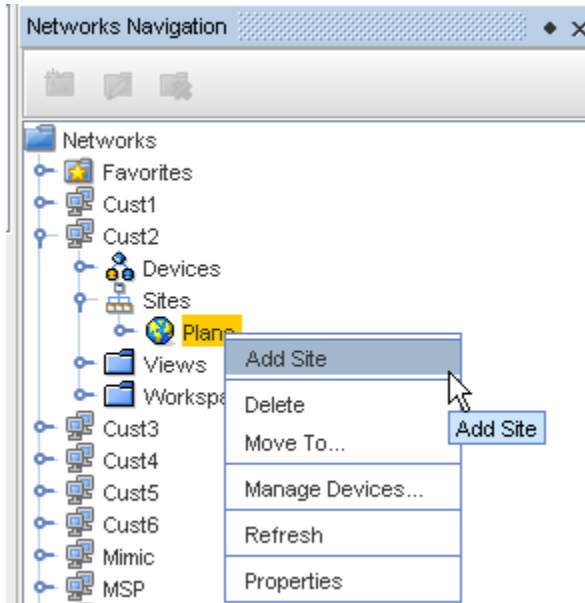
A site type can be edited in two ways:

- Editing the site type properties
- [Editing Device Associations to Sites](#)

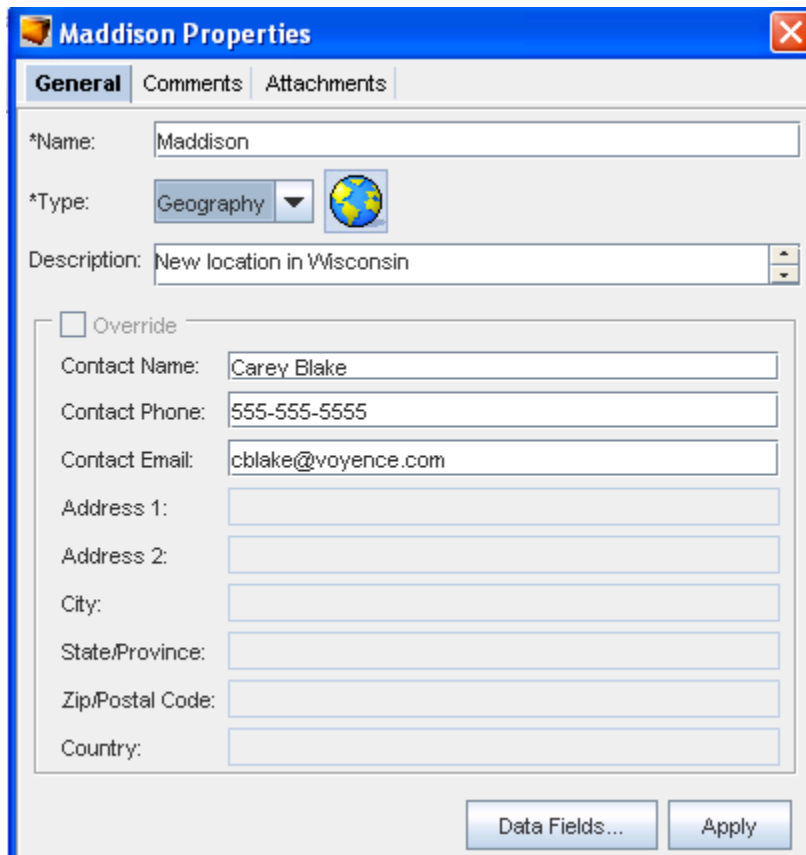
The ability to edit the site type properties allows you to modify the Name, Site Type, Description, and Override information, if needed. This information works hand-in-hand with the ability to edit the devices associated with the site type. Anytime that you edit the site type, you should review the devices associated to the modified site type.

To edit a site types properties,

- 1 In the tree menu, open the **Sites** branch.
- 2 Expand the tree menu, then right-click the appropriate **Site**.



- 3 From the right-click options, select **Properties**. The [Site Name] Properties window opens.

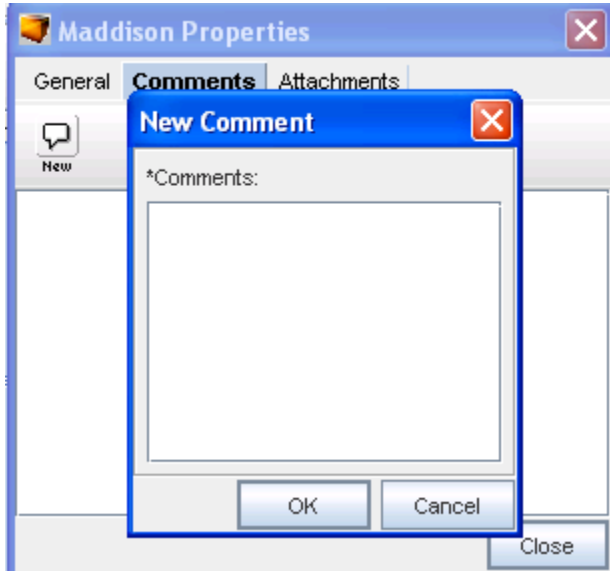


- 4 All fields in the properties window can be edited. **Edit the information** as needed.

- 5 To enter contact information specific to this site (in the **Building**, **Floor**, **Room**, and **Rack** types - selected from the Type drop-down) check the **Override** box. The Contact field information window activates allowing you to add additional entries to the previously empty sections.
- 6 When finished, click **Apply**. The [Site Name] Properties window closes.

## The Sites Comments Tab

The **Comments** tab contains a running list of comments, related to the site.



The comments are logged as they are entered. Each comment identifies who created the comment, and when. A broken line indicates the end of each comment.

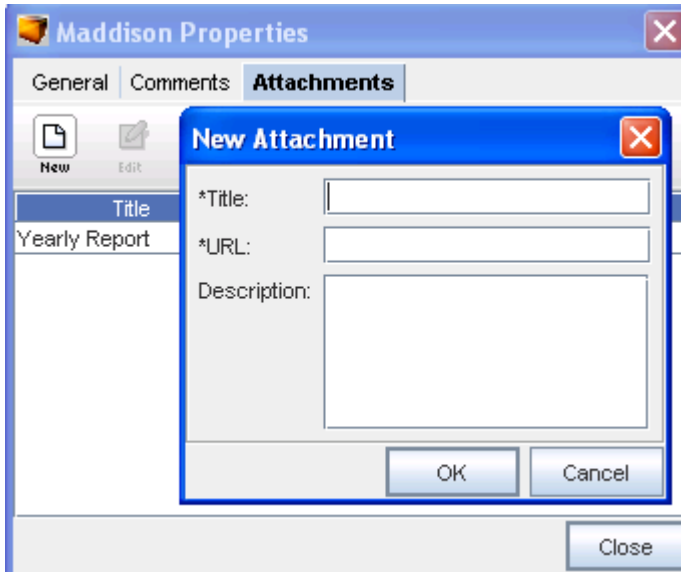
To create a new comment,

- 1 On the Comments tab, click the **New Comment icon**. The New Comments dialog window opens.
- 2 Enter your **comments**. The Enter key can be used to create paragraph breaks in the comments.
- 3 Click **OK**. The New Comments window closes. Each new comment is added to the top.
- 4 For each new comment, repeat **steps 1-3**.

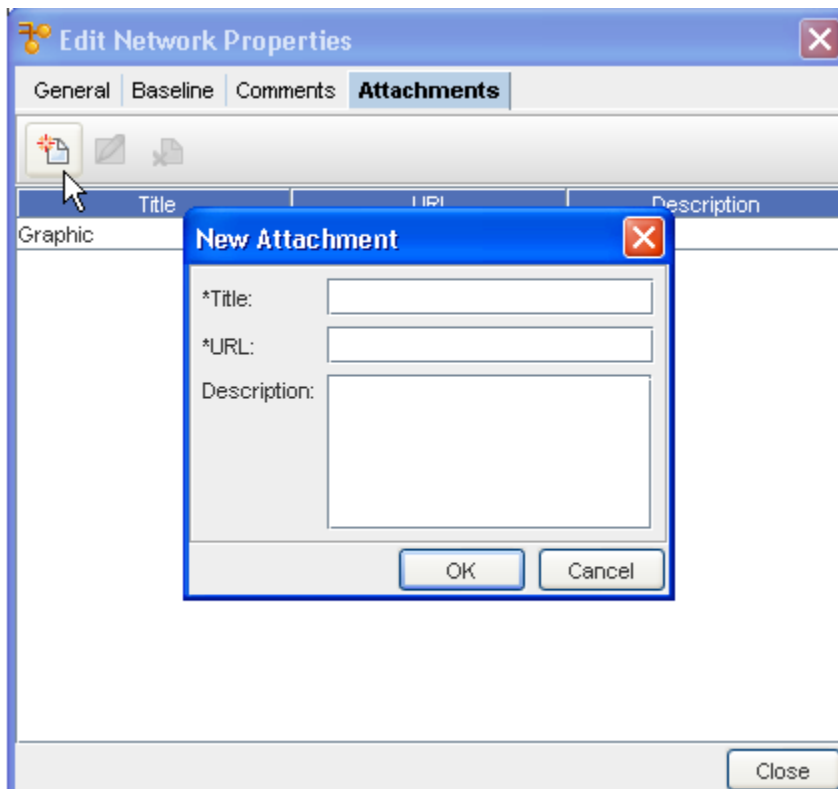
## The Sites Attachments Tab

The **Attachments** tab allows you to associate an external file to the site. This can include worksheets, documents, or .html files. Any document that can be opened in a web browser can be mapped as an attachment.

Multiple attachments can be added to each site.



### Adding an Attachment



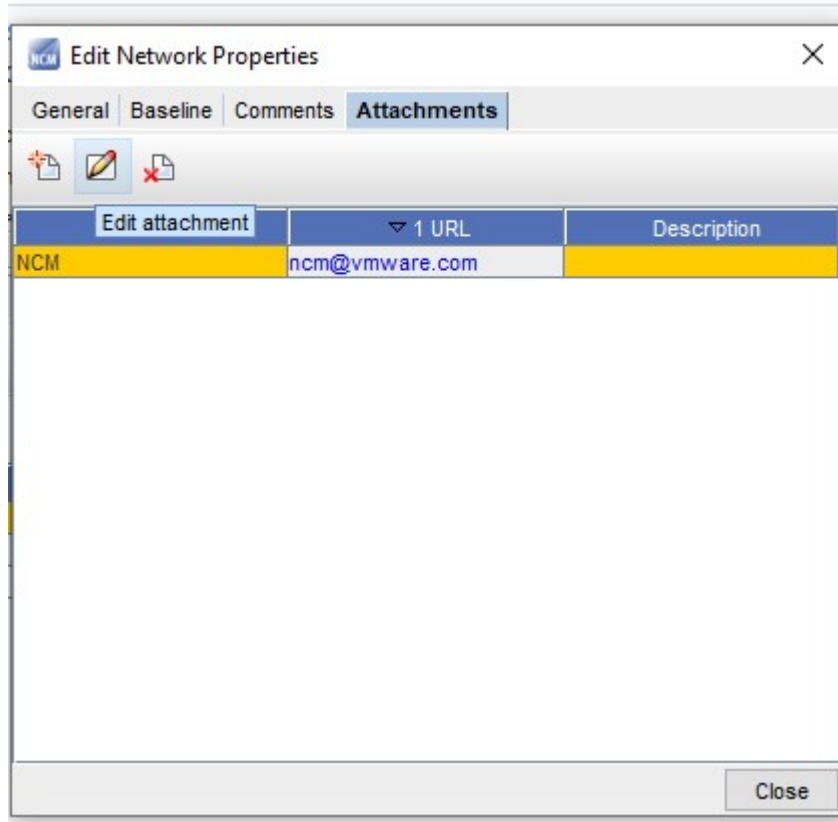
To add an attachment,

- 1 On the **Attachments** tab, click the **New icon**. The New Attachments dialog window opens.
- 2 Enter a title **for the attachment** .
- 3 Enter a **URL**. Remember, the document must be saved in a format that will open in a browser.
- 4 If needed, enter a **description**.

- 5 Click **OK**. The New Attachments window closes.
- 6 For each new attachment, repeat **steps 1-5**.
- 7 Click **Close** when you are finished adding attachments.

**Note** The Edit and Delete icons are only active when one or more attachments have previously been created.

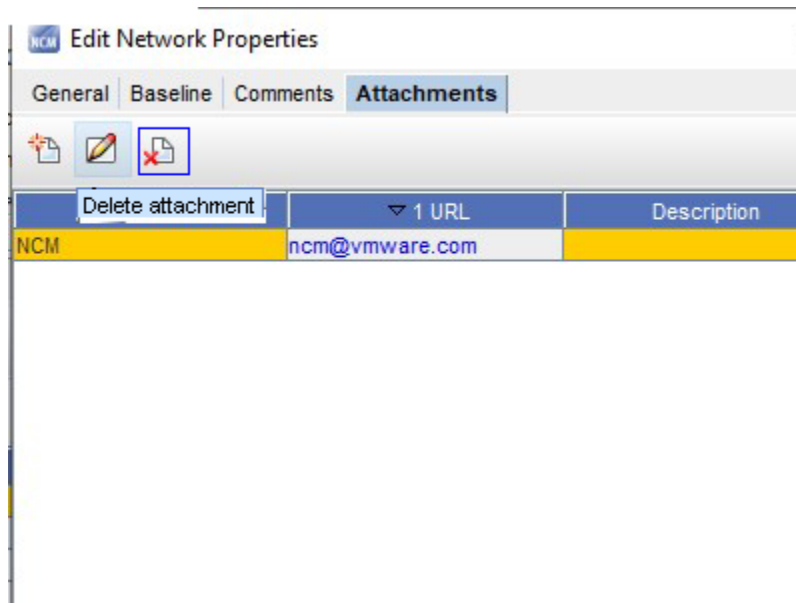
## Editing an Attachment



- 1 First, select an attachment from the listing of attachments.
- 2 On the Attachments tab, click the **Edit** icon. The Edit Attachments dialog window opens.
- 3 The Title, URL and Description fields can all be edited. Make any changes as needed.
- 4 Click **OK**. The Edit Attachments window closes. The attachment row updates with the edited details.
- 5 Click **Close** to close the Edit Network Properties window.

## Deleting an Attachment

When deleting an attachment, the actual document that you are referring to is **not** deleted. You are removing its linked reference from Network Configuration Manager.



- 1 First, select an attachment from the list of attachments.
- 2 On the Attachments tab, click the **Delete** icon. The Confirm dialog window opens asking, "Are you sure?".
- 3 To delete, click **Yes**.
- 4 Click **OK**. The Confirm window closes. The Attachment tab refreshes.
- 5 Click **Close** when you are finished deleting attachments from the list.

## Working with Views

### Views Overview

---

**Note** Views have no relationship with Sites!

---

Each network in Network Configuration Manager contains a single view folder construction, which is created at the same time as the network. There is no requirement to create and manage views within each network.

If your organization prefers to manage network resources using sites to create a geographical relationship, there may be no benefit to organizing your devices logically in Views. By default, the views folder is empty. However, a separate view, called the All Devices view is provided and populated with every device discovered in the network.

As there is no need for a relationship to existing between devices in a view, there are no predefined view types. And unlike Sites, devices can display in as many Views as needed, eliminating the need to support symbolic-linked devices in Views. Views are simply logical collectors for devices, and as such have no attributes except for having a name.

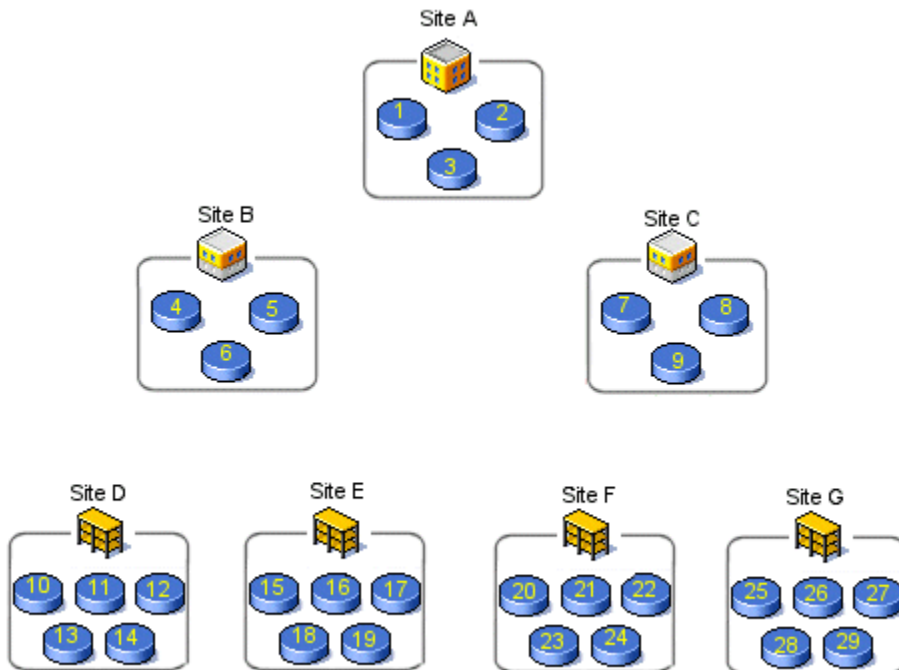
Views and their folder structure can be completely customized to fit your organizational needs.

- One sub-set of folders could be dedicated to Views of devices organized by vendor and model.
- Another sub-set could be dedicated to devices sorted by connection type.
- A third could be grouped by organizational responsibilities. In effect, you can slice and dice your devices any way you choose in Views.

Views enables you to create and organize collections of the devices in a network. When creating a view of a device, there is not a dependency on site type, logical connections, or physical location. A view allows you to select devices and group them together.

As an example, the following is a collection of devices in a network. Using the devices in the collection, you could make the following Views. Since devices in a view do not require a relationship, physical relationships, or logical connections, the Views are random groupings of devices of your choosing.

View 1	View 2	View 3	View 4	View 5
Contains Devices: 1, 7, 20, 21, 24	Contains Devices: 4, 9, 12, 18, 23	Contains Devices: 3, 10, 11, 14,	Contains Devices: 5, 6, 13	Contains Devices: 25, 26, 27, 28, 29



**Note** The examples are not the only view scenarios that can be extracted from the graphic.



## View Memberships

Views offer a unique feature that allows you to automatically assign devices to a view through the use of memberships. Memberships provide a dynamic network filter capability in a view. You do not need to manually assign devices to a view with a membership filter.

Memberships are based on the same pre-defined attributes, providing the ability to create device types or technology type memberships, or any combination of the two. For example, to see a view that contains all routers in your network that have Frame Relay connections.

You could easily create a new, empty view named "Frame Routers" and set the membership of that view to include device type 'router', and technology type 'frame relay'. At that point, the view would be populated with all Frame Relay routers. Additionally, the view will dynamically update each time it is opened with any new frame routers that have been discovered into the network, and delete any that have been removed from the network.

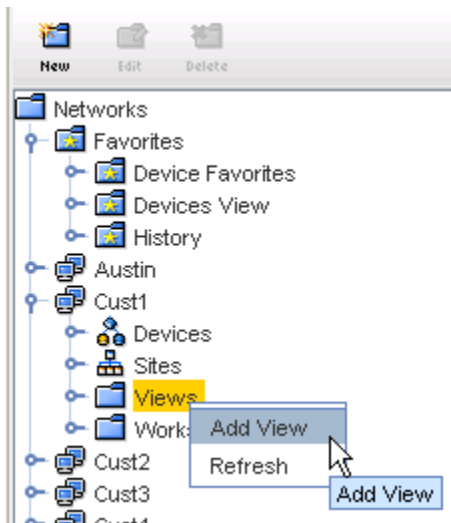
View memberships provide a quick and flexible way to logically segment your network by device and/or technology.

See: [How Sites and Views Work](#) for more information.

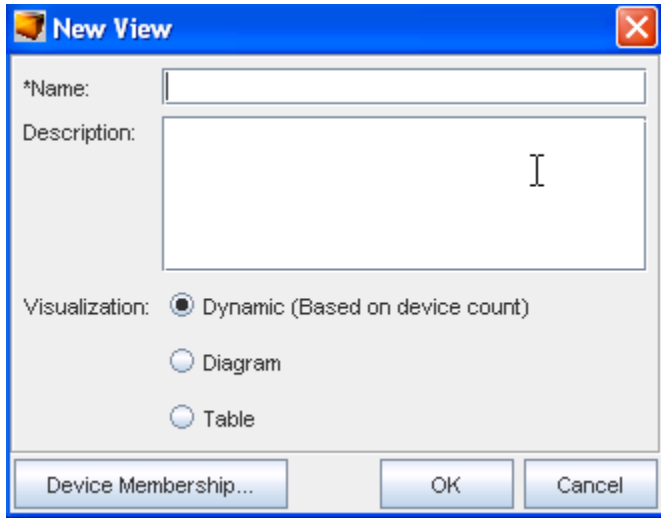
## Creating Views

To create a view:

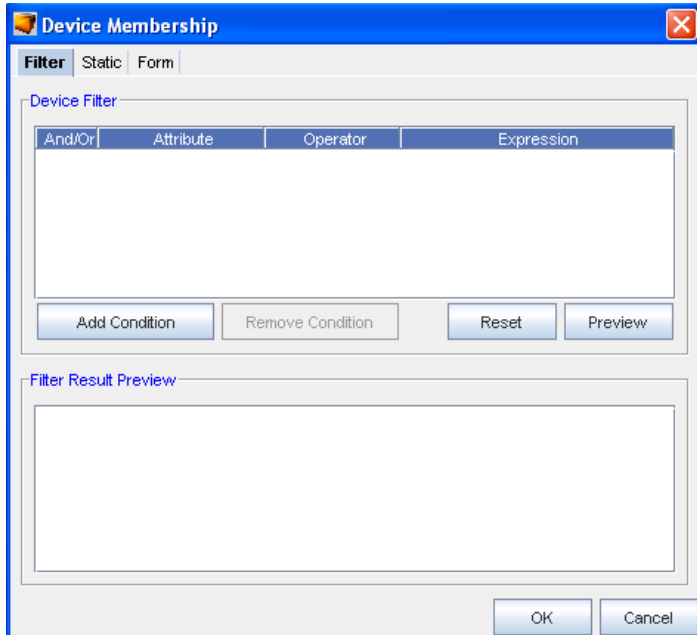
- 1 In the Networks navigation tree, right-click **Views**.
- 2 From the menu options, select **Add View**.



The **New View** window opens.



- 3 In the New View window, enter the **view name**. There are three options for how the view will display when opened.
  - **Dynamic** - (based on the device count. This will open in either the diagram or table view, depending on the device count). Note that this is the default.
  - **Diagram** - layout using device icons
  - **Table** - layout of device properties in table format
- 4 To change the default setting, select a new **visualization** (view) option.
- 5 To add devices to the view, click **Device Membership**. The Device Membership window opens.



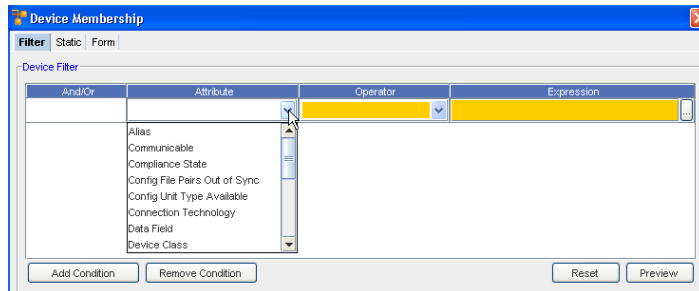
The Device Membership window contains three tabs:

**Filter** Allows you to filter devices by setting conditions based on the device type, name, vendor, or model, or other criteria, and then save the filter settings

**Static** Allows you to select from a list of all the available network devices

**Form** Allows you to select from a list of queries

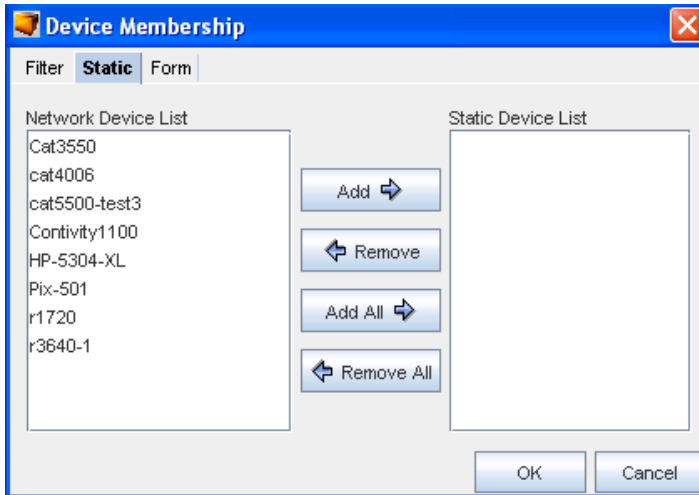
To filter devices:



- 1 Click **Add Condition**. A row is added in the Device Filter section. Determine if you want to use the **And/ Or** for the filter, then select accordingly.
- 2 Click once inside the Attributes column, the attributes the devices can be defined by are displayed.
- 3 Select an **Attribute** from the list.
- 4 Click once inside the **Operator** column. Select an **Operator** from the list.
- 5 Double-click once inside the **Expression** column. Select from the available options (if provided), or enter an expression. Enter the **Expression** that defines the attribute.
- 6 If entering more than one filter, click **Add Condition**. A new row is added to the Device Filter section.
- 7 To add additional filters, repeat **steps 1-6**.
- 8 When the filters are set, click **Preview**. A preview of the filtered results displays in the Filter Result Preview window.
- 9 When finished setting the filter, click **OK**. The Device Membership window closes. The filter devices display in the selected view.

To select from a static list of network devices:

- 1 In the Device Membership window, select the **Static tab**.



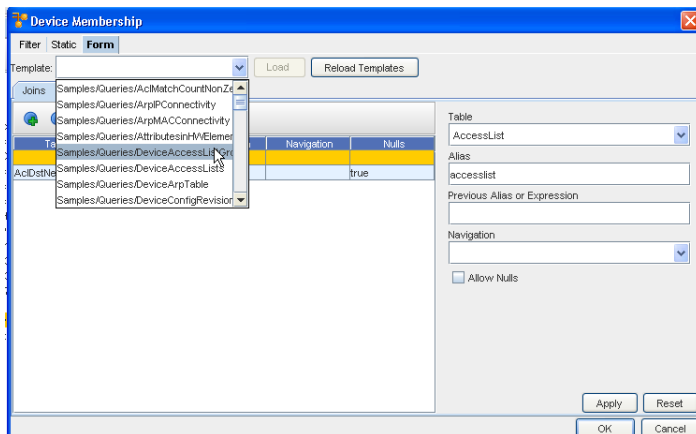
The Static tab contains two columns:

- 2 Using the **Add** and **Remove** buttons, create a list of static devices from the selections in each list.
- 3 When finished, click **OK**. The Membership Device window closes.
- 4 On the New View window, click **OK**. The New View window closes, and the created view opens, allowing you to review the configuration.

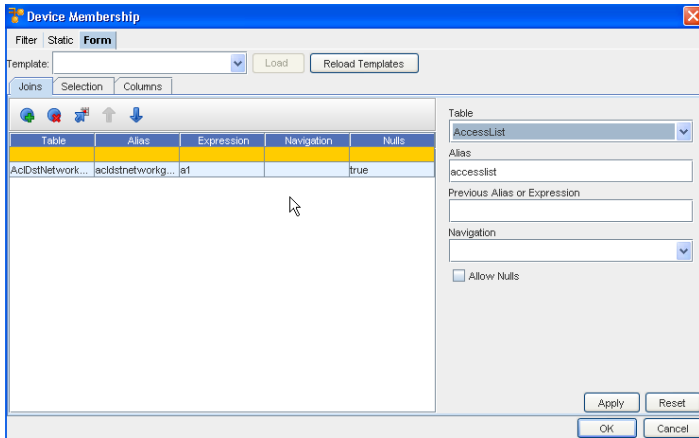
**Network Device List** Here are the devices that are associated with your network. These devices are available even if they are not set up in a site hierarchy.

**Static Device List** These are the devices that are used in a defined view.

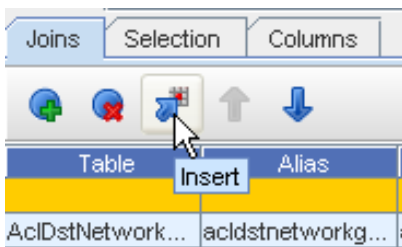
To use the Form tab:



- 1 From this tab, first click the **Template** drop-down, and then select a template from the list.
- 2 If you are not using a pre-defined template, make selections from the **Table** drop-down.



3 Click the **Insert** icon to insert a table.



4 Add an **Alias**, and also a **Previous Alias or Expression** .

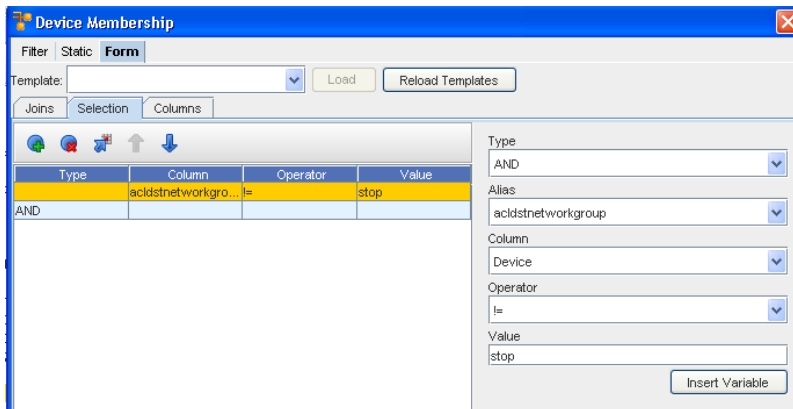
5 Select a **Navigation**.

6 Check to **Allow Nults** if needed.

To complete the Selection section:

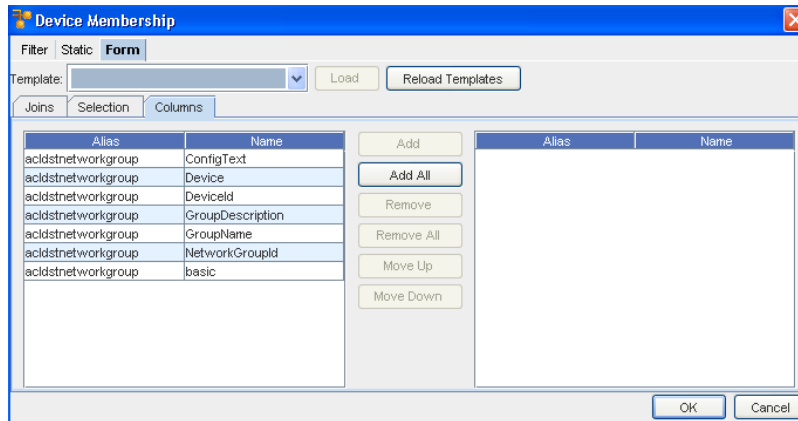
1 Insert a line, then select a **Type**, **Alias**, **Column** and **Operator** from the drop-down arrow menus.

2 Enter a **Value**, then click **Ok**.



**Important** Ensure you note the red warning signs and information. You must make sure those errors are gone before clicking OK to continue.

To complete the Columns section:



- 1 First determine the **columns** you wanted added, then select them from the listing.
- 2 Next, use the **Add** or **Add All** to move the selected columns into the right pane.
- 3 Click **Ok**.
- 4 Now, back at the **Filter** tab, click **Apply**.

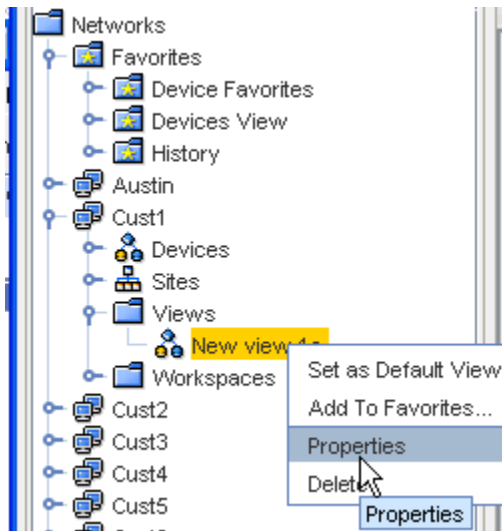
## Editing Views

There are two ways to edit a view:

- Editing the general properties of the view
- Editing the devices within the view

To edit the view properties,

- 1 In the navigation pane, select the **Network**, then **Views**.
- 2 Right-click on the **View**.



- 3 In the right-click menu, select **Properties**. The [View Name] Properties window opens. All text fields are editable. Make changes as needed.
- 4 When finished, click **OK**. The [View Name] Properties window closes.

---

**Note** You can select this view as your **Default View**, and you can also Add this View to your **Favorites**.

---

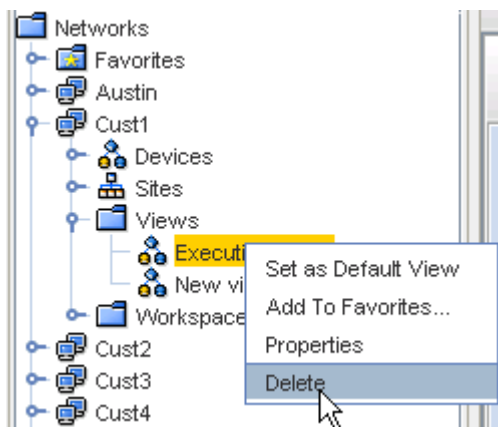
To edit devices within a view,

- 1 In the navigation pane, select the **Network**, then **Views**.
- 2 Right-click on the **view**.
- 3 In the right-click menu, select **Properties**. The [View Name] Properties window opens.
- 4 Click **Device Membership...** The Device Membership window opens.
- 5 You have three options:
  - On the **Filter** tab, use device filters to locate devices
  - On the **Static** tab, select from a list of network devices
  - On the **Form** tab, make your edit changes in the Joins, Selection, and Columns tabs
- 6 When finished, click **OK**. The [View Name] Properties window closes.

## Deleting Views

To delete an existing view,

- 1 In the navigation pane, select the **Network**, then **Views**.
- 2 Right-click on the **View**.
- 3 In the right-click menu, select **Delete**.



The Confirm window opens asking: Are you sure?

- 4 If okay, click **Yes**. The confirm window closes.

- 5 If the navigation pane does not automatically refresh, right-click on the Network's View folder and click **Refresh**.

## Working within a Workspace

### Workspaces Overview

As Configurations cannot be saved to the repository, Workspaces serve as **work in progress containers** for projects. Working copies of existing Network devices and new virtual devices can be stored in a Workspace during the design phase.

When an existing device is copied into a design Workspace, it actually represents a different object.

Workspaces are work areas that can contain both virtual and network devices. Workspaces are not an actual view of a network, but a configuration of possible network scenarios. When actual devices are placed in a Workspace, the device's relationship to the network that is managing it, is unaffected. Relationship to the original device is maintained to reflect which configuration revision was used for the Workspace copy.

Workspaces are designed to provide flexible and convenient ways of:

- Creating disaster scenarios
- Designing technology upgrades
- Managing additions to existing networks
- Planning new network configurations
- Alerting you when a config has been modified locally, and differs from the network config

Workspaces are directly associated with a specific network and cannot be shared with other networks. If a similar Workspace is required, the workspaces can be saved as new workspaces, and then changed to reflect the needs of the new design.

With Multi-Config, you can design devices with a copy of the operational device state that includes multiple files. You can also create virtual devices, and then add the content of each file type supported by the device.

Workspaces use the same iconic representation of devices that are seen in the Views and Sites diagrams of the network. As changes to devices are made, device indicators show the status of the device. The device status represents its relationship to the device, as currently deployed in the network.

The exception to Views and Sites is the **Schedule** feature (in the menu bar) available only in the Workspaces view when a device is selected from the view.



## Workspace - Menu Bar options



You can go directly to the Schedule Manager to [Scheduling a Run Time](#) from this window. This feature is identical to the **Schedule** right-click option, when viewing the Workspaces.







## Workspace Tool Bar Options











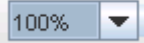
Here are the options located on the **tool bar** when Workspace Devices are displayed.







**Note** Those options in the tool bar that are grayed-out are not accessible.



The options include the following:

Icon	Icon Meaning	Action
	Print	Takes you your browser's print facility, where you can print the current view.
	Export	Takes you to the Save window where you can select the location to save this view, and in what format you want to save.
	Device Search	Takes you to the Device Search window where you can enter information to search on a specific device.
	Config Editor	Takes you to the Config Editor. This editor is designed for editing a single, full running configuration file that affects one or more devices.
	Configlet Editor	Takes you to the Configlet Editor. This editor is used to edit whole or partial configurations that are Pushed to the network.
	Interface Editor	Takes you to the Interface Editor. This editor is used to <b>make changes to multiple interfaces on multiple devices</b> . Global area.

Icon	Icon Meaning	Action
	Command Editor	Takes you to the Command Editor. The intent of the Command is not to change or update a device's configuration, although a Command can be used for this purpose. The intent is to provide access to device-level information for completing actions.
	Schedule	When accessed, you are taken to the Schedule Manager.  Note: When you select more than one device to be scheduled, you are presented a list of all devices contained within the Workspace. You must check which devices you want to schedule. After this selection, you are then taken to the Schedule Manager.
	New Virtual Device	Only available in the <b>Workspace view</b> . This allows you to create a device that can be added to a workspace for testing or creating "possible" networks.
	Properties	When accessed, the Device Properties tabs are displayed.
	Table View	Displays the list of devices in a table format.
	Diagram View	Displays the list of devices in a diagram format. When accessed, you can switch between Diagram and Table format.
	Birds-Eye View	Displays a birds-eye view of the network only in Diagram view.
	Connection	Displays the Network connections.
	Zoom In	Allows you to zoom in on the Diagram view.
	Zoom Out	Allows you to zoom out on the Diagram view.
	Enlarge/Reduce	Only available in the Diagram view. This can be used to enlarge or reduce the size of the viewing window.

Icon	Icon Meaning	Action
	Align	<ul style="list-style-type: none"> <li>■ Bottom aligns all devices along the bottom of the window.</li> <li>■ <b>Horizontal</b> aligns all devices horizontally in the window.</li> <li>■ <b>Left</b> aligns all devices to the left of the window.</li> <li>■ <b>Right</b> aligns all devices to the right of the window.</li> <li>■ <b>Top</b> aligns all devices along the top of the window.</li> <li>■ <b>Vertical</b> aligns all devices vertically in the window.</li> <li>■ <b>Horizontal</b> aligns all devices horizontally in the window.</li> <li>■ <b>Around</b> not active in this layout.</li> </ul>
	Rearrange Connections	<p>Rearranges the current view of the connections. Including:</p> <ul style="list-style-type: none"> <li>■ Around</li> <li>■ 90 degrees</li> <li>■ Stagger</li> <li>■ Top/Left</li> <li>■ Bottom/Right</li> <li>■ Arrange Connections</li> </ul>
	Legend	<p>Takes you to the legend list. This list contains all the symbols used for the various device states, devices, and connections.</p>
	Apply Filter	<p>Use this to access the Device Display Filter window and select other filter criteria.</p>
	Cancel Filter	<p>Use this to cancel a filter you have just selected, or to cancel a pre-existing filter or set of filters.</p>
	Refresh	<p>After making changes, use the Refresh icon to refresh your current view.</p>

## The Workspace Window

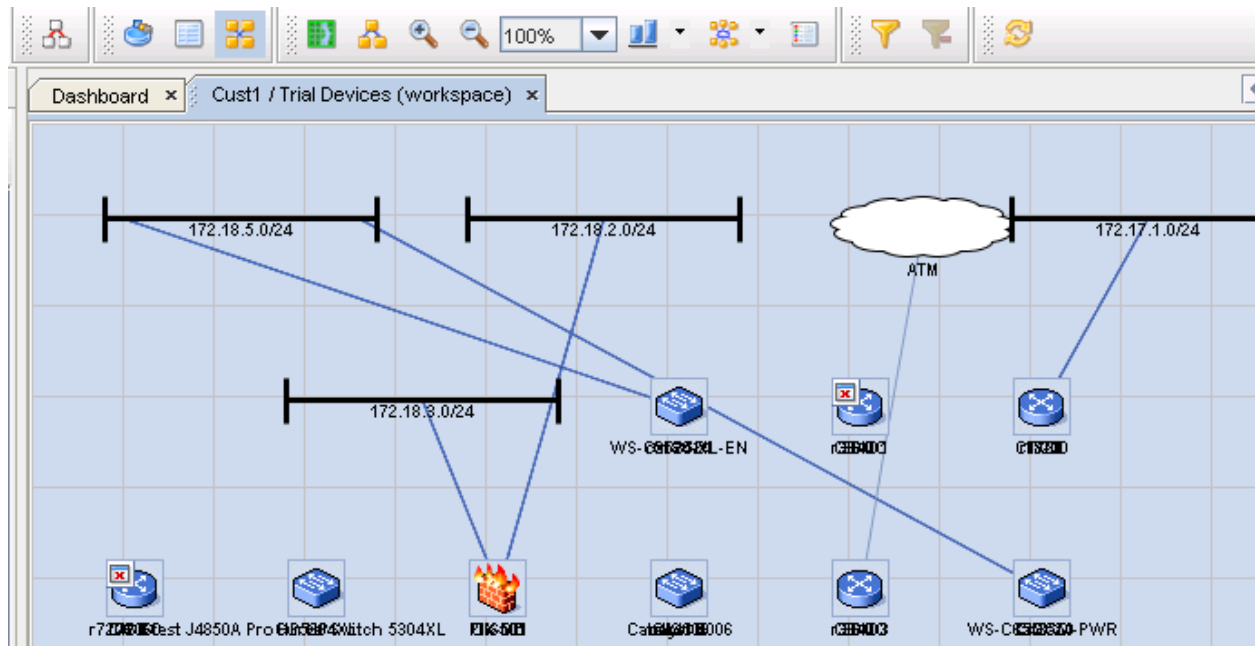
As in a View or Site, how the Workspace displays is determined by selecting the appropriate icons found on the Display section of the menu bar:



- **Diagram view** - a display of all the devices in a network shown in diagram layout, with icons and other visual aids
- **Table view** - a display of all the devices in a network shown in table form
- **Properties view** - opens the properties tabs, at the bottom of the window, of any selected device

## Diagram

Here is an example of the Diagram View.



## Table

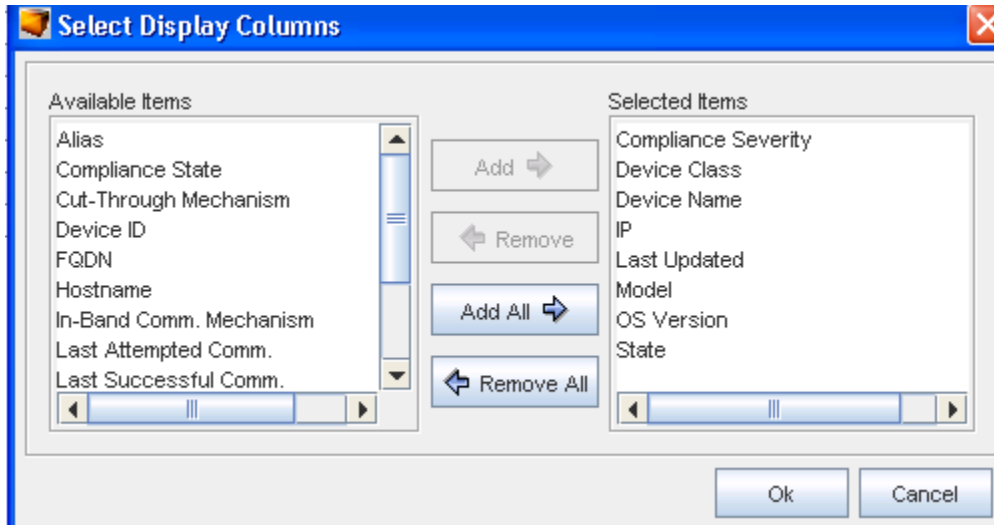
Here is an example of the Table View.

State	Device Name	IP	Device Class	Model
	cat-3524	172.18.5.4	Cisco IOS Switch	WS-C3524-XL-EN
✖	r3640-1	172.18.18.18	Cisco IOS Router	3640
	r1720	172.17.1.2	Cisco IOS Router	1720
✖	r7206-1-test	172.17.0.2	Cisco IOS Router	7206
	HP5304XL	172.17.0.22	HP Procurve Switch	J4850A ProCurve Switch 5304XL
	Pix-501	172.18.2.2	Cisco PIX	PIX-501
	cat4006	172.18.5.6	Cisco CatOS Switch	Catalyst 4006
	r3640-3	172.18.24.8	Cisco IOS Router	3640
	Cat3550	172.18.5.3	Cisco IOS Switch	WS-C3550-24-PWR

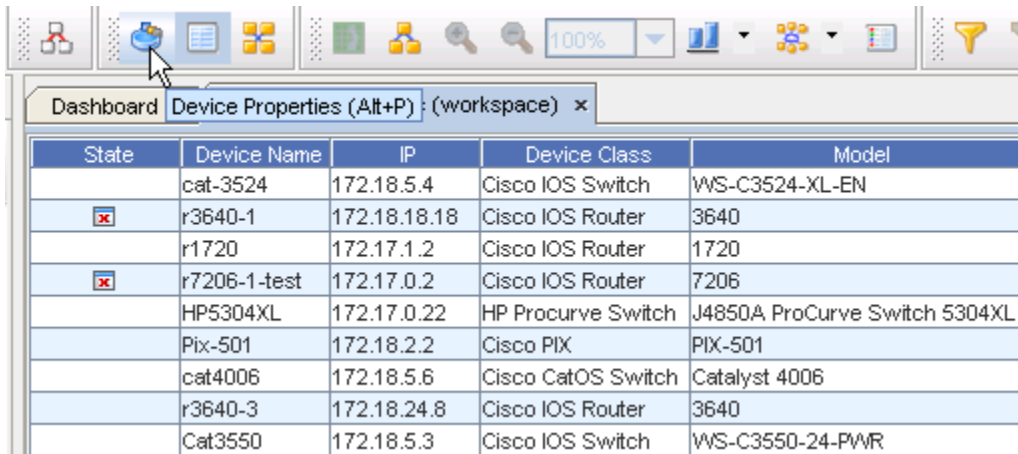
Note the **Refresh** button on the menu bar.

## Column

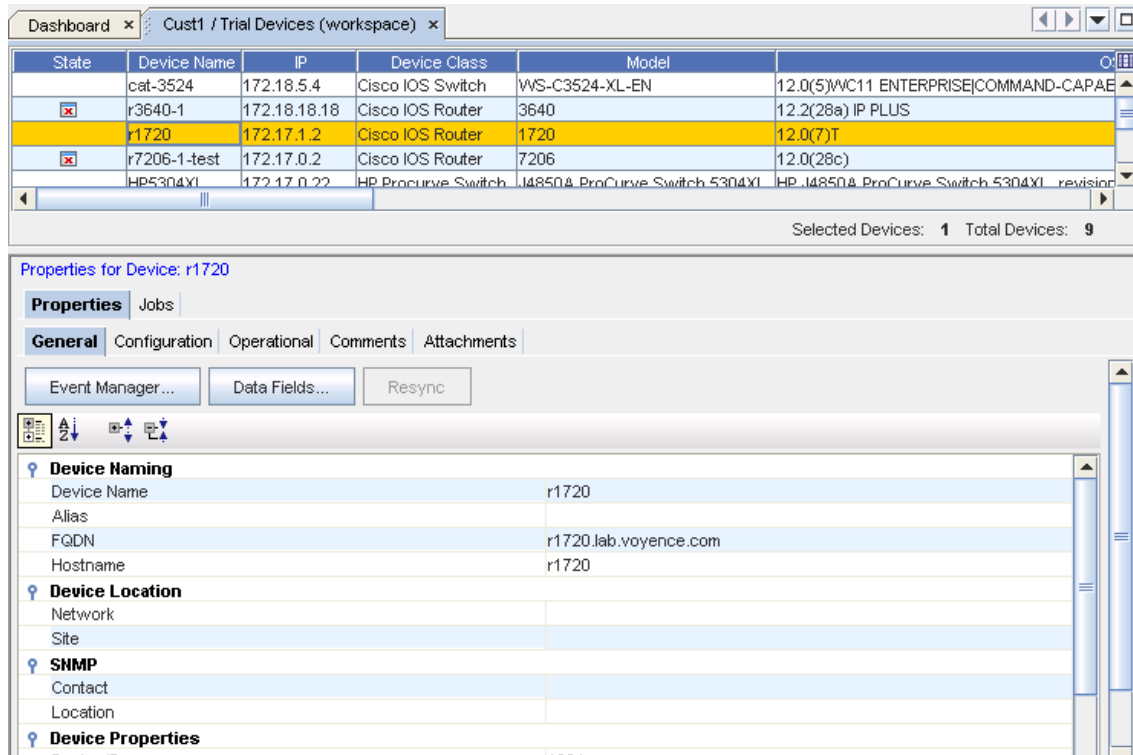
When the Column icon is selected (by clicking within any column heading) , the Select Displayed Columns window displays. From here you can select which columns to display in the Table view of the workspace.



## Properties



When the **Properties** icon is selected, the Properties section is displayed.

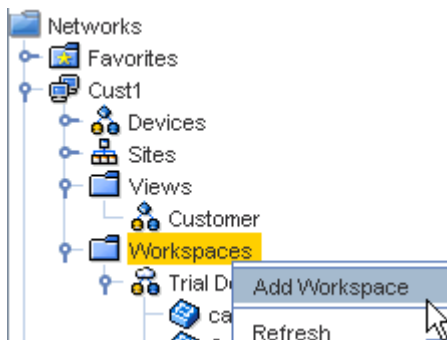


## Creating Workspaces

Workspaces are created within a network, in the Workspaces folder. Because a Workspace and its contents do not affect the network to which it is associated, a network can contain an **unlimited number** of Workspaces with any configuration.

To create a Workspaces,

- 1 Expand the navigation tree, then open the network where the Workspace will reside.
- 2 Right-click on the **Workspaces folder**.

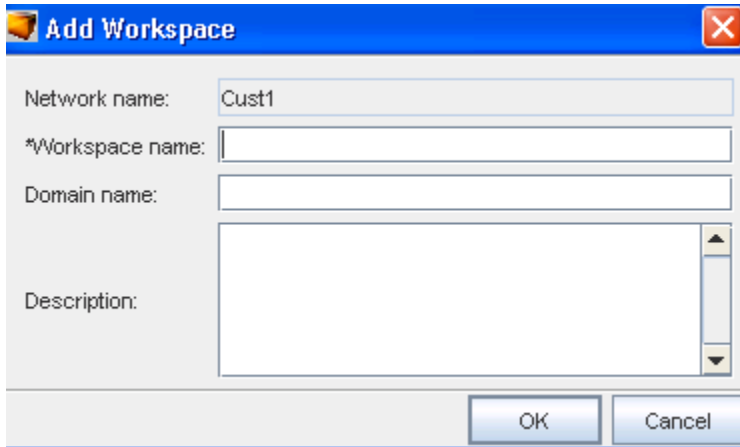


- 3 Select **Add Workspace** . The Add Workspace window opens.

---

**Important** By default, the Network Name field is already populated. This field cannot be changed. If the field does not reflect the network where you intended to create the Workspace, click **Cancel** and select the correct network.

---



- 4 Enter a **Workspace Name** .
- 5 Optionally, enter a **Domain Name** and **Description** for the design workspace.
- 6 When finished click **OK**. The Add Workspace window closes.

---

**Note** In the navigation tree, the Workspaces folder refreshes and contains the new Workspace that you created. If the window does not refresh immediately, right-click the Workspaces folder and select **Refresh**.

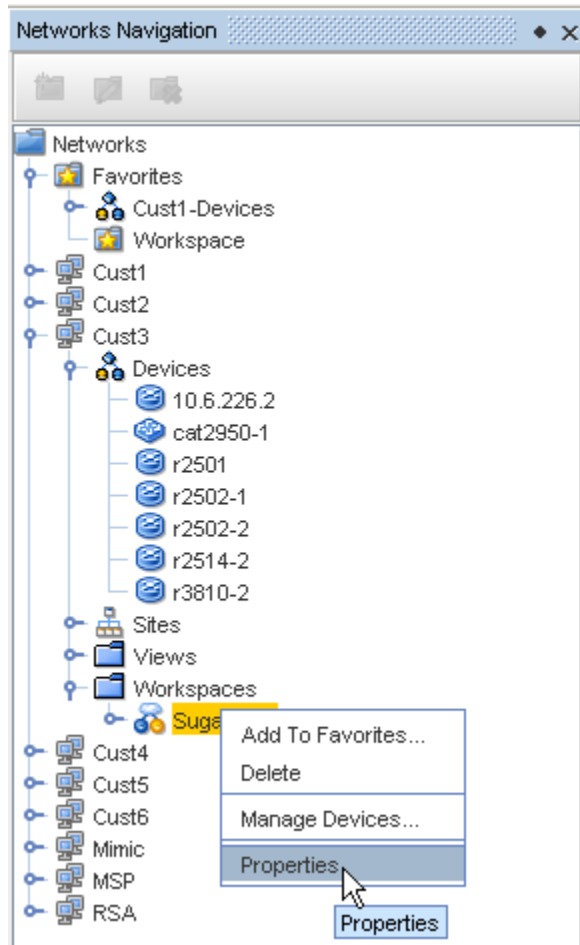
---

Now that the Workspace is created, start [Adding Virtual Devices](#) .

## Editing Workspaces Folder names

Once the Workspace has been created, you can then edit the information within the Workspace to make any needed changes, or add or remove devices within the Workspace.

- 1 From the Navigation tree, select the **Workspace** you want to make changes to.
- 2 Right-click on the Workspace, then select Properties. You can then edit information contained within the properties section.



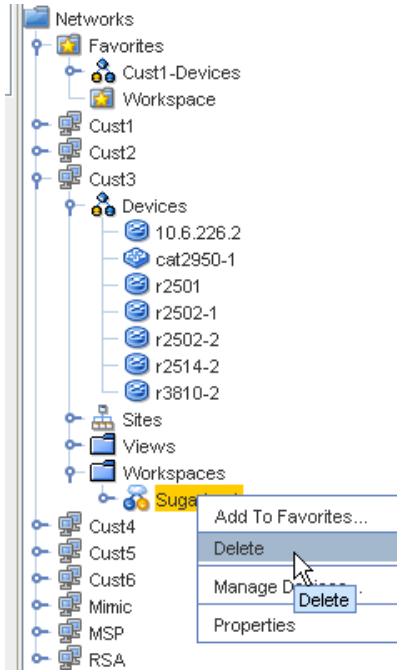
## Deleting Workspaces

When a Workspace is no longer needed, it can be removed from the Workspaces folder. Once removed, the workspace cannot be retrieved. Removing a workspace, and the devices contained within that workspace, does not affect the network it is associated with, or its devices.

To delete a Workspace,

- 1 Expand the navigation tree, then open the network where the Workspace resides.
- 2 At the **Workspace**, right-click to see the menu options.
- 3 Next, select **Delete**.
- 4 The Confirm window opens asking "Are you sure?" If okay, click **Yes**. The Confirm window closes.
- 5 If the navigation tree does not automatically update, right-click in the **Workspace folder** and click **Refresh (if appropriate)**.

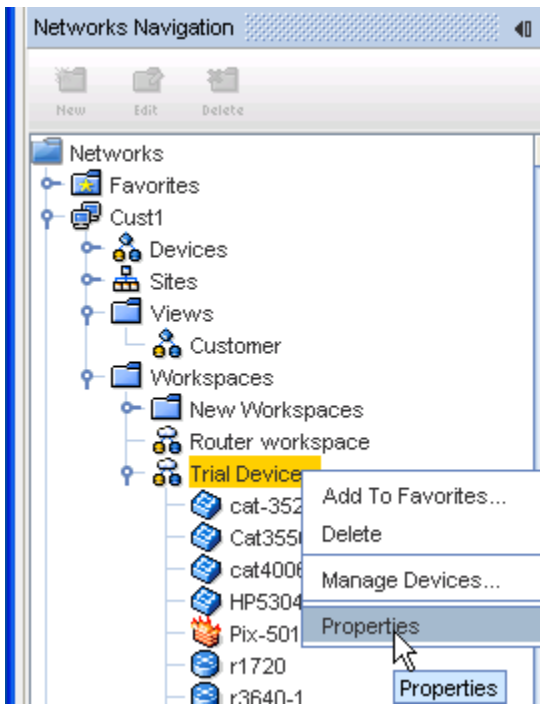




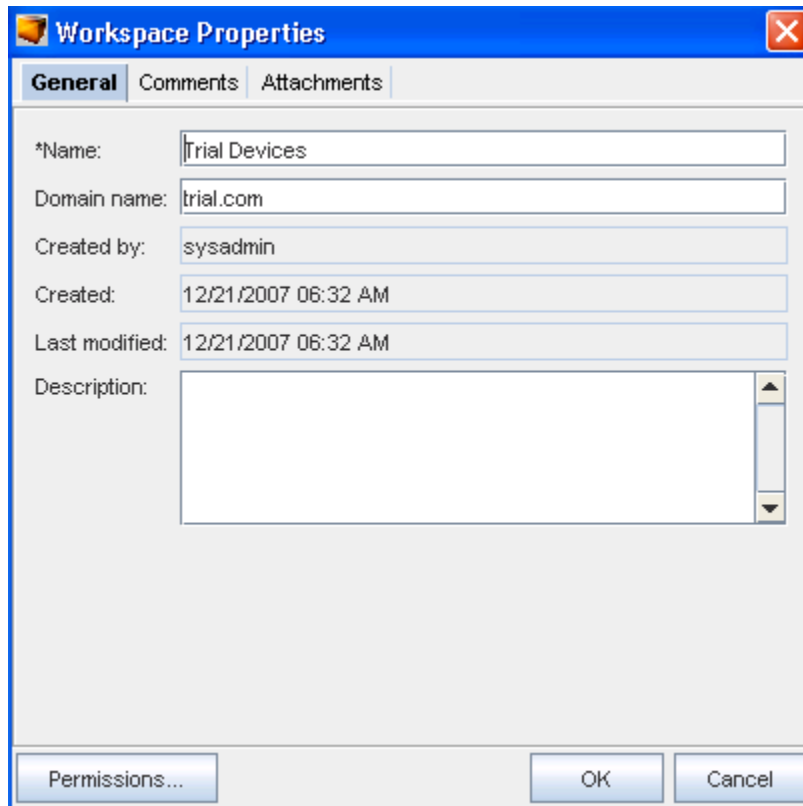
## Workspace Properties - Right-Click Options

### Workspaces Properties Overview

From the Navigation tree, select the workspace you want to make changes to, then right-click and select **Properties**.



The **Workspace Properties** window opens.



The screenshot shows a dialog box titled "Workspace Properties" with a blue header bar and a close button (X) in the top right corner. Below the header is a tabbed interface with three tabs: "General" (selected), "Comments", and "Attachments". The "General" tab contains several text input fields and a description area:

- \*Name: Trial Devices
- Domain name: trial.com
- Created by: sysadmin
- Created: 12/21/2007 06:32 AM
- Last modified: 12/21/2007 06:32 AM
- Description: (empty text area with a vertical scrollbar)

At the bottom of the dialog, there are three buttons: "Permissions...", "OK", and "Cancel".

You can also add this Workspace as a [Favorites Overview](#), or **Delete** this Workspace using the options in the right-click menu.

## The General Tab

**Workspace Properties**

**General** | Comments | Attachments

\*Name:

Domain name:

Created by:

Created:

Last modified:

Description:

Permissions... OK Cancel

#### To make changes to fields in the General tab:

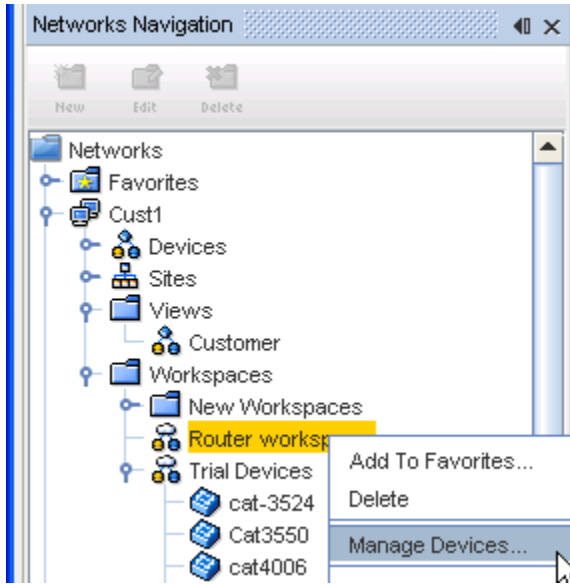
- 1 Click inside the text field, and enter any **new text**.
- 2 To [Setting Workspace Permissions](#) for the workspace, click **Permissions**.
- 3 Click **Ok**, or click the **Comments** tab to continue.

## Adding (Managing) Network Devices

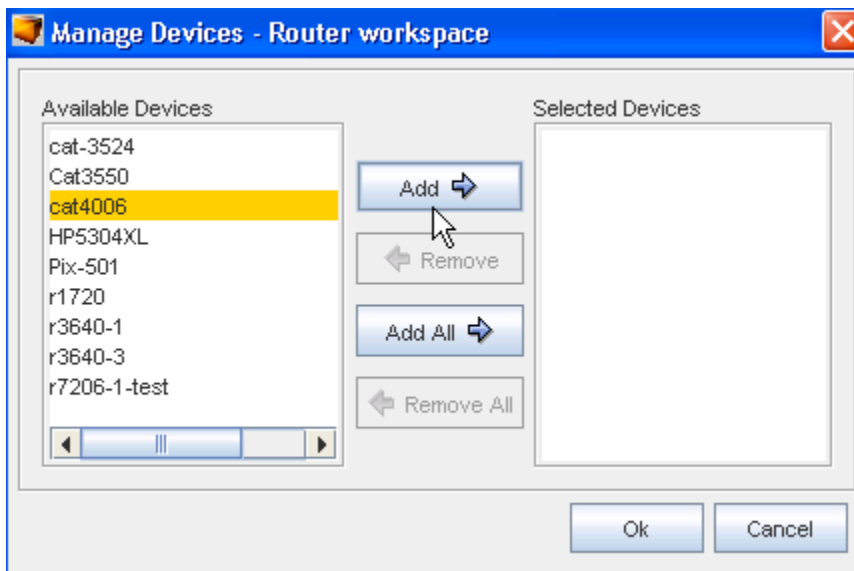
After creating a Workspace, you can begin configuring the layout by [Adding Virtual Devices](#) and adding network devices. Network devices are devices that actually reside, and are managed in a network.

To add network devices,

- 1 In the navigation pane, expand the **Network** where the workspace resides.
- 2 Double-click the **Workspaces folder** to display its contents.
- 3 From the list, select, then right-click on the **workspace**.



4 Select **Manage Devices**.



5 Determine then highlight the devices you want added to the workspace from the Available Devices column, then click **Add**. The selected devices move to the Selected Devices column. You can click Add All if appropriate.

6 Click **Ok**.

---

**Note** In the navigation tree, the Workspaces folder refreshes and now contains the network devices that were added. If the pane does not refresh immediately, right-click the Workspaces folder, and select **Refresh**.

---

When double-clicked, network devices opens a config file you can edit. For more information on editing a config file, see [The Config Editor Window](#)

### Moving a Virtual Device from a Workspace Into a Network

To move a device from a workspace into the Network, first you must **push** the virtual device from the workspace. You must then complete an **Auto Discovery** on that device to get an operational copy. There is no linkage between a device that started out as a virtual, and then becomes operational.

## Adding Virtual Devices

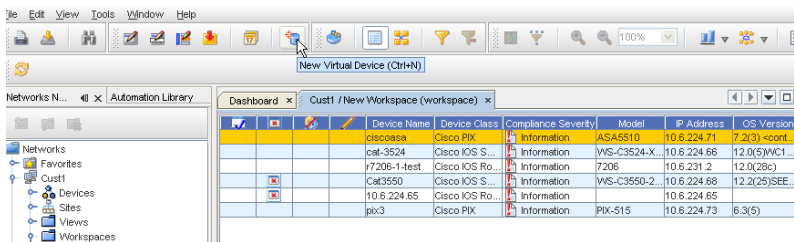
Virtual devices are added to a Workspace using the Virtual icon . A new Virtual devices icons are configuration containers for new Network devices that have not yet been deployed.

Virtual device configurations can be pushed to new devices via out-of-Band mechanisms.

After creating the Workspace, you can begin configuring the layout using Virtual and Network devices.

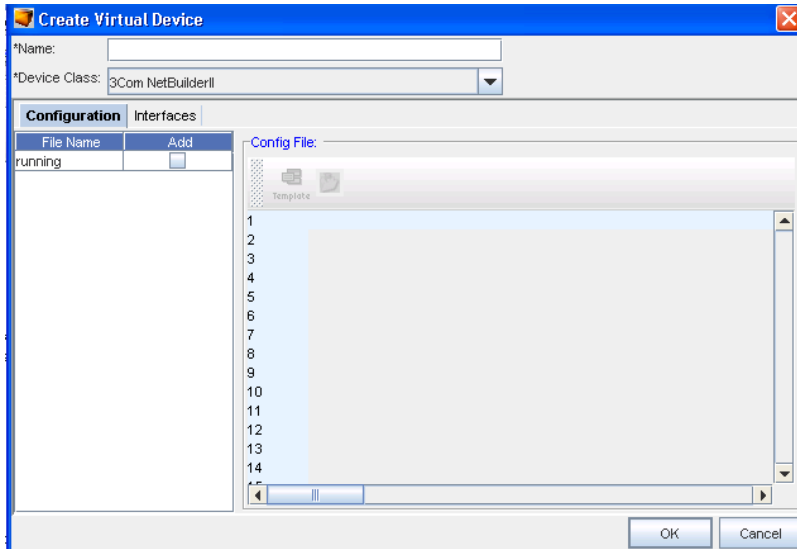
To add virtual devices,

- 1 With the Workspace displayed, select the **Virtual Device** icon from the menu bar. The Create Virtual Device window opens.

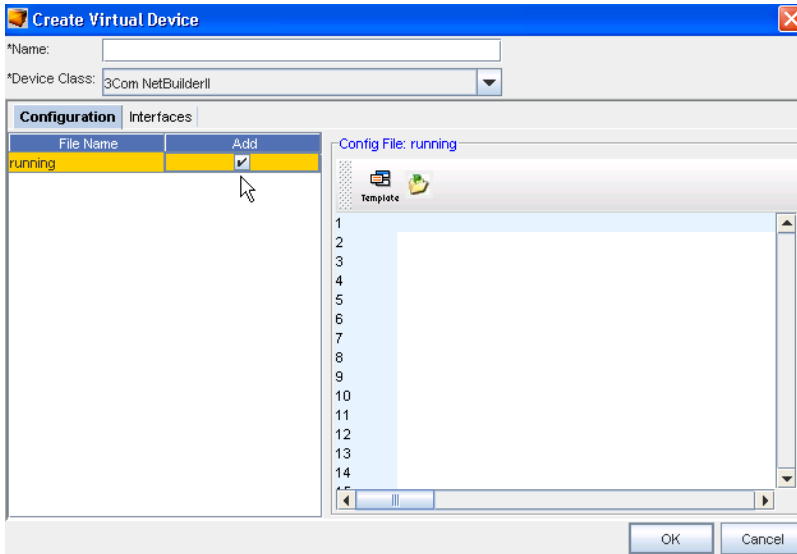


Notice that there are three tabs in this window:

- Configuration
  - Interfaces
- 2 Enter a **Name** for the Virtual Device (if appropriate).
  - 3 You can also use the **Device Class** drop-down and select a different class if needed.
  - 4 In the **Configuration** tab, click **Add** to add any additional items to the workspace.

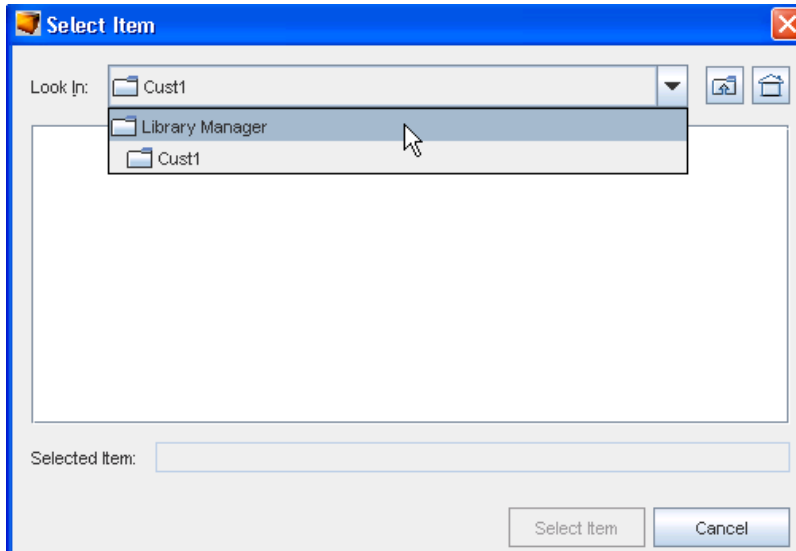


5 Click the **Template** icon to locate a Template to the Config file.



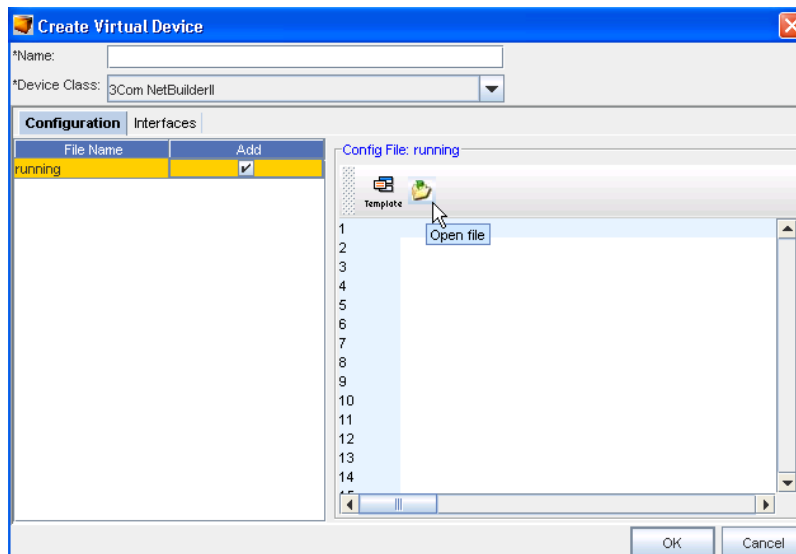
6 Continue to go through the windows to select the appropriate **Template**.

7 Click **Ok** when you have made your selections.



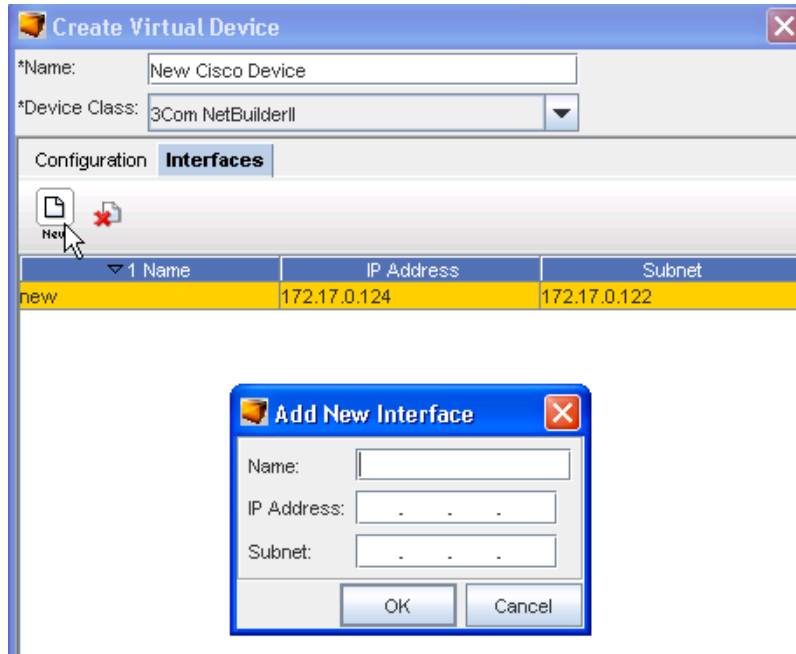
- 8 Next, to add additional items to the running Config file, click the **Open File icon** , and again go through the various windows to add your item.
- 9 Click **Ok** when you have added all items, or click the **Interfaces tab** to continue.

Working with the Configuration tab,



Working with the Interfaces tab,

- 1 Click the **Interfaces tab**.
- 2 Click the **New** icon to add a new interface.
- 3 At the Add New Interface window, enter the **IP Address** and the **Subnet** address in the fields.
- 4 Click **Ok**.



**Important** To remove any interfaces, select the Interface from the list, then click the **Delete icon** . Click **Yes** at the confirmation message.

## Assigning User and Groups Permissions

There are two phases for setting permissions for a workspace:

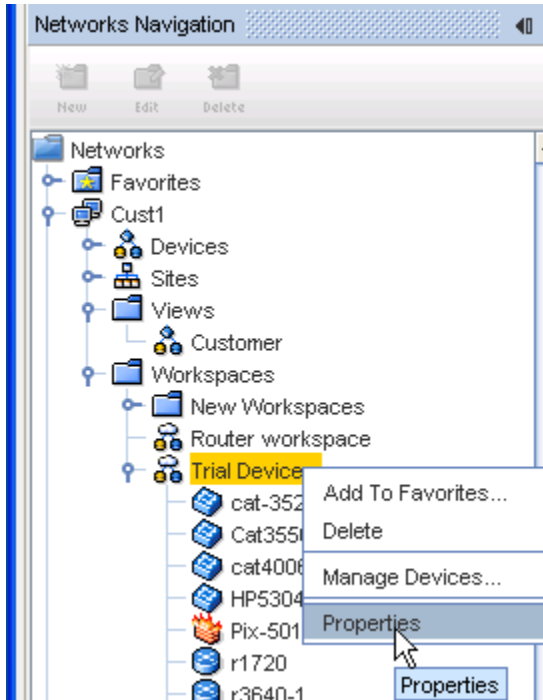
- Selecting the **users and groups** that will have permissions
- Selecting the **permissions** the user and groups will have to the workspace

When a workspace is created, users and groups can be assigned permissions to the workspace. By default, as a user, you cannot edit your own permissions, but you are able to manage the permissions of other users, as well as manage permissions of groups.

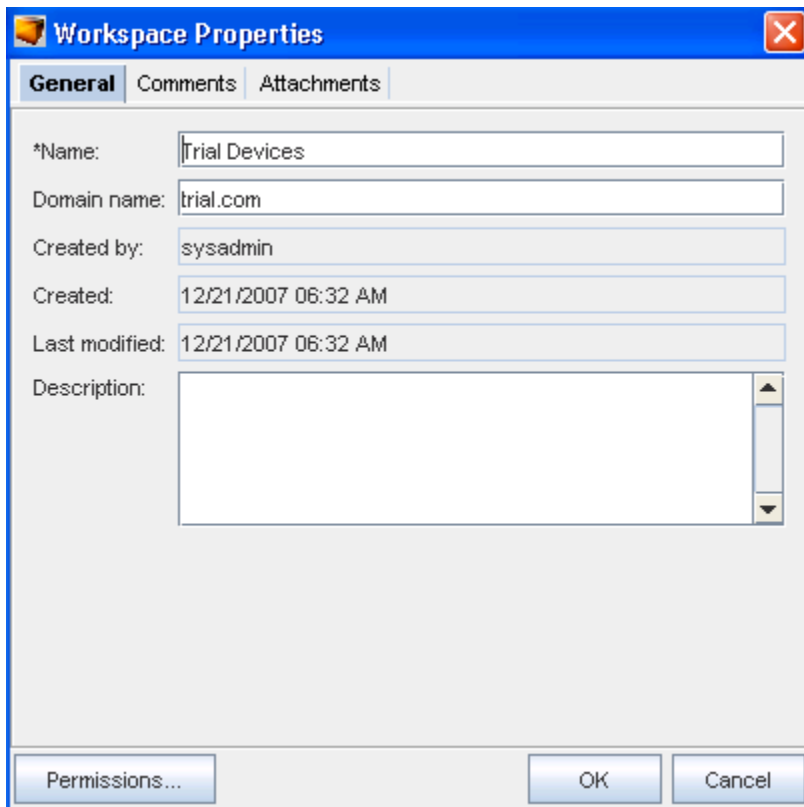
To designate users and groups to have workspace permissions,

- 1 In the navigation pane, open the network where the design workspace is located.
- 2 Expand the **Workspaces** folder, then select the **workspace**.
- 3 Right-click on the **workspace**.

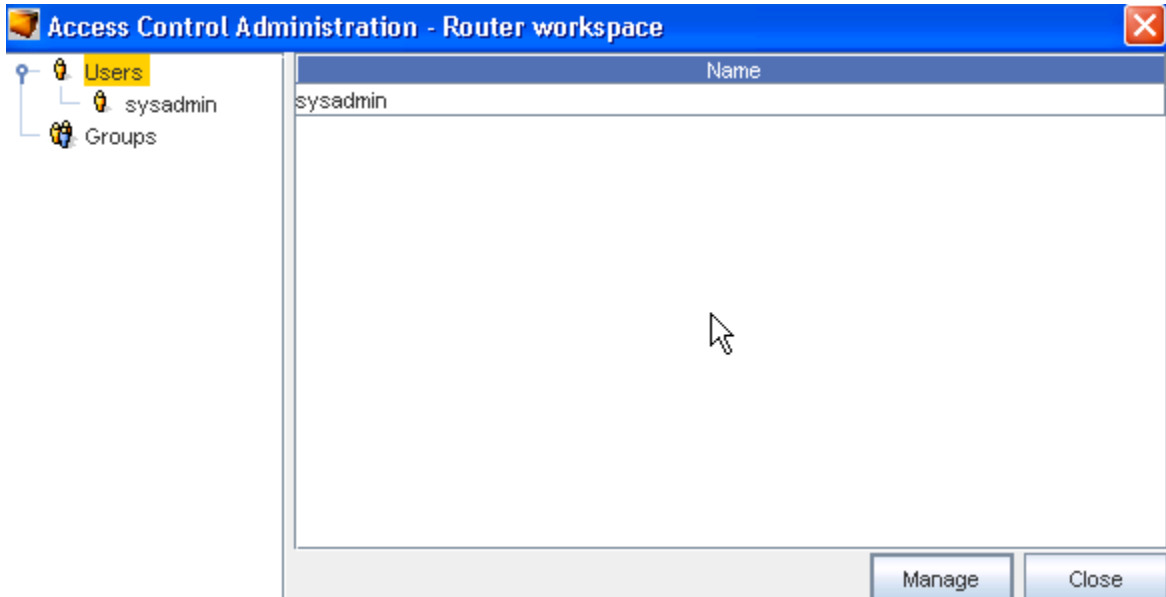




4 Select **Properties**. The Workspace Properties window opens.

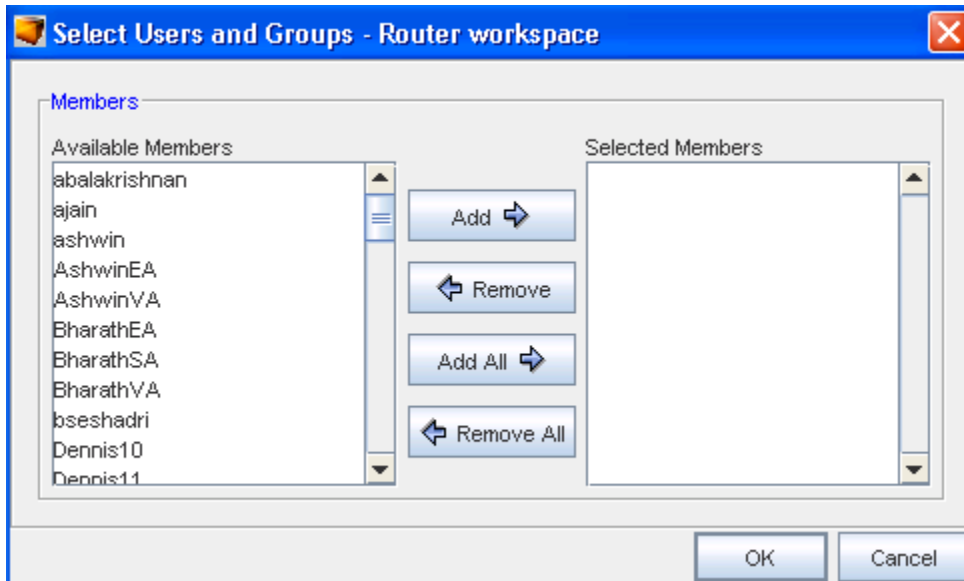


5 Click **Permissions**. The Access Control Administration window opens. There are two groups: Users and Groups



By default, your user name is listed as a User. All other users that have been given permissions are categorized and listed in one of the two groups.

- 6 At the bottom of the window, click **Manage**. The Select Users and Groups window opens.



- Users and groups that do not have permissions are listed in the Available Members column.
- All users and groups with permissions are listed in the Selected Members column.

- 7 To give users or groups permissions to the workspace, in the Available Members column, click the **name of the user or group**.

---

**Note** A string of users/groups can be selected by holding down the Shift key while selecting users/groups. Or, multiple, non-sequential users/groups can be selected by holding the Ctrl key while selecting users/groups.

---

- 8 Click **Add (or Add All)**. The selected users and groups are moved to the Selected Members column, and now have permissions to the workspace.
- 9 To remove a user or a groups permissions, in the Selected Members column, select the name or group. Click **Remove (or Remove All)**. The selected users and groups are moved to the Available Members column, and no longer have permissions to the workspace.

---

**Note** Clicking **Add All** moves all users and groups listed in the Available Members column to the Selected Members column. Clicking **Remove All** moves all users and groups back to the Available Members column. If you perform this action, remember to put your own user name back into the Selected Members column.

---

- 10 Once you have designated the users and groups that are to have access to the workspace, click **OK**. The Select User and Groups window closes.

The Access Control Administration window refreshes, and all users and groups are re-categorized to reflect the changes that were made. You are now able to set the individual permissions to the users and groups.

## Setting Workspace Permissions

---

**Note** You must have **System Administrator** permission to set permissions for others.

---

There are two phases for setting permissions for a workspace:

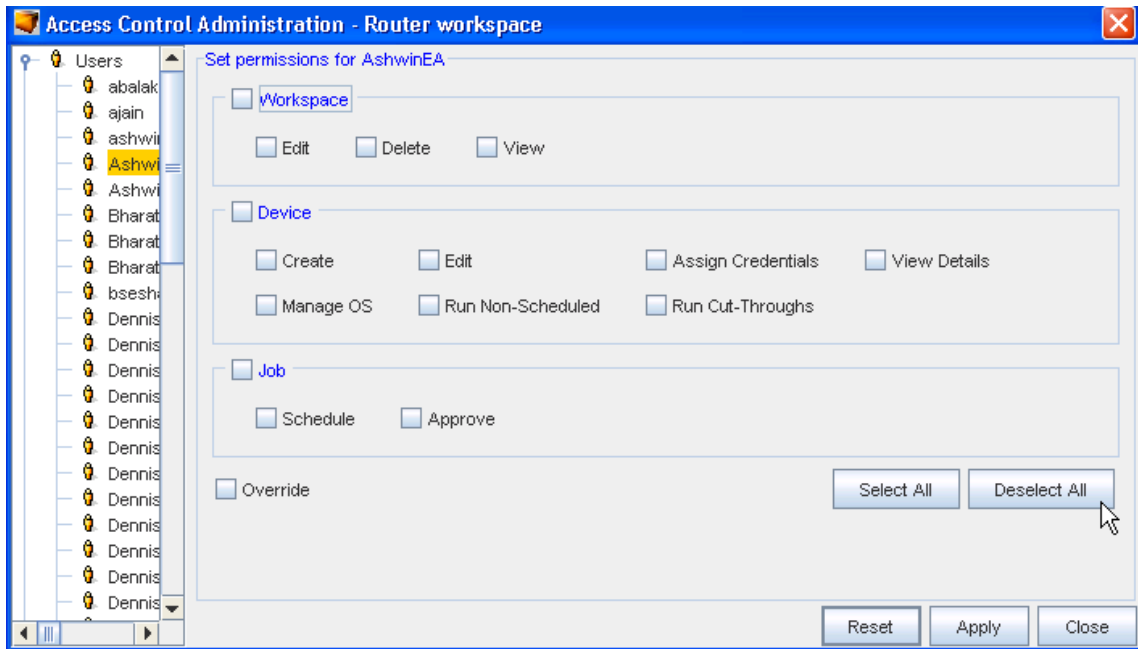
- Selecting the Users and Groups that will have permissions
- Selecting the Permissions that each User and Groups will have to the workspace

Once you have determined the Users and Groups that have permissions to your workspace, you can determine the **set of permissions** the users and groups will have.

Permissions are set through the Access Control Administration window. For more information on using this window and setting the permissions, see [Setting User and Group Permissions](#).

To set permissions for each user and group,

- 1 On the **Access Control Administration** window, expand the navigation tree, and locate the user or group.
- 2 Click the **Users** or **Group**. The Set Permissions for (the individual or group) are shown in the right pane.



Using the check boxes, select any **permissions** for the User or Group within the separate sections.

---

**Important** Use **Select All** to select each permission in each category. Click **Deselect All** to begin again to make permission selections. To return to the original set of permissions, click **Reset**.

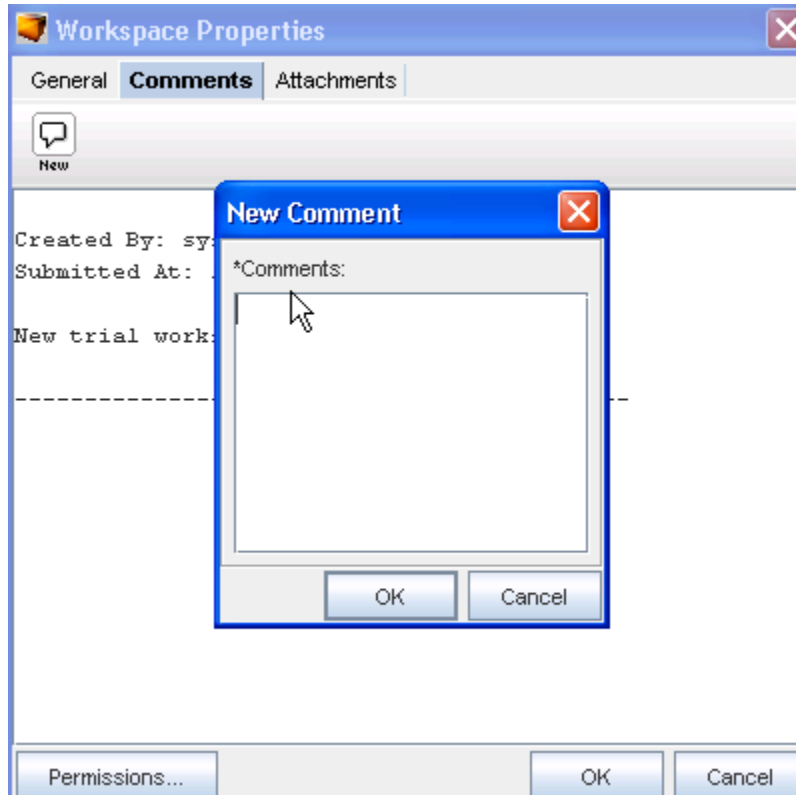
---

- 3 Once you have finished setting the permissions, click **Apply**. The Set Permissions pane closes (and the Access Control Administration window refreshes).
- 4 Now, click **Close** to close the Access Control Administration window. Click **Close** once again, to close the Workspace Properties window.


## The Comments Tab

The **Comments** tab contains a running list of comments, related to the Workspace.

The comments are logged as they are entered. Each comment identifies who created the comment and when. A broken line indicates when the comment has ended.



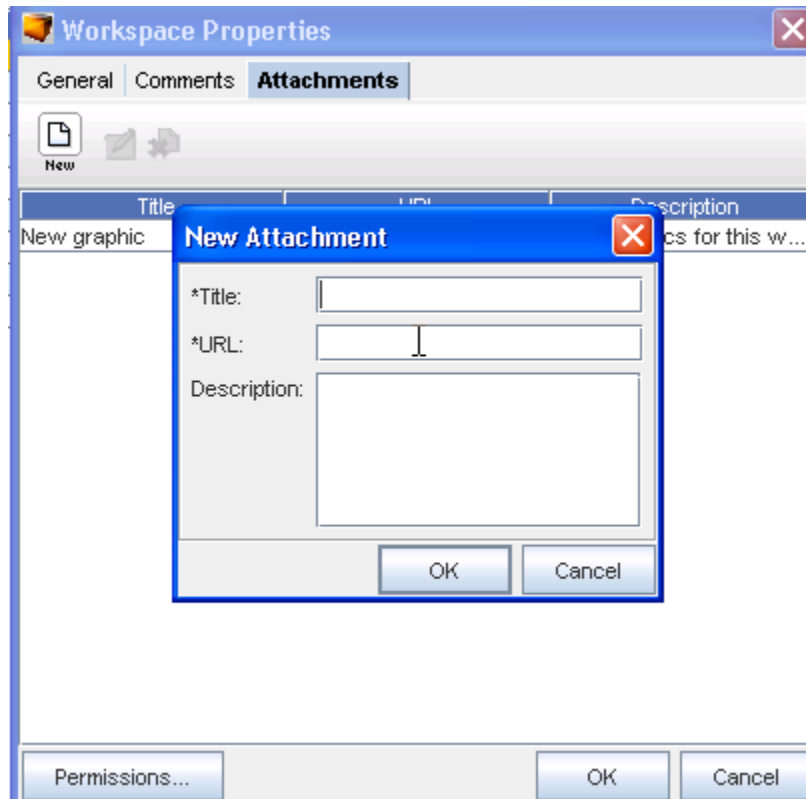
To create a new comment,

- 1 On the Comments tab, click the **New Comment**  icon. The New Comments dialog window opens.
- 2 Enter your **comments**. The Enter key can be used to create paragraph breaks in the comments.
- 3 Click **OK**. The New Comments window closes. Each new comment is added to the top.
- 4 For each new comment, repeat steps 1-3.


Note that you can access the **Permissions** window from here. See [Managing Network Access Permissions](#).

## The Attachments Tab

The **Attachments** tab allows you to associate an external file to the Workspace. This can include worksheets, documents, or .html files. Any document that can be opened in a web browser can be mapped as an attachment. Multiple attachments can be added to each Workspace.



To add an attachment,

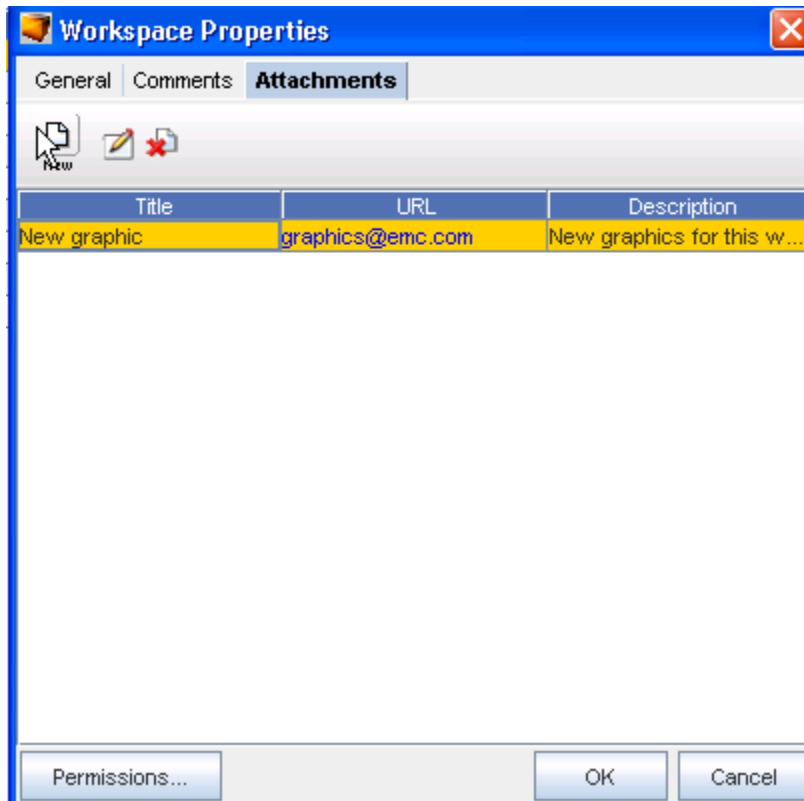
- 1 On the Attachments tab, click the **New**  icon. The New Attachments dialog window opens.
- 2 Enter a title **for the attachment** .
- 3 Enter a **URL**. Remember the document must be saved in a format that will open in a browser.
- 4 If needed, enter a **description**.
- 5 Click **OK**. The New Attachments window closes.
- 6 For each new attachment, repeat **steps 1-5**.

---

**Note** The Edit and Delete icons are only active when one or more attachments have been created.

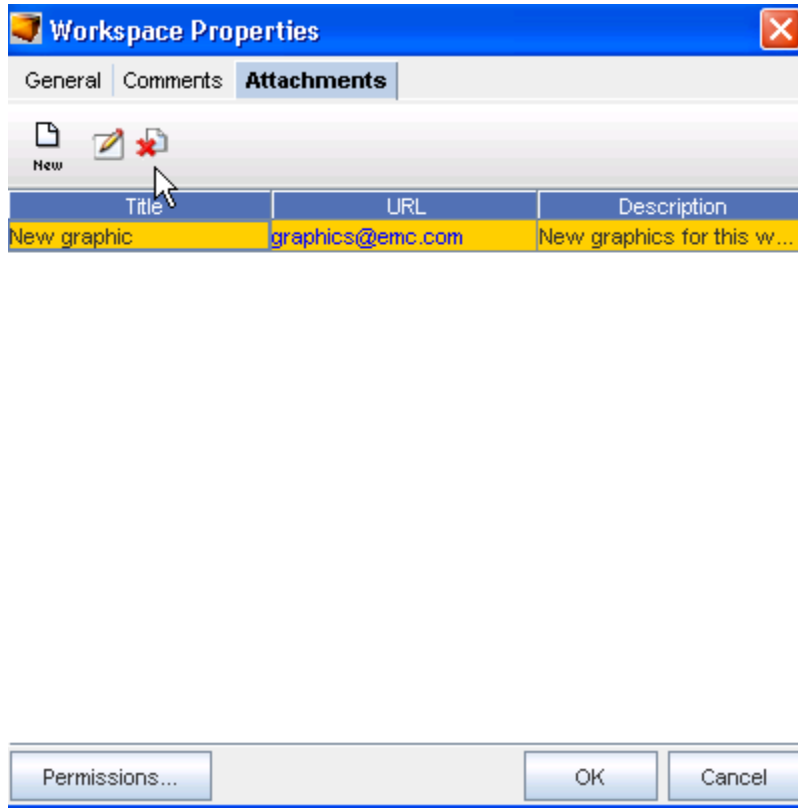
---

To edit an existing attachment,



- 1 On the Attachments tab, select an **attachment**, then click the **Edit icon**. The Edit Attachments dialog window opens. The Title, URL and Description fields can all be edited.
- 2 Make any changes as needed.
- 3 Click **OK**. The Edit Attachments window closes. The attachment row updates with the edited details.

To delete an attachment,



When deleting an attachment, the actual document that you are referring to is not deleted. You are removing its **linked reference** from Network Configuration Manager.

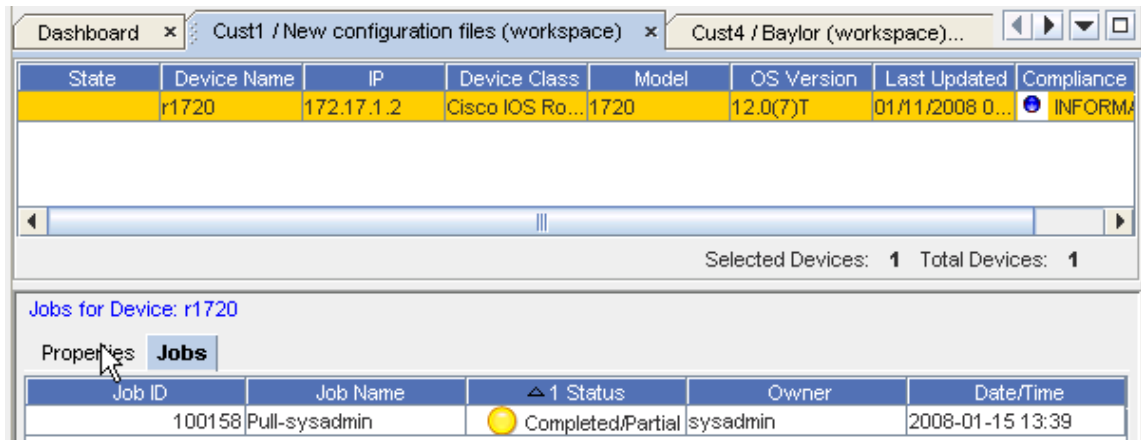
- 1 On the Attachments tab, select an attachments, then click the **Delete** icon. The Confirm dialog window opens asking, "Are you sure?".
- 2 To delete, click **Yes**.
- 3 Click **OK**. The Confirm window closes. The Attachment tab refreshes.

## Workspace Properties - Tabs

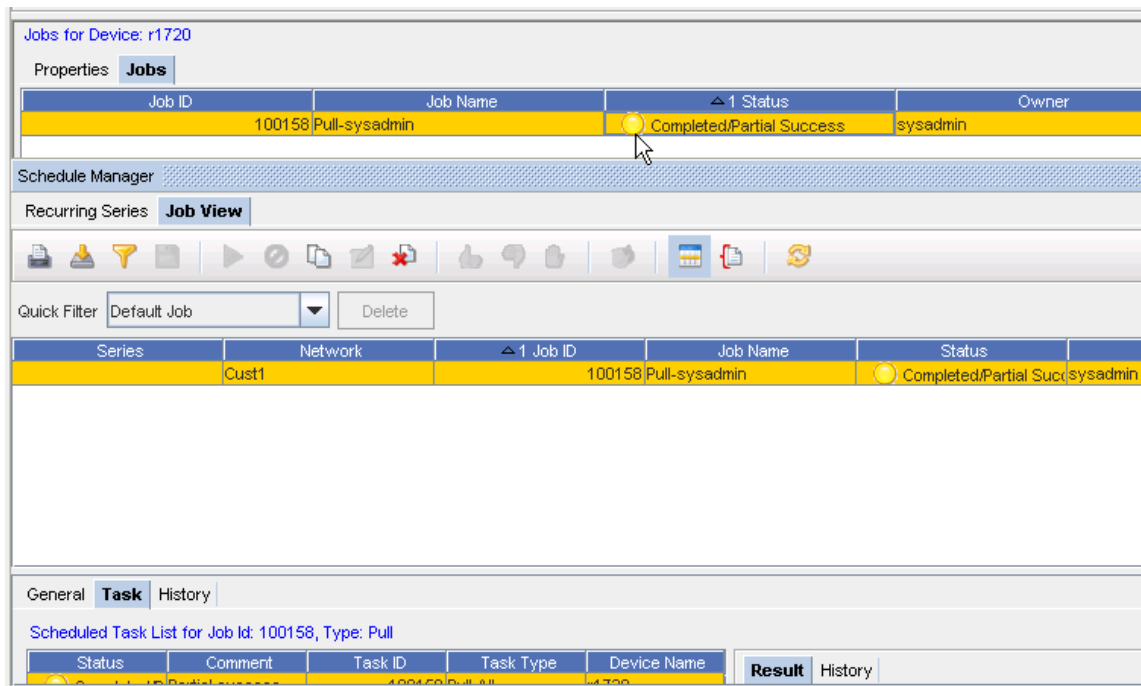
### Properties - Jobs

From within the Workspace, you can see if any Jobs are currently running, or the status of any completed jobs that have previously been scheduled.





When you click a job from this listing, the **Schedule Manager** opens.

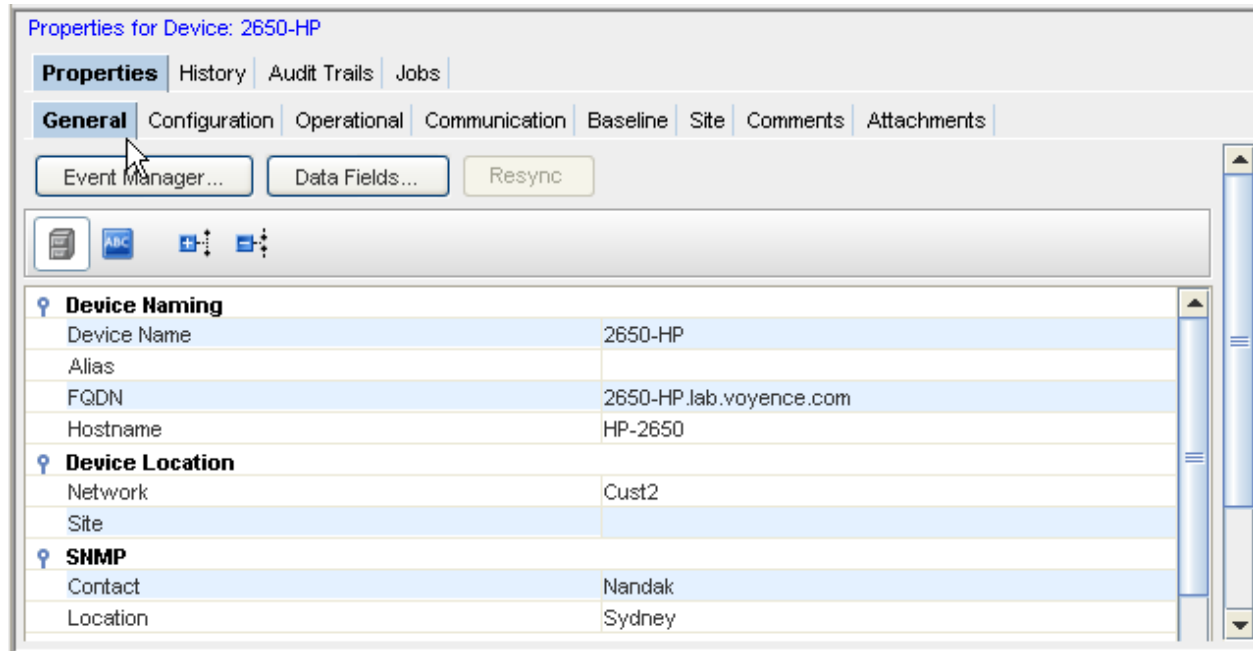


From the Schedule Manager you can view additional job information, including **History**, **Results**, and **Job Summary**.

For more information, go to [Working with Jobs](#)

## General

This tab includes information of a **General** nature.



Including:

- Device Naming
- Device Location
- SNMP
- Device Properties

You can also work with the **Event Manager** , as well as **Data Fields** .

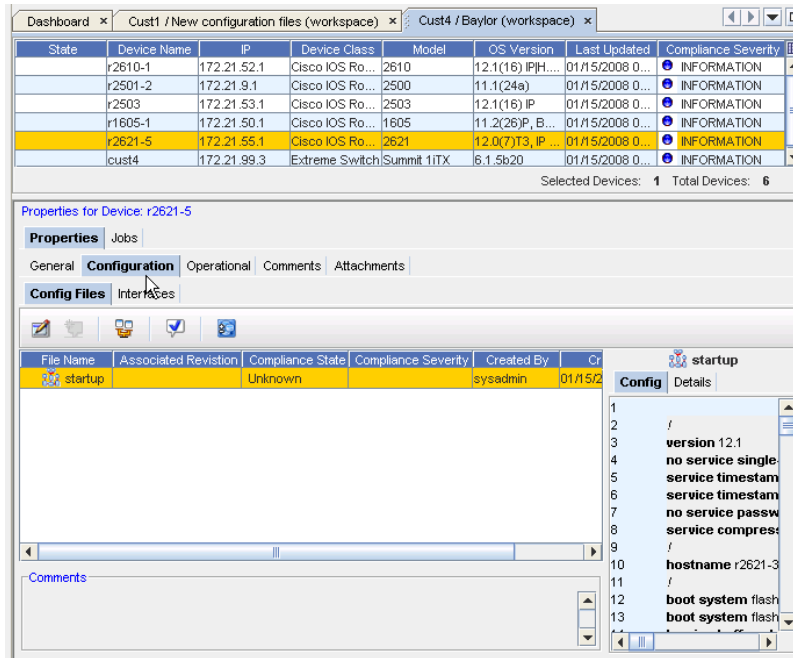
If Devices are out-of-sync, you can use this location to **resync** them back to the correct configuration.

Data Fields






## Configuration

### Config Files

From this tab ( **Config Files**) within the Configuration tab, you can view information on the running configuration. You can also complete tasks.



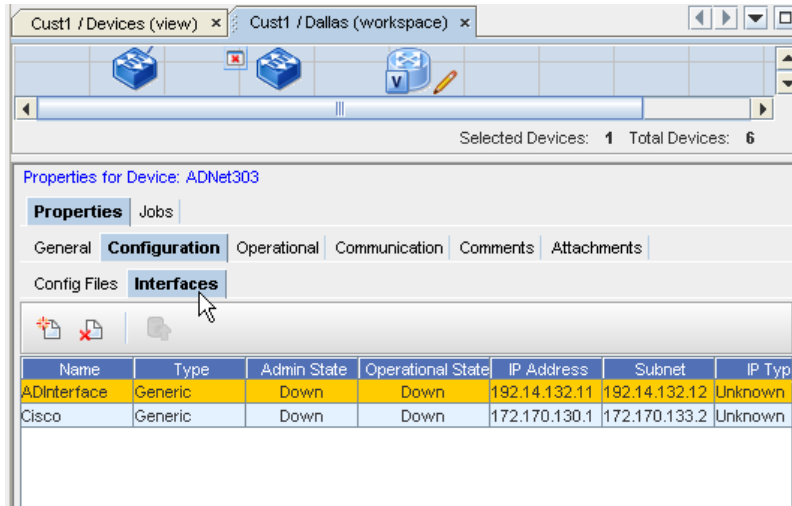
You can review the contents of the running Configuration on the right. You can also click the **Details** tab (on the right) to see the details of the configuration.

- Use the **Config Editor**  icon to access the actual editor to make any changes to the running Config, as well as viewing more information.
- Use the **New Comment**  icon to add additional comments.
- Use the **Compare Configs**  icon to compare any two existing configurations.
- Use the **Audit Config**  icon to complete an Audit on the running configuration.
- use the **Manage Design Device Config File**  to Add or Remove running config files.

## Interface

The **Interfaces** tab provides a listing of all the physical and logical interfaces that are configured on the selected device. The Management interface is the Interface IP used to manage the device in Network Configuration Manager. Management Interfaces can be changed from this tab.

From this tab ( **Interfaces**) within the Configuration tab, you can Add, Delete, or select another Interface to become the Managing Interface.

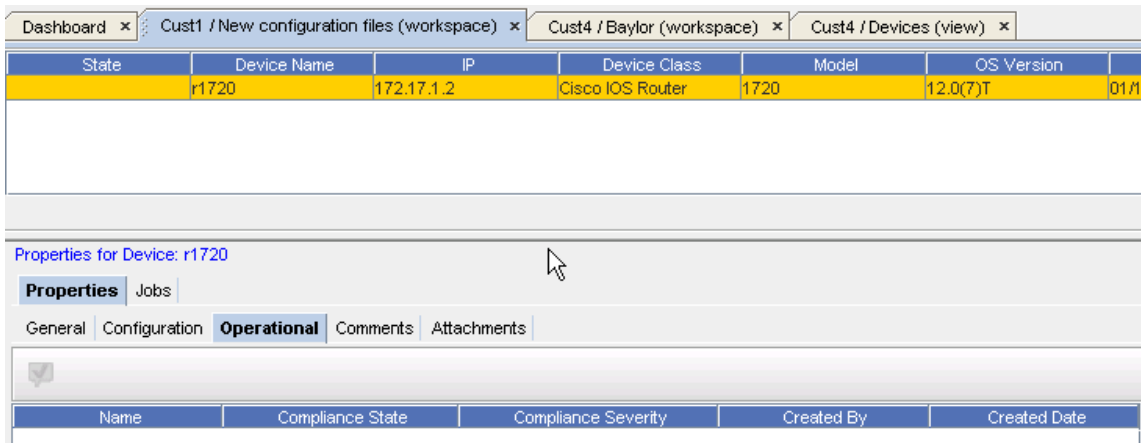


**Note** You **cannot** add or delete an Interface anywhere but within a Workspace.

To manage the Interfaces, see How to [Managing Interfaces](#)

## Operational

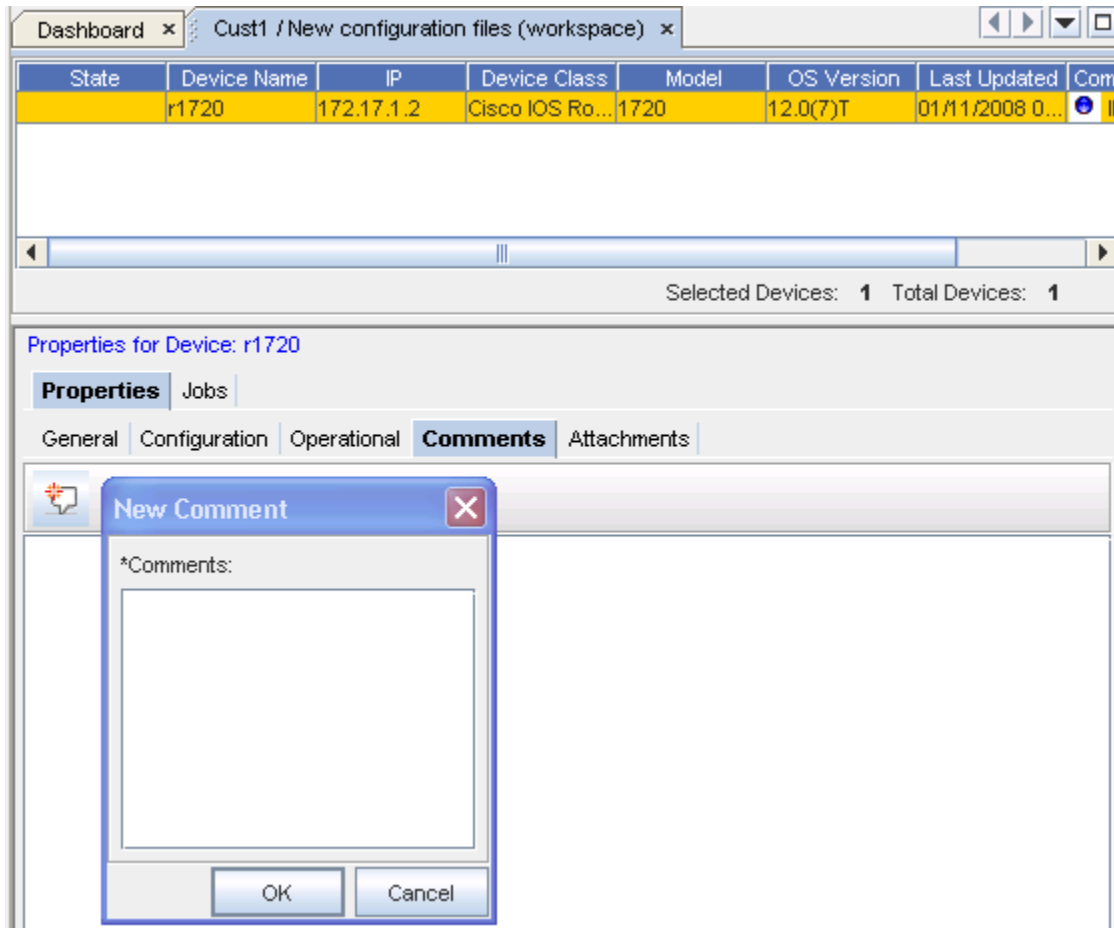
From within the Workspace properties, you can access the **Operational** tab.



For more information on the contents of this tab and the task you can complete ( **Audit Config**), go to [Operational Units Tab Overview](#)


## Comments Tab

The **Comments** tab contains a running list of comments, related to the Workspace.

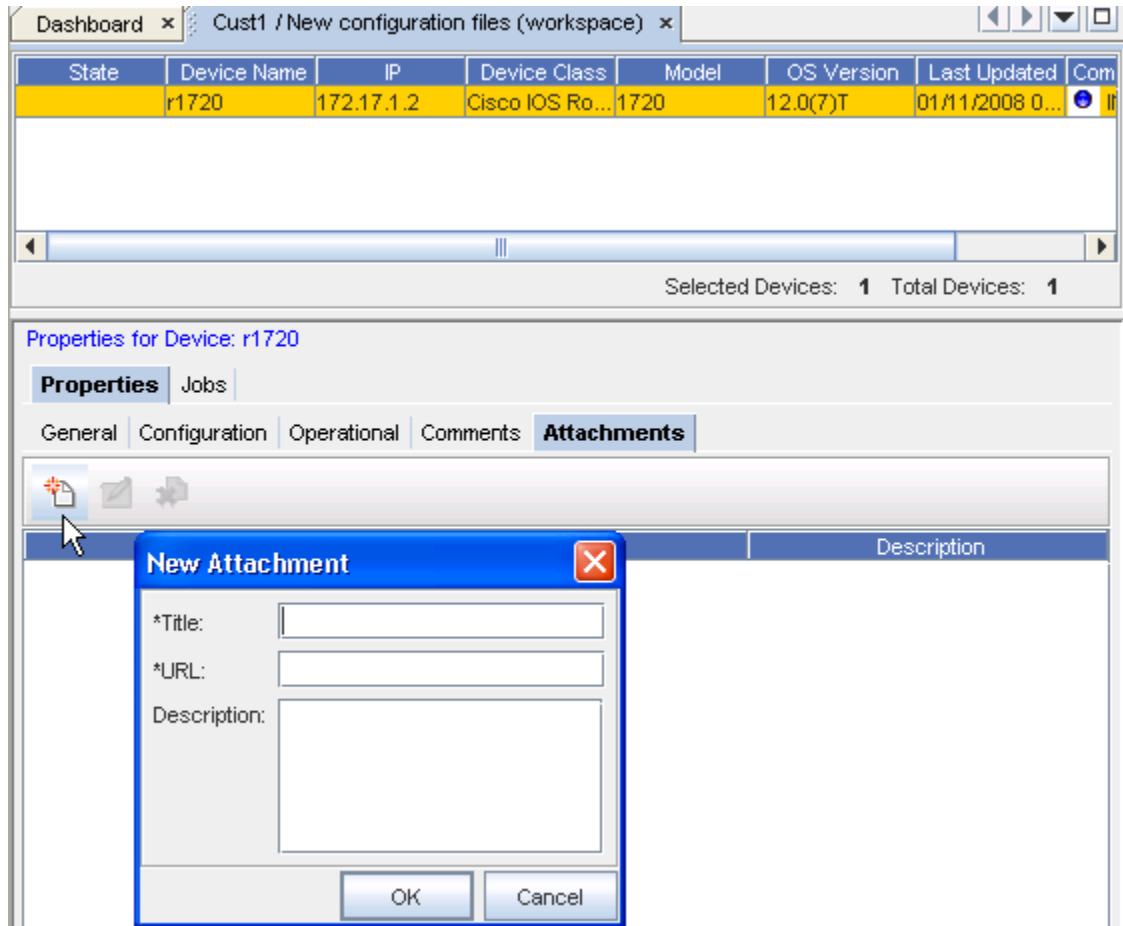


The comments are logged as they are entered. Each comment identifies who created the comment, and when. A broken line indicates the end of each comment.

To create a new comment,

- 1 On the Comments tab, click the  **New Comment icon**. The New Comment dialog window opens.
- 2 Enter your **comments**. The Enter key can be used to create paragraph breaks in the comments.
- 3 Click **OK**. The New Comments window closes. Each new comment is added to the top.
- 4 For each new comment, repeat **steps 1-3**.

## Attachments



To add an attachment,

- 1 On the **Attachments** tab, click the **New** icon. The New Attachments dialog window opens.
- 2 Enter a title **for the attachment** .
- 3 Enter a **URL**. Remember, the document must be saved in a format that will open in a browser.
- 4 If needed, enter a **description**.
- 5 Click **OK**. The New Attachments window closes.
- 6 For each new attachment, repeat **steps 1-5**.
- 7 Click **Close** when you are finished adding attachments.

---

**Note** The Edit and Delete icons are only active when one or more attachments have previously been created.

---

## Multi-Configuration File Support

### Multi-Configuration Overview

Previously, Network Configuration Manager handled only devices with single configuration file states.

With the **multi-config feature** implementation, the system now supports devices with multiple configuration files by revisioning all config files defined in a device package -- for a **device class** .

Multi-Config offers you a known view of any device at any point-in-time!

With **Multi-Configuration**, Network Configuration Manager can ensure:

- Cisco devices can be restored if they have a second configuration file.
- Devices with multiple configurations are supported.
- Firewalls are supported, along with new communication methods.
- Compliance can be enforced on more than one configuration file on a device

Within configuration management, generally devices have 1 -n configuration units.

---

**Note** A configuration unit can be a file or interpreted data. The term configuration unit is used interchangeably with configuration file . A good number of devices resemble "Unix-like" devices.

---

Following are the "families" of devices, based on **multiple configuration units** , that are supported:

- Alcatel
- Checkpoint
- IOS Config
- Juniper
- Cisco Firewall Switch Module
- Cisco VPN Concentrator
- Passport MSS
- Nortel ARN

## Device Package

A device family (or class) is represented by a **device package**. A device package is a collection of driver code and class metadata that is used to manage all devices of that class. Device packages are field deployable.

The Device Package:

- Declares the configuration files that are to be captured from the device
- Declares the potential destinations and operations supported for the files
- Ties every file with a choice of supported destinations and push mechanisms
- Ties every file with a choice of activation methods and post operations. For example, pushToMemory, copyToStart.

- Declares device level operations. For example, reboot.
- Includes defaults that should be used for autonomous operations

## Configuration Unit

A configuration unit is a logical set of information that describes or controls the behavior of a device in the context of a network and its relationship with other devices. A configuration unit may be available as "read-only" data, in which case, it may contribute to the state of a device but it is not available for modification.

### Device States

When all the configuration units (as declared in the device package) are captured without any errors, the device state is **Completed**. Rollback and Restore can be performed from this completed state.

When a certain configuration unit (although declared in the device package) is not captured due to errors or intermediate pulls, the state of the device is **Partial**. You can complete a rollback or a restore from a single configuration unit in the partial state.

On the other hand, configuration units are available for modification that Network Administrators often modify to control the higher level services offered on that network.

## Pull/Push Activities

With **Multi-Config** you have the ability to control the pulls through a configuration , meaning that the pulls are no longer completed automatically by the Device Services.

When you select to pull a configuration you have the option to pull the entire configuration set, or to pull individual files and configurations.

### Pull Configurations Options

You have the following **Pull** options:

- Pull after an Auto Discovery
- Pull after a Push
- Pull after an OS Upgrade
- Pull after a Credentials Update

### What happens during this operation?

- After your pull option is selected, the Application Server sends a Pull Configuration Command to the Device Services indicating if it is a complete pull, or a subset, with relevant parameters such as TARGETS/CONFIG CATEGORIES, etc.
- The Device Services Communications Manager transforms this command into a set of calls into the relevant driver by referencing the META DATA XML, which describes TASK->OPERATION mapping.



- The Driver returns a configuration unit, per driver call.
- The Communications Manager compares each configuration unit with its cached copy, and creates a complete set of changed configuration units and in the new XML interchange format to be sent to the application.
- The Communications Manager sends additional messages, such as NEW\_REVISION, COMMUNICATION\_ATTEMPTED, SYNC\_STATE change etc.

## Push Configuration

When you select a push configuration you also have the option of pushing the entire configuration set, or individual files or configuration units, or even configlets.

### What happens during this operation?

- The Application Server sends a Push configuration command to the Device Services, indicating if it is complete push, or a subset with relevant parameters, such as TARGETS / CONFIG CATEGORIES, etc.
- The Device Services Communications Manager transforms this command into a set of calls into the relevant driver by referencing the META DATA XML, which describes TASK->OPERATION mapping.
- The operation defines the push routine input parameters.
- The driver returns a success or failure, per driver call, into a pushConfig or pushFile.
- The Communications Manager refers to Meta DATA XML to find out its operation set, describing the next steps based on META DATA XML

### Example of META DATA Info:

- Does each push failure result in complete failure?
- Does the push have to be a best effort?
- Does it need to pull the entire config after a successful / failed push?
- The Communications Manager sends additional messages, such as PUSH\_SUCCESS, NEW\_REVISION , COMMUNICATION\_ATTEMPTED, SYNC\_STATE change, etc.

## Supported Operations

Following are the operations (tasks) supported by **Multi-Config**:

- **Pull Configuration** – Pull all configuration files, pull file system information, and pull memory
- **Pull Specs** – Pull hardware, file system information, and pull memory
- **Pull All** – Pull Configuration, and Pull Specs. This should pull the complete device configuration state.
- Pull after Auto Discovery
- Pull after Push

- Pull after OS Upgrade
- Pull after Credential Update

## Additional Pull Configuration Information

- All Pull operations result in a new device configuration state, if the state has actually changed on the device.
- After an Auto Discovery, the application (by default) automatically attempts a "Pull All" configuration, automatically.
- The pull operation uses the appropriate dependency metadata declared against each configuration unit in the device package to pull the appropriate set of configuration units.
- Pulling the configuration units is a best effort. For example, the device services does its best to pull all the configuration units. In cases where an error is encountered when pulling a configuration file, the error is then reported against that configuration file.
- If there is no error, all the configuration units are pulled, or if there were one or more errors encountered when pulling specific configuration units, the resulting device configuration state is marked as **Partial**.
- You can pull a specific configuration unit.

Following are the results for the pull tasks scheduled:

- **Task Success** : If the specified configuration unit is pulled successfully, along with the rest of the files constituting the device state.
- **Task Failure** : If all the specified configuration units are not pulled successfully.
- **Task Partial Success** : If only a subset of the specified configuration units are not pulled successfully.

If the system determines that there are no new changes on the device , the task indicates this with a comment such as, Device State Already Consistent.

While there may be no changes on the device since the last revision update, you can still be given the ability to force a pull from the device, which results in a new revision of the device state or the configuration unit.

The system executes a diagnostic command, which is configurable on the device as part of all pull operations, and returns the diagnostic results as part of the revision update.

## Device Configuration State

### Device Configuration State (and Revisioning)

A Device Configuration State (DCS) is defined by multiple configuration files or domains.

A Device will now have multiple Configuration States, each identified by a state number. Each Configuration State is comprised of one or more revisionable units.

Revisionable Units can be categorized into:

- Config Files
- Hardware
- File System Information
- Storage Information
- Interface information
- Extended Attribute Model information

With multiple configuration unit support, the system revisions every device configuration state. As part of the device configuration state, the following configuration units will be revisioned:

- Configuration Files
- Diagnostic Result
- Interface Information
- Physical Hardware
- Memory Information
- File system Information
- Attributed Information – This may include items such as, ACLs, VLAN, and ARP.

Note that not all configuration units become part of the revisioned state. The device package is used to configure configuration units as "revisionable" or not. If not revisionable, the configuration unit is updated without any historical record. However, the device configuration state represents all the configuration units of the device that have been pulled.

### Device Configuration State Information

Every **Device Configuration State** includes the following attributes, along with the configuration file it is included within.

Attribute	Description of Attribute
Device Configuration State number	Incremented for each revision of the device state. Starts with 1.
Comments	Comments associated with this particular DCS
Job Number	The job number of the push/pull job that may have caused this new DCS
Approver Name	The approver of the job, specified by Job Number
User Name	The user that submitted the job, specified by Job Number
Creation Time	Time the DCS was created
Pull Results	The results of the job, specified by Job Number
Baselines	Baselines that this configuration unit is a part of

Each of the **configuration units** revisioned, includes the following information.

Attribute	Description of Attribute
Revision number	Incremented for each revision of the configuration unit. Starts with 1.
Comments	Comments associated with this particular DCS
Job Number	The job number of the push/pull job that may have caused this new DCS
Approver Name	The approver of the job, specified by Job Number
User Name	The user that submitted the job, specified by Job Number
Creation Time	Time the DCS was created
Baselines	Baselines that this configuration unit is a part of

### Device State

The device state is defined by a collection of configuration units "pulled" from the device at any point in time. The state can be either **Complete** or **Partial**.

In addition to the configuration units, the device state is made up of the following attributes:

- Description
- Host Name
- Contact
- Location
- Management IP Address
- Model
- Device Type (Router, Switch, etc.)
- Chassis Serial Number
- OS Version
- Memory (Non Volatile)
- Name
- Capacity
- Current Usage
- File System Information
- Miscellaneous Key Value Pairs

A device state can be incomplete, depending on the most recent configuration units/files pulled from the device (specific files can be pulled on demand, which can create an incomplete device state).

**Important** Any change in any of the configuration units changes the **device state**, with respect to time.

## Rollback / Restore Device Configuration State

You can rollback or restore the device configuration to a well known device state listed as part of the device state history. That well known state could be a network baseline, or a specific configuration state that is "complete". If the device configuration state is "incomplete", you get a warning that the restore will be not be complete as a result. You can then override and continue.

The rollback to a specific Device Configuration State (DCS) automatically schedules a **push job** against that device, with the task containing the content extracted from the individual configuration units. Note that not all configuration units will be available for rollback due to the category and nature of the configuration unit, with respect to the device.

Once you select to **Roll Back**, the Schedule Push Job work page displays. See [Schedule Push Job](#) for more details.

## Device State History

You can **rollback or restore** the device configuration to a well known device state listed as part of the device state history. That well known state could be a network baseline, or a specific configuration state that is "complete". If the device configuration state is "incomplete", you get a warning that the restore will be not be complete as a result. You can override and continue.

A Device State History may appear as the following (in the Device Properties view).

The screenshot shows the 'History for Device: cust4' window. It has tabs for 'Properties', 'History', 'Audit Trails', and 'Jobs'. Below the tabs is a 'Schedule Manager' section with a 'Recurring Series: Job View' and a toolbar. A 'Quick Filter' dropdown is set to 'Default Job' with a 'Delete' button. Below this is a table of jobs:

Series	Network	Job ID	Job Name	Status	Owner	Date/Time
Cust1		100158	Pull-sysadmin	Completed/Partial	sysadmin	2008-01-15 13:39

Below the job table is a 'General | Task | History' section. The 'History' tab is active, showing a table of job states:

State	Updated By	Time / Date
Completed/Partial Success	system	2008-01-15 13:41
Running	system	2008-01-15 13:39
Approved	sysadmin	2008-01-15 13:39

## Working with Editors

### Editors Overview

Editors in Network Configuration Manager are the means by which device **configurations are altered** , and then **scheduled** into the Network.

## Common Editor Functionality

Each of the four editors within Network Configuration Manager; Config, Configlet, Interface, and Command, have the following common behavior .

- **Cut, Copy, Paste, Preview** - all text editing options
- **Print** - sending the Config/Configlet to a printer
- **Search** - Find and Replace text or unresolved variables
- **Audit** - Check changes for Compliance before they enter the Network
- **Insert Template** - Place a pre-defined configlet into the editor window at the current cursor point
- **Insert Reference Variable** - Place a pre-defined variable into the editor window a the current cursor point. The Reference Variable will be replaced with its value at schedule time
- Save or Schedule Changes
- Schedule a Job

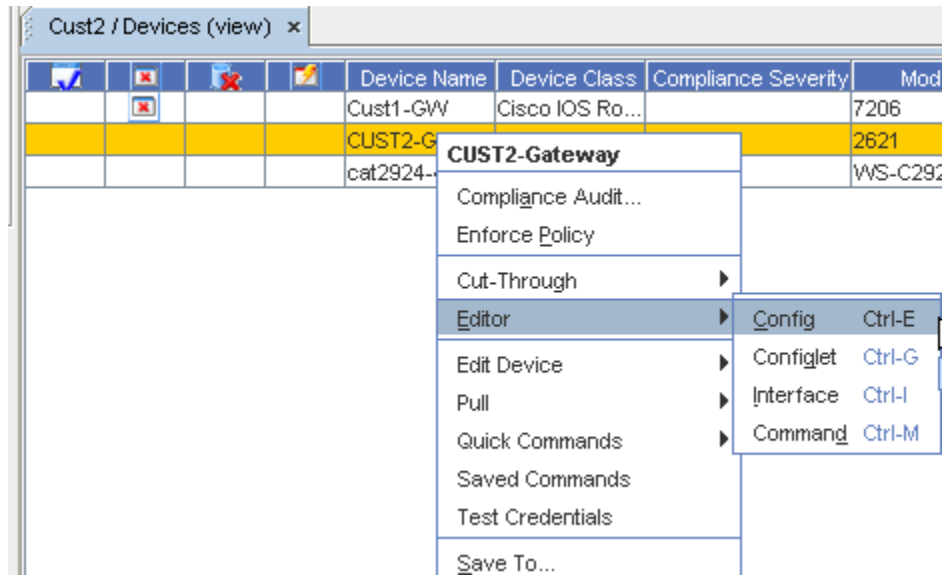
Network Configuration Manager has **four editors** used to construct config files.

<b>Config Editor</b>	Allows the editing of a full device configuration for scheduling to the Network
<b>Configlet Editor</b>	Allows for the creation of a set of commands (configlet) that can be scheduled to be pushed to one or many devices
<b>Command Editor</b>	Is like the Configlet Editor, but is used to construct system commands to report on device status
<b>Interface Editor</b>	Allows for the creation of Interface stanza data that can be applied to either single or multiple interfaces on one or more devices

You can access the editors from the menu bar, (shown in the Devices View in table format)



Or, by right-clicking on any Device within the Devices View, then selecting **Editor**.



Each editor is connected to the Scheduler, allowing you set the date and time, and the sequence of when each job task is to take place.

### Editor and Tasks

The Config Editor,

- Provides an area for contextual editing of the device config file
- Allows the comparison of device's config. Keeps a historical record of revisions
- Opens with a selected device config in the editor, or opens multiple windows for selected devices simultaneously
- Expands or collapses the editor area for addition real estate
- Contains pre-defined locators in the navigation pane
- Uses the Find and Replace feature to quickly locate single or string alphanumeric data

The Configlet Editor,

- Allows you to take pieces of configuration code or templates that are less than a complete config file, but equal to one or more commands
- Allows you to schedule configlets to be pushed to one or more devices in a network
- Allows you to schedule recurring configlet pushes
- Opens with no config (blank) - for making the same change to one or more devices; then scheduled for push at the same time

The Interface Editor,

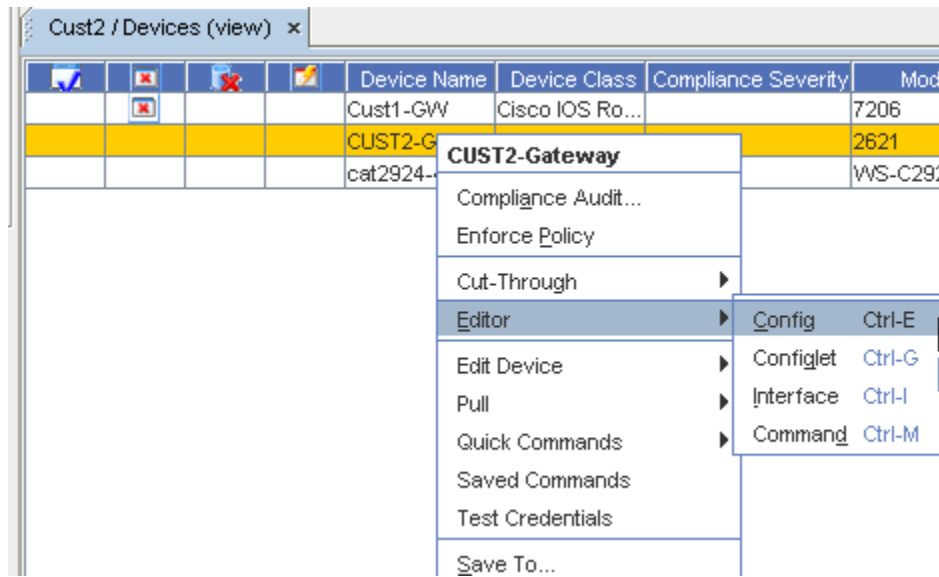
- Allows you to select multiple devices, and send changes to the interfaces of each device
- Allows you to set scheduled interface changes

The Command Editor,

- Provides a verification if a previous configuration change was completed correctly. For example, sending a "show interfaces" command to see that a new interface was successfully added.
- Completes operations on the router for verifying the integrity of the network. This includes pings, tracers, and show routes
- Completes router verification and diagnostics. This includes running internal diagnostics on a router, rebooting a router, and reloading alternate configurations.

## Accessing Editors

When using the right-click menu in the Devices View (either Table or Diagram layout), you can access each Editor from the **Editor** option.



For more information on working with Editors, go to [Editors Overview](#).

## Using Reference Variables

Reference Variables are system variables in Network Configuration Manager that can be used as placeholders for device data in configuration Commands. This includes; device hostname, device management IP, device model, and IP pool allocation addresses. Variables can be inserted in most editor sessions, and in templates, and are replaced with data when scheduling.

Reference Variables allow you to add pre-configured variables to a template. The templates then reside in the Template Library. The Reference Variables can be used in a Config, Configlet and Interface editors.

Reference Variables use pre-defined value names.

---

**Note** These are not user-defined.

---



## Additional Device Reference Variable

A new Device reference variable containing the **IP Address for the Device Server** (managing the Device) has been included in this release. If the Device Server has been assigned a NAT'd IP address, the new device reference variable resolves to that IP address.

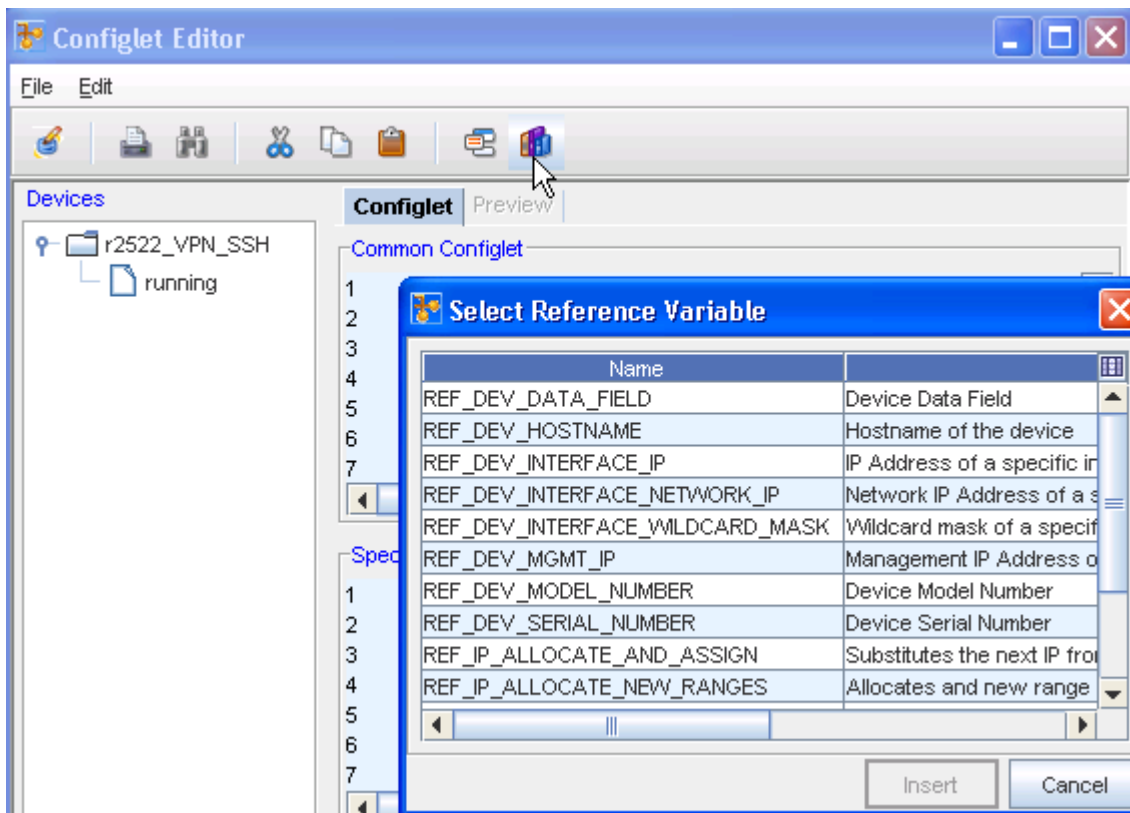
**Note** Virtual devices that have no assigned Device Server do not have a value for the IP Address variable.

When a Reference Variable is used, you must edit the value placeholders that are pre-defined for that variable. Each value substitution is pre-defined, based on the selected value.

In the example below, a reference is inserted into a config file. The steps are the same for a Configlet and Interface editors.

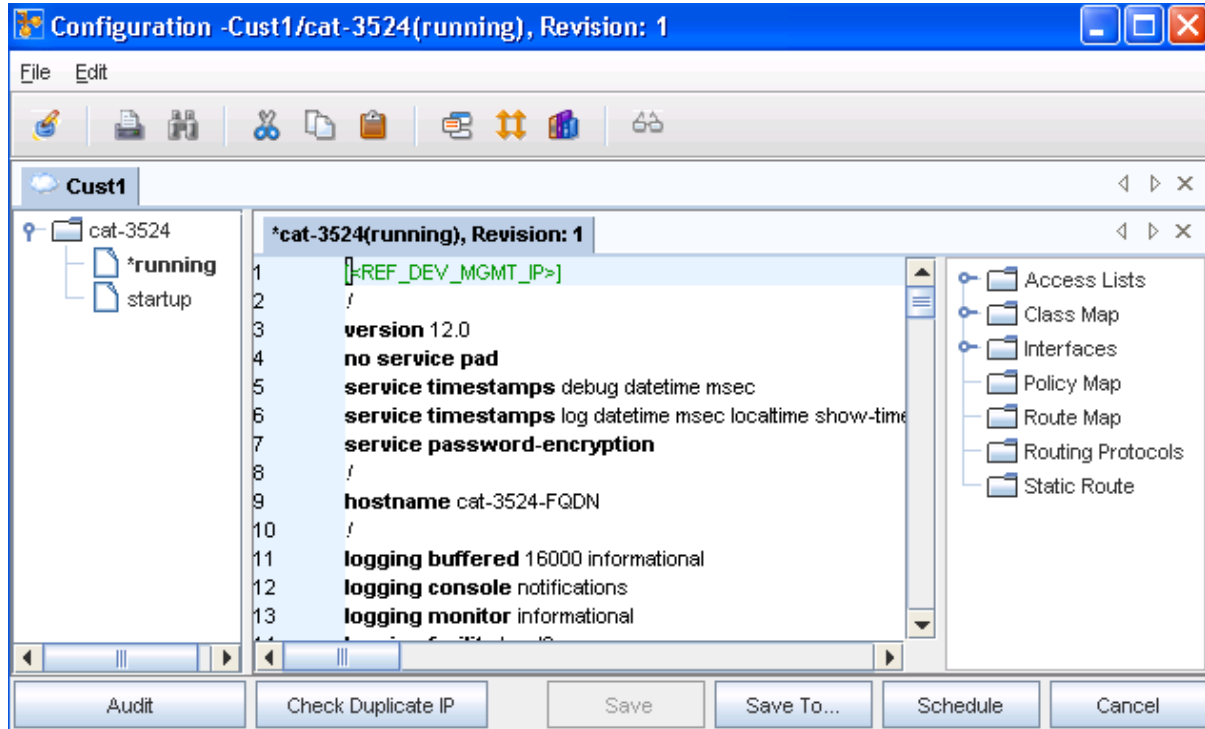
To insert reference variable into a file,

- 1 Select the **devices**, for which the [Creating a Config](#).
- 2 Insert the cursor in the location where the Reference Variable will reside.
- 3 In the toolbar, click the **Reference Variable icon**. The list of available Reference Variables displays.



- 4 Double-click the variable to be used. Depending upon the selected variable, you have two outcomes: Either the Reference Variable is inserted directly into the config, and is edited there, or a **Device Command Parameters** window opens, and the values must be entered prior to insertion into the config.

In the following example, the Reference Variable is inserted **directly** into the config.



- 5 You must now **edit** the variable value.
  - 6 Once all variables values are entered, click **Schedule** to initiate a push to the network.
- Go to [Inserting Reference Variables](#) for more information.

## Additional Reference Variables

### New Reference Variables - Templates and Tests

The following new reference variables have been added to use in templates (as is implemented today), and also in tests.

- Variable to get the value of a network data field
- Variable to get the value of a device data field
- Variable to get the value of a site data field
- Utility Variable/Functions
- Apply a mask to an IP address and return the network number - IPV4GETNET

- Add a number to an IP address and return the IP address - IPV4ADD
- Subtract a number from a IP address and return the IP address - IPV4SUB
- Variable to get device credential related data
- Ability to use nested reference variables - reference variable used as an arguments to other reference variables.

**Example:** IPV4GETNET and IPV4ADD can be nested to get the next Subnet

---

**Note** Workaround for Global Variables - will be default values for the data fields.

---

## Allow Usage of Reference Variables in Compliance Tests

- The reference variables, in addition to its usage in Templates, could now be used in Compliance Tests (attributed and regex)
- Pre-conditions
- Check Patterns
- RHS of the variable definition in Attributed Tests
- Remedies

The UI provides the appropriate convenience to insert relevant reference variables in the above areas. The buffers in these areas would be preprocessed with the available context to resolve the reference variables. Users are warned of unresolved reference variables, as appropriate.

## Template Merge

During template merge, reference variables may not be resolved, depending upon the data available in the context for resolution. Unresolved variables remain in the template, and can still be saved against a design device in a workspace.

## Miscellaneous

Multi-valued variables - The user provides the ability to define a list of values for a single data field, which can then be used in templates to control iterations, based on these variable values.

**For Example:** VarIPs --> [ "192.168.24.1", "192.168.24.2", "172.17.0.163"], VarPorts --> ["8880" , "8881"]

provide the ability to describe a "repetition" in the template, based on multi-valued variables

**Example:**

```
#repeat (permit [<VarIPs>])should generate
permit 192.168.24.1
permit 192.168.24.2
permit 172.17.0.163
```

## Using IP Address Ranges

To allocate IP addresses from designated address pools, use the Insert IP Address, or IP Allocation Reference Variables. When inserting a single IP, you can choose to allocate an available IP from an existing pool, or create a new pool for allocation. There are several insert formats to select from.

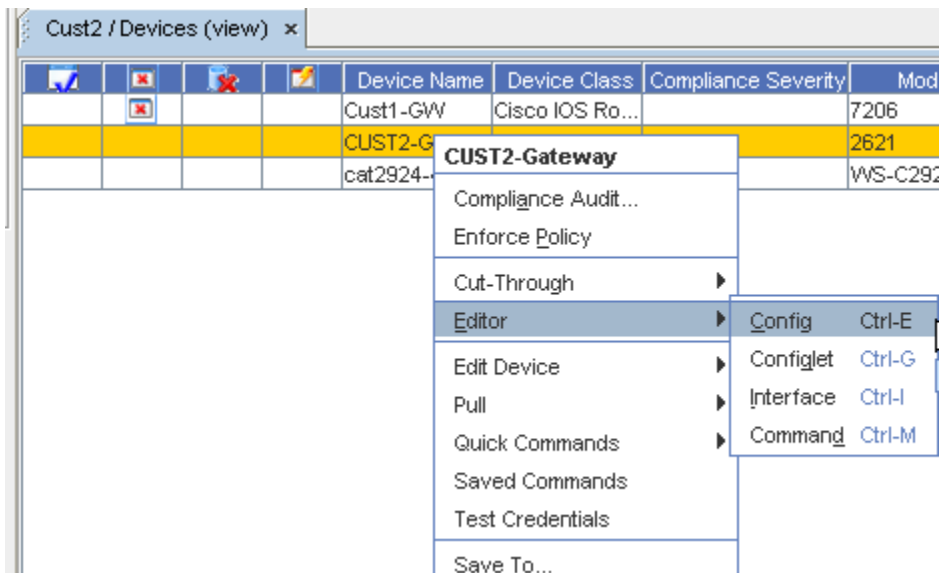
Within the Editors (Config and Configlet) is the ability to use the IP Address pool feature. (Address pools are defined in the System Administration window.)

---

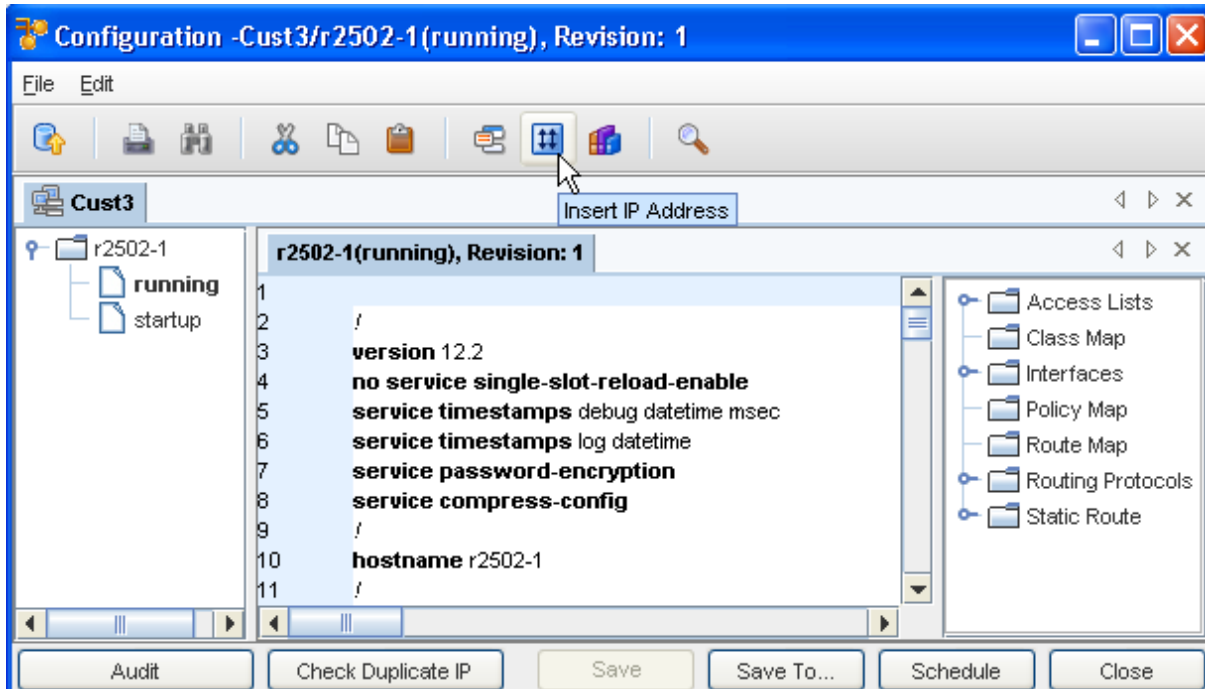
**Important** You must place the cursor at the insertion point where the IP address information is to be located BEFORE opening the Allocate Address window.

---

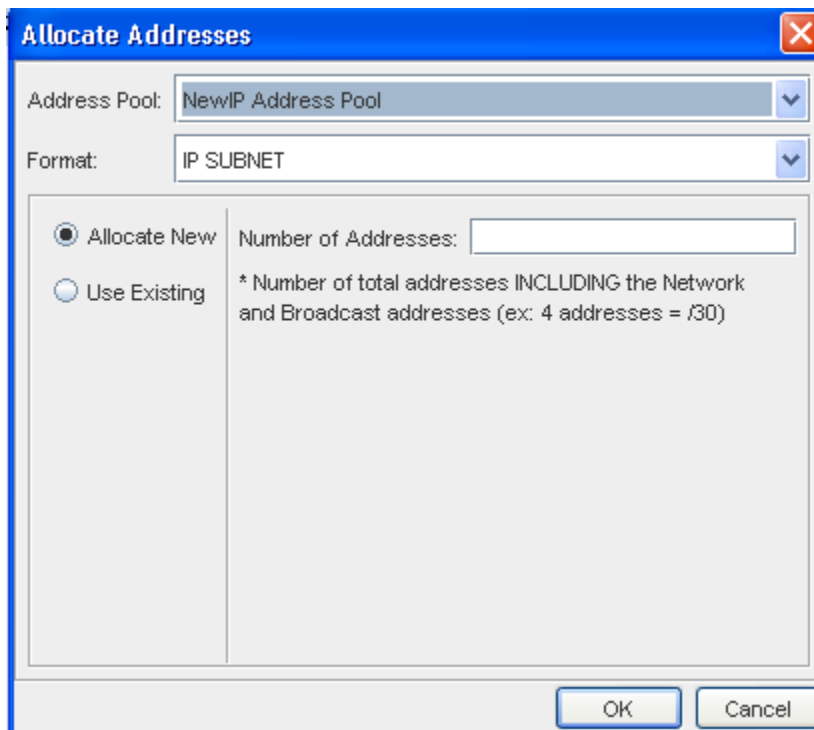
- 1 From the **System Administration** tool, locate the devices.
- 2 Click a **device**, then right-click, and open an **Editor**. The Config Editor opens. If you are creating a Configlet, a blank editor window displays.



- 3 Select the **IP Address** icon.



The following window opens.



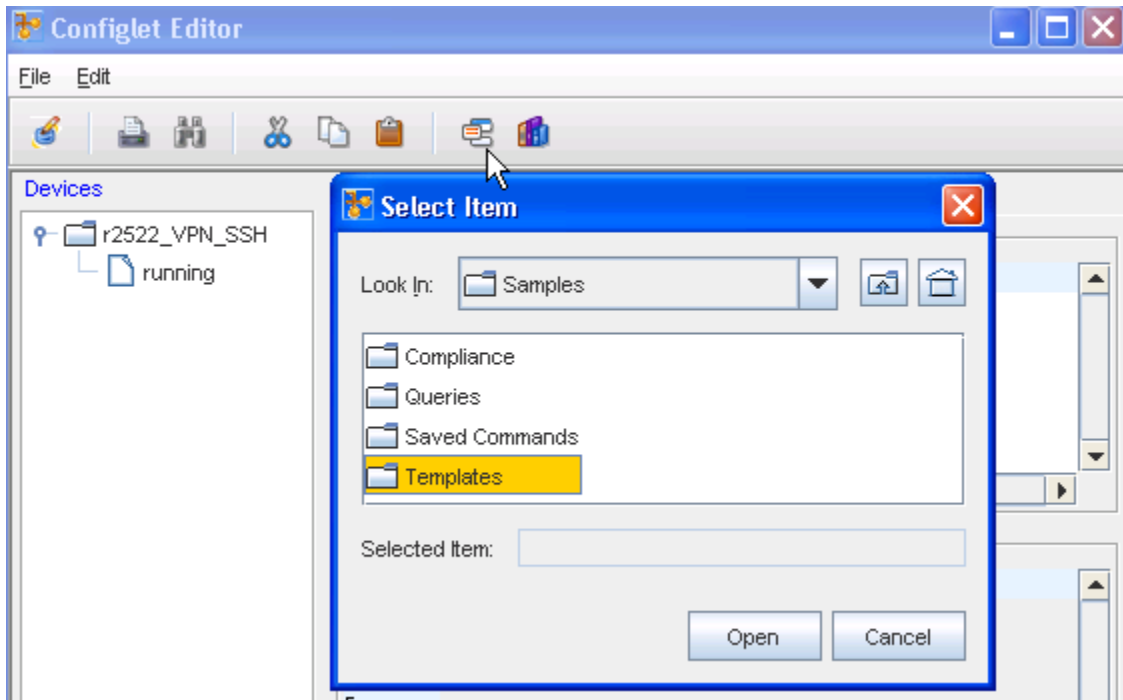
- 4 From the drop-down arrow, select the **Address Pool** to select another Address.
- 5 From the **Format** drop-down arrow, make a selection if you want to change the current Format.
- 6 You can also enter a Number of Addresses if the **Allocate New** radio button is selected, or select the **Use Existing** radio button to use the existing Address.

- 7 Click **Ok**. The Allocate Address window closes, and your selections are now inserted into the file.

## Inserting Template Variables

In place on entering a Configlet, you can select to **Insert an existing Template** .

- 1 In the Configlet Editor window, place the cursor where the template is to be inserted, then click the **Template** icon. The Select Item window opens.



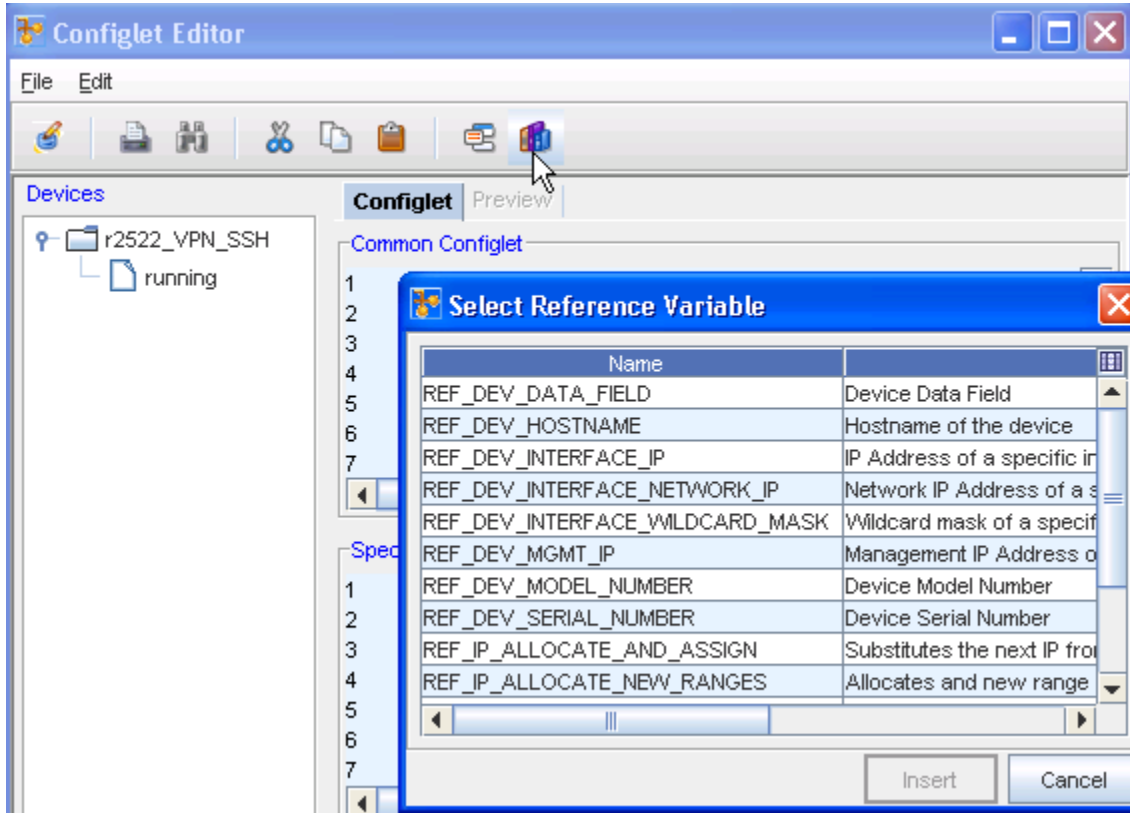
**Note** By default, the Select Item window opens to network specific templates. You also can choose to enter the Library Manager, and select from the available System templates.

- 2 Navigate to the folder location of the template.
- 3 Select the **Template**.
- 4 Click **Select Item** . The Template Variable Substitution window opens. From here you can view the **Variables** and also **Preview** the template you selected. Note that you can select an Integer or a string to add.
- 5 Make your selections, then click **Ok**. The Template Variable Substitution window closes, and the selected template is inserted into the Configlet at the pre-designated cursor location.

## Inserting Reference Variables

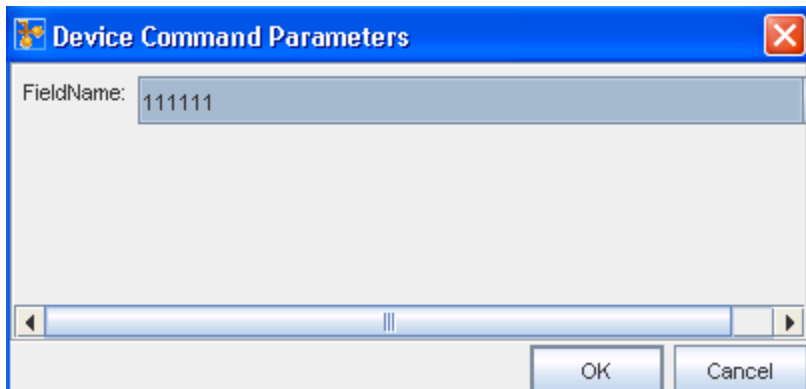
While working with Configlets, you can insert Reference Variables. Variables can be inserted in most editor sessions, and in templates, and are replaced with data when scheduling.

- 1 In the Configlet Editor window, place the cursor where the Reference Variable is to be inserted, then click the **Insert Reference Variables** icon.



The Select Reference Variable window opens.

- 2 Make your selection, then click **Insert**. Depending on your selection from the Select Reference Variable window, the Device Command Parameters window opens.

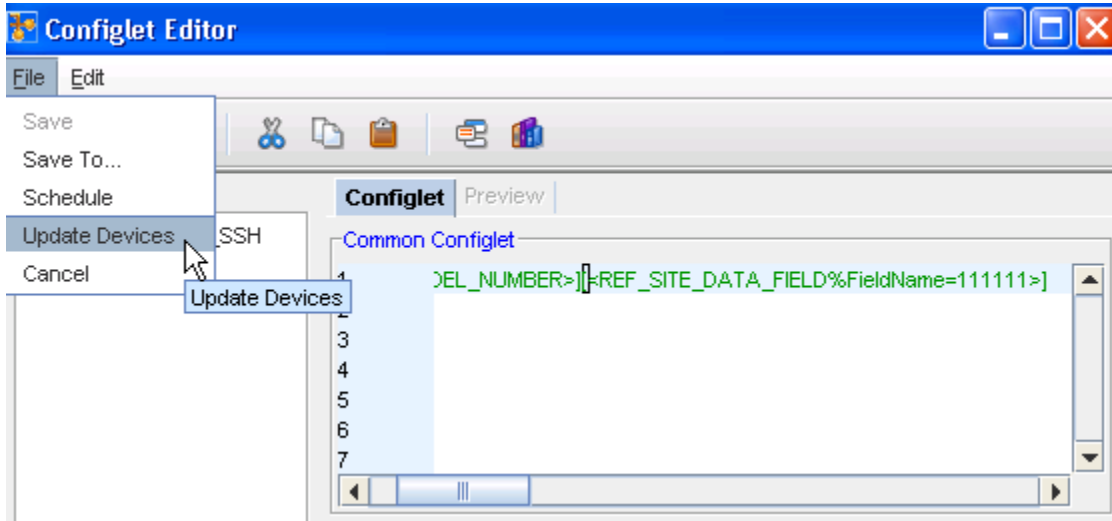


- 3 Enter a **parameter** for the reference variable you previously selected.
- 4 Click **Ok**.

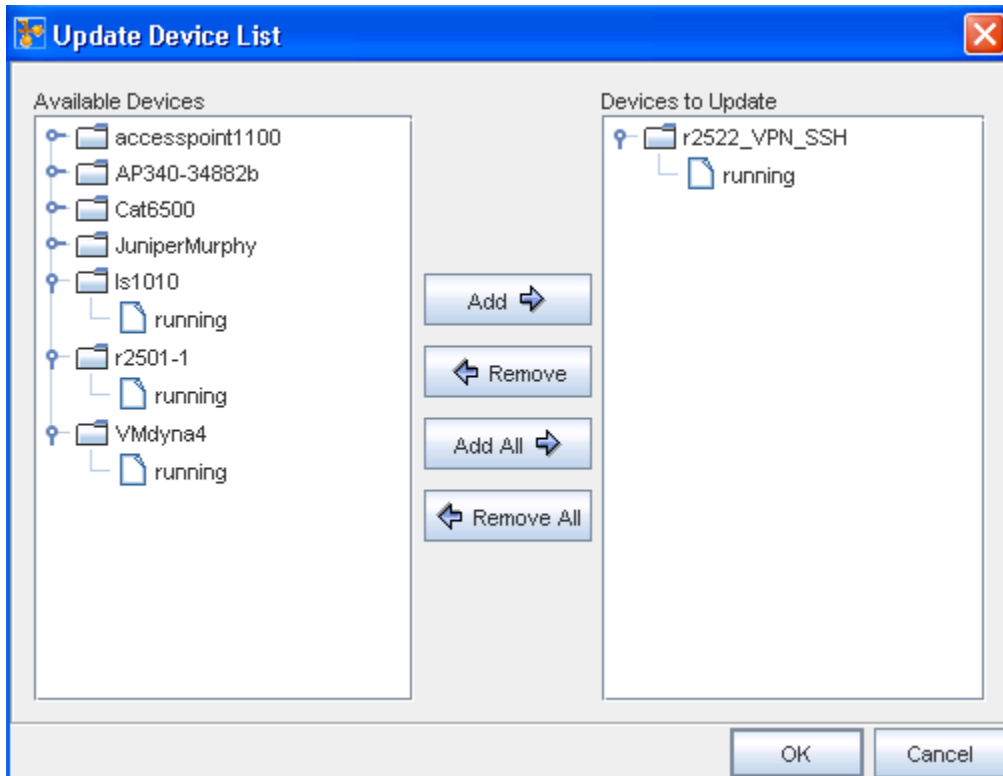
The Reference Variable that you selected and inserted is now in the Edit Configlet portion of the Configlet Editor window.

## Updating Devices

- 1 Within the Editors menu bar, the File option allows you to Update Devices. Select **Update Devices** from the File menu.



Once selected, the Update Device List displays.





- 2 From this window, you can select from the Available Devices, and have them moved into the Devices to Update category. Make your selections then move those selections using the **Add** or **Add All** buttons. If there are existing devices in the Devices to Update pane, you can select **Remove** or **Remove All** to begin to make selections.
- 3 After making your selections, click **Ok**. Your selections are now shown in the Editor window, under Devices.

You can now select [Saving in Editors Scheduling Jobs in Editors](#), and **Cancel** the action.

## Using Find and Replace in Editors

The **Find and Replace** feature allows you to locate and replace information in a Config, Configlet, Command, or Interface Editor file. Find and Replace allows you to:

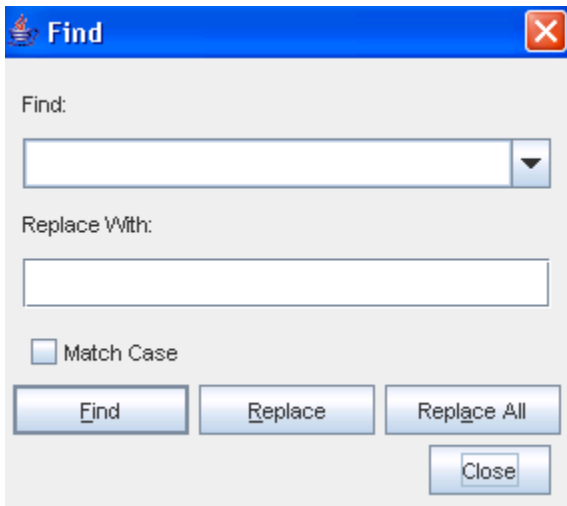
- locate "like text" for review
- locate text to remove or replace within a file
- locate template variables for single or global replacements

To find and replace lines,

- 1 In an open editor window, click the **Search**  icon.



The Find window opens.



- In the Find field, enter a **word or partial words**.

---

**Note** Previously entered words are available by clicking the drop-down arrow to the right of the Find field.

---

- In the **Replace with** field, enter the **full or partial words** that will replace the text in the Find field.
- To match exactly the text in the Find field, check **Match Case**.  
There are three Find options:
- Using one of the above options, **Find and Replace** the word or words as needed.

---

**Note** If your search started in the middle of a window, you are asked: "Restart from the top?". If needed, click **Yes**. The search restarts from the top of the window to locate any matches.

---

- Repeat **steps 2-5** until all changes have been made.
- When finished, click **Close**.

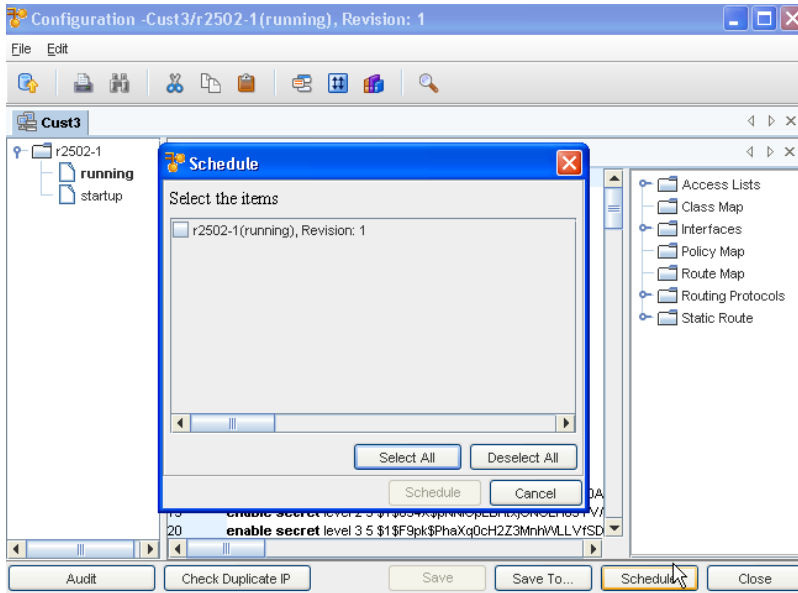
<b>Find</b>	Locates each instance of the words, one at a time. Works in conjunction with the Replace button by allowing you to review the words with the option to leave the words unchanged, or to replace the instance.
<b>Replace</b>	Works in conjunction with the Find button. Once an instance of the words is located, you can complete a single change to the highlighted instance of the words.
<b>Replace All</b>	When <b>Replace All</b> is clicked, all instances of the words are changed to the text in the Replace with field. Unlike the clicking Find, you do not have the option to skip any instances of the matching words.

## Scheduling Jobs in Editors

Once a Config file is edited, it can be **scheduled** to be Pushed to the network immediately, or scheduled to run at another time. Completing this action saves the Config to the device. You can have more than one device listed under the config editor.

To schedule a config,

- From the Config Editor window, click the **Schedule** button located at the bottom of the window.



At the **Schedule** window, you can quickly see which configurations have had changes made to them. Those with changes are now designated with a check mark. Those configs that have not been changed, do not have check marks.

You can:

- Use the **Select All** button to select all configs
- Use the **Deselect All** button to remove the check marks from all checked configs
- Click **Schedule** to schedule those configs that have been checked
- Click **Cancel** to leave this window

2 Click **Schedule**. The Schedule Job window opens.

3 In the **Job Details** portion of the window, enter the following:

- **Job Name** .
- **Job Owner**. The Job Owner should reflect the name of the logged in user.
- **Description** in the field, if needed.
- **Priority** level. Select from Low, Medium, or High priority.

4 In the **Schedule Job** portion:

- At the Schedule job section, by default, all jobs are scheduled to **Run upon approval** . All selections in the following example are displayed as being active in the schedule for viewing purposes only. With adequate permission, you can click the Submit button located at the bottom of the window.
- Note that you can select to have the job **Run in the next maintenance** window.
- If you select the **Run upon operator initiation** option, and Submit for approval, this keeps the job in a pending state after approval. After this, any user, with Schedule permissions, can then execute this job.
- To set a specific time, select **Run at scheduled date/time**. The related date and time fields activate.
- Enter a **Date**. For assistance, use the Calendar icon to open a monthly calendar.
- Select the **time**. The hour, minute, and AM/PM settings must be designated.
- To set a recurring schedule, select **Run as recurring series**. The recurring setting options activate.

- Set the recurring options: Frequency, Start and End Times, and Time Interval.

---

**Important** When the recurring schedule is selected, the new **time zone** drop-down options are available. Make your selection from the drop-down options. The time zone you select must be the **client's time zone** . The new time zone field will be propagated with the client time zone automatically when creating a new Maintenance Window or recurring scheduled job.

---

- 5 After making your schedule selections, click **Submit**.

---

**Note** The appropriate permission levels allow you to both Approve and Submit the job immediately.

---

After selecting Submit, the job is sent to the Schedule Manager. The Schedule Job window closes.

For more details on the components of the scheduling jobs window, and using the scheduling jobs options see [Schedule Manager Overview](#) .

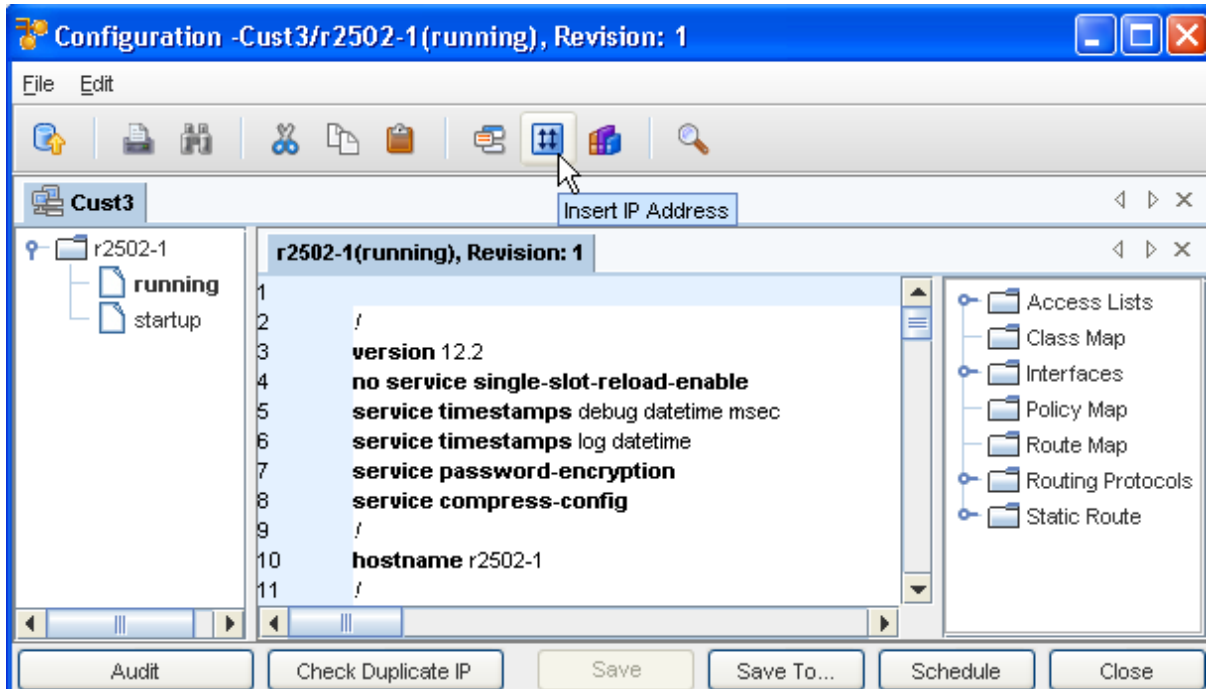
## Saving in Editors

There are three options when saving a Config file:

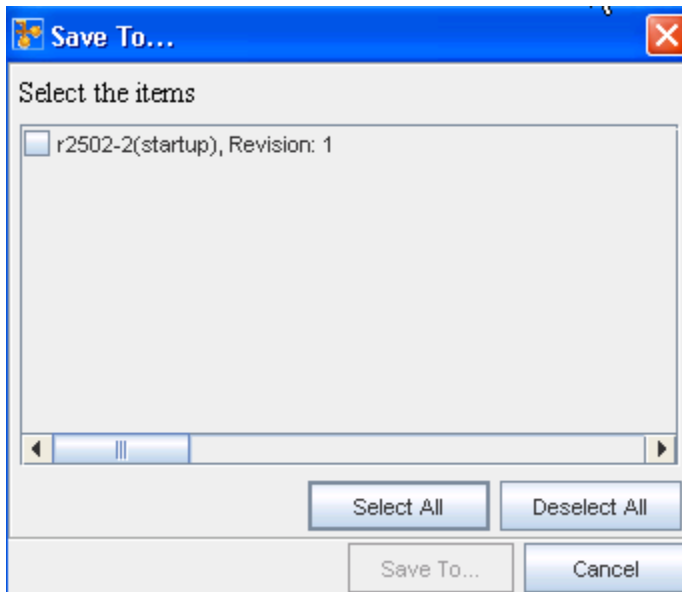
- Schedule the Config for push to the network
- Save the file as a new workspace, save it into an existing workspace
- Save as a .txt file that is located on your local computer or Save a Config as .txt File

To save the config file,

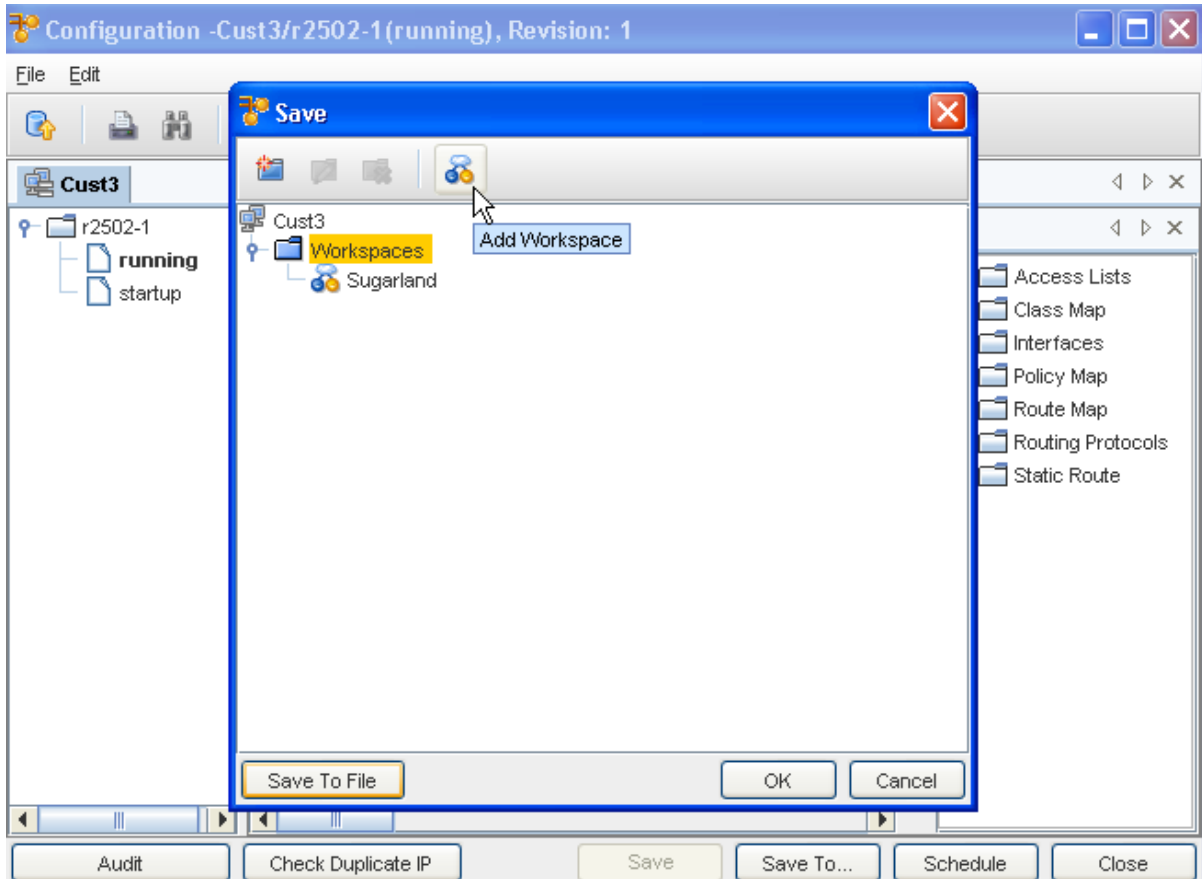
- 1 Once edited, click **File** -> **Save To...** (or click the **Save To...** button located at the bottom of the Config Editor window).



The Save To...window opens.



- 2 From this window, determine which configs you want to save by using the **Select All** or **Deselect All** buttons, then manually selecting which configs to save by clicking within the individual check boxes.
- 3 At the bottom of the window, click **Save To...** Another (additional) **Save** window opens.



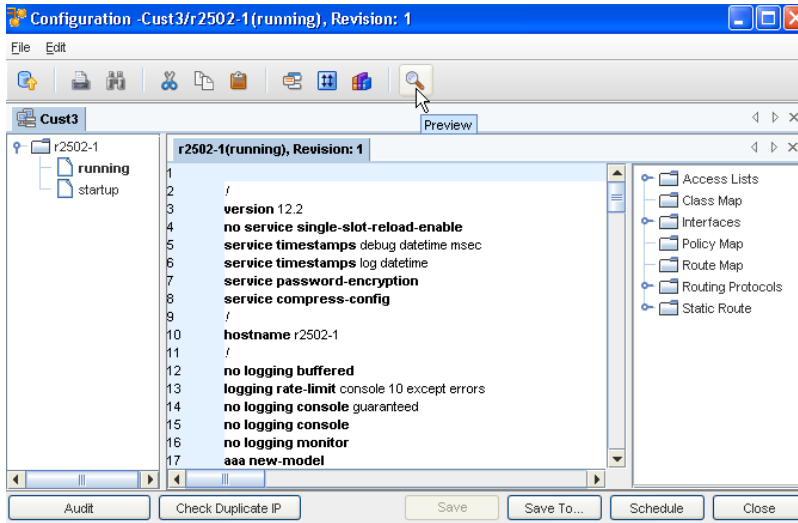
From this window, you can complete the following:

- Create a **new Folder** -using the New icon. By creating a folder, you are able to sort the location of the config. If this is not needed, navigate directly to the folder where the config will be stored.
  - **Edit** an existing Folder name - using the Edit icon
  - **Delete** an existing Folder - using the Delete icon
  - Create a **new Workspace** - using the Workspace icon to **Add a Workspace**
  - **Save To File** - allows you to navigate to your local computer or to a network drive where you can store the file. Configs that are saved as .txt files can be opened using either WordPad<sup>®</sup> or NotePad<sup>®</sup>. WordPad opens with the Config formatted the way it was saved. NotePad opens with concatenated lines of text.
- 4 Click **Ok** when you have made your Save To...selection.
  - 5 When finished, **close** the Config Editor window.

## Previewing Changes in Editors

Once you have made changes (for example, when adding a Reference Variable) you can then preview the changed editor.

- 1 Use the **Preview** icon to review any running configuration.




- 2 Click **Close** when you are finished previewing the configuration.

## The Config Editor

### The Config Editor Window

The Config Editor is designed for editing multiple configurations on a file that affects one or more devices.

The Config editor is accessible:

- When the Config  icon is active, for example, in a workspace's toolbar.
- By right-clicking a device (in the Devices View) and selecting **Editor -> Config** from the menu.
- By double-clicking a single device.


The editor allows you to open one or more instances of the Config editor for multiple devices.

To open one or more config files,

- 1 **Note** If you are using the Table layout to view devices, select **devices** from the table. Or, if you are using the Diagram view, select the **devices**. In a Table layout, a series of devices can be selected by holding down the Shift key while selecting devices. Or, in a Table or Diagram layout, multiple devices can be selected by holding the Ctrl key while selecting devices.

- 2 In either layout, right-click on the **last selected device** . The right-click menu opens.

- 3 Select **Editors**, then **Config**. The Config Editor window opens. Or, once you have selected the

devices, in the menu bar, click the Config  icon.

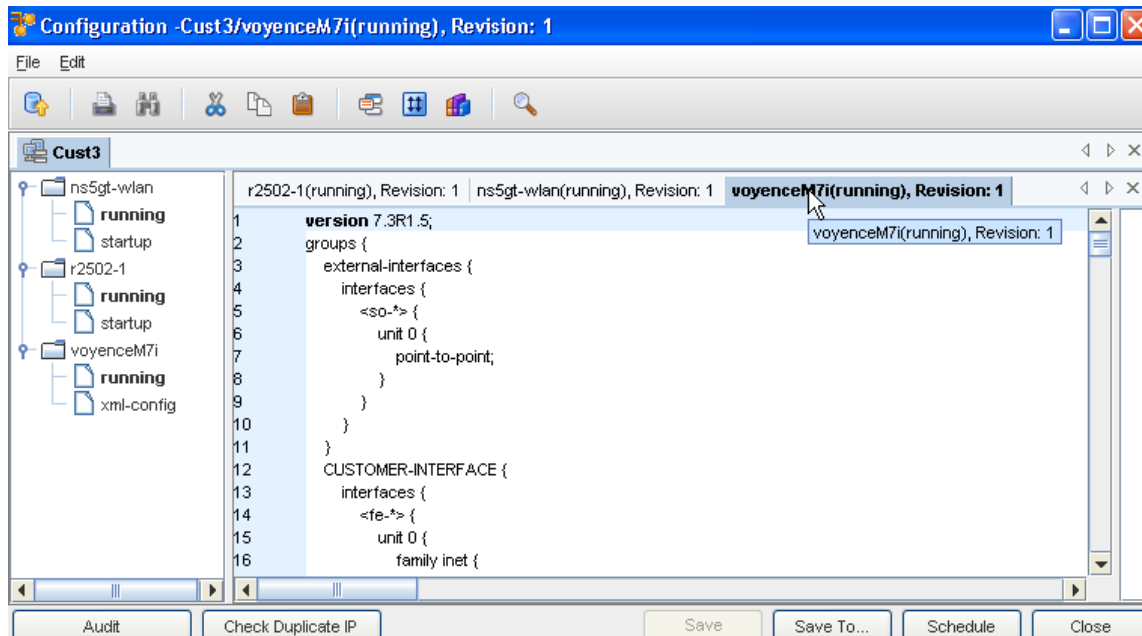


When multiple devices are selected, each device's Config is opened in separate, cascading editor windows. For consistency, text can be Cut, Copied and Pasted between the editors, as needed.

### Additional features in the Config Editor

Along with the new look and feel of the tabbed user interface (see [The Dashboard](#)), you can also use the Config Editor in much the same way. When the Devices View is displayed, you can select a device from the listing to review the configuration for that device. As noted previously, you can select more than one device to review the configurations.

With multiple devices selected, the Config Editor keeps a running "tab" of all the selected devices, allowing you to toggle between the devices to review the configuration details, and to complete tasks on a device. In the following example, several devices were selected from the Devices View list, and are now displayed across the top of the config window panes as tabs. Notice that the Network name ( **Cust3**) is displayed above the listing of tabbed device names.



The tabbed Config Editor view stays accessible until you decide to close the entire editor. While the editor is open, you can also select to close individual devices by right-clicking on the device name, then selecting to close that device. You can also use the right-click options to close all open config views, or to display the device config's in horizontal or vertical views.

While the Config Editor window is active, you can also **select another Network from the dashboard**, select a device (or devices) from that Devices View list, and then click the Config Editor to re-display the Config editor to have both networks, and the devices from each network displayed in the Config editor.

- The active network and device is always **highlighted** in the Config Editor window.
- With more than one Network displayed in a tab format, you can toggle between the Network tabs to work with devices within that Network.

- While the Config Editor view is open, you can complete any tasks on a device by accessing the tabs on the bottom of the window, including Audit, Check Duplicate IP, Save, Schedule, and Cancel.
- The Config Editor runs in the application background until you decide to close it.

The following **components** are available in the Config Editor window.

### Application Menu Bar Options











The menu options are:

File	Provides access to editor tasks
Save or Save To	Allows you to save the Configlet file as a new workspace, or as a .txt file
Schedule	Opens the Schedule Job window for scheduling when the Config is pushed to the network
Update Devices	Opens the Update Devices window, and allows you to update the Device List and display the devices as tabs
Close	Closes the Config Editor window
Edit	Menu options for making changes to the Config file
Undo	Allows you to reverse any action completed in the editor window
Redo	Works with the undo feature, and allows you to "put back" your changes
Cut	Allows you to remove selected text
Copy	Allows you to copy selected text
Paste	Allows you to deposit the copied or cut text into another location
Select All	Allows you to select all the text on a page for copying
Find	Opens the Find and Replace feature
Goto	Allows you to jump to a specific line number

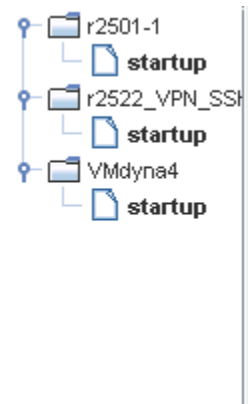


### Toolbars

The icons located on the segmented toolbars reflect actions that can be completed when using the editor.

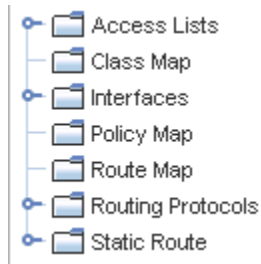
Update Device List	Allows you to select or remove devices from the list
	
Print	Allows you to print the contents of the Config Editor (as shown)
	
Search	Opens the Find window, allowing you to find and replace details in the config
	
Cut	Allows you to select details in the content area and Cut text. Cut text can then be copied elsewhere in the content area, or copied into other editor sessions.
	
Copy	Allows you to Copy any selected details, and Copy them elsewhere in the content area, or Copy into other editor sessions
	
Paste	Used with either the Copy or Cut feature to insert information into the content area of any open editor session
	
Template	Allows you to insert a saved template
	
IP Address	Allows you to select, and then insert Address Pools.
	
Insert Reference Variable	Allows you to select, and then insert a Reference Variable
	
Preview	Allows you to review the current configuration
	

**Navigation Pane - on the left**



- Shows the configurations

## Navigation Pane - on the right



The navigation pane contains the following items. You can expand or collapse each item.

- Access List
- Class Map
- Interfaces
- Policy Map
- Route Map
- Routing Protocols
- Static Route

## Editor Content Area

Contains the content of the Config that is being pushed to the devices listed in the navigation pane.

<b>Buttons</b>	Provides access to editor tasks
<b>Audit</b>	Opens the Select item window where you can select items
Check Duplicate IP	Allows you to check if a Duplicate IP is in existence.
<b>Save To</b>	Allows you to save the Config file and the related device to a new workspace, or as a .txt file
<b>Schedule</b>	Opens the Schedule Job window for scheduling when the Config is pushed to the network
<b>Cancel</b>	Cancels any changes made to the Config(s), and then closes the Config Editor window

## Creating a Config

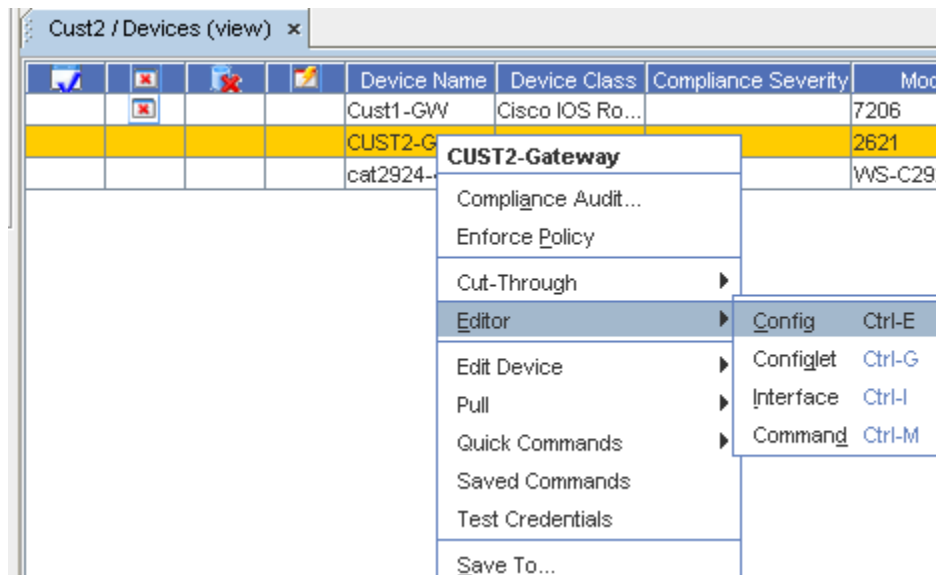
The Config Editor is designed for editing a single, full configuration file that affects one or more devices.

- The Config editor is accessible when the Config icon is active, for example, in a workspace's toolbar by right-clicking a device, and selecting **Editor** -> **Config** from the menu.
- It is also available by double-clicking a single device.

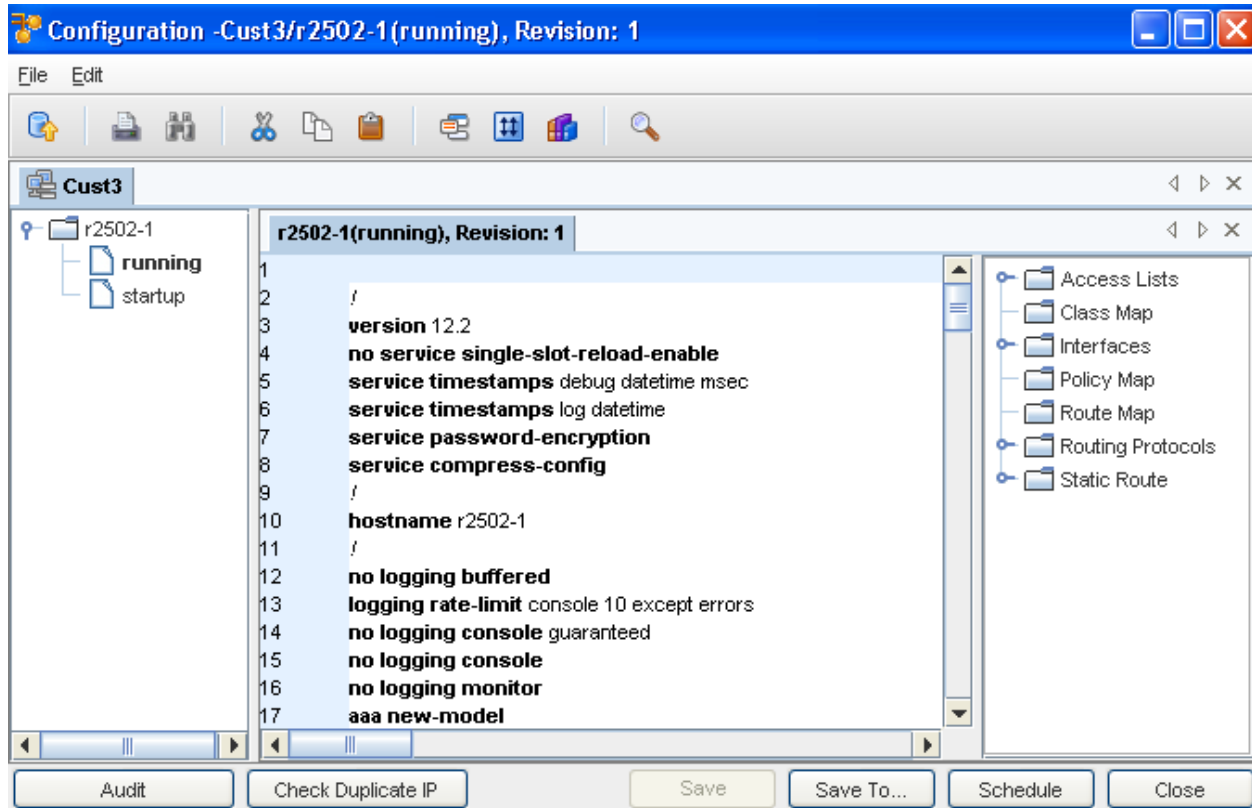
This editor allows you to open one or more instances of the config editor for multiple devices.

To open one or more config files, use one of these methods:

- If you are using the Table layout to view devices, select devices from the table.
  - If you are using the Diagram view, select the devices. In a Table layout, a series of devices can be selected by holding down the Shift key while selecting devices.
  - In a Table or Diagram layout, select multiple devices can be selected by holding the Ctrl key while selecting devices.
- 1 In either layout, right-click on the **last selected device** . The right-click menu opens.
  - 2 Select **Editors**, then **Config**. The Config Editor window opens. Or, once you have selected the devices, in the menu bar click the **Config** icon.



When multiple devices are selected, each device's Config is opened in a tabbed format, allowing you to toggle between configs. For consistency, text can be Cut, Copied, and Pasted between the editors as needed.



## Editing a Config

Once a device Config file is opened in the editor window, it can be edited manually, or by using templates. When editing manually, locate the insertion point for the new information, and enter the text directly into the Config file.

- When using templates, global and network specific templates can be inserted.
- When templates are used, remember to click the insertion point where the template should go. Failing to do so inserts the template text wherever the cursor is within the Config file. By default, when the editor window opens, the cursor is located on line 1.

The navigation pane of the editor window contains the pre-defined locators that auto-parse the content of the Config window. These locators are:

- Access Lists
- Interfaces
- Routing Protocols

To use the pre-defined locators,

---

**Note** The Interfaces locator is used in the following example, but the instructions work for Routing Protocols and Access Lists.

---

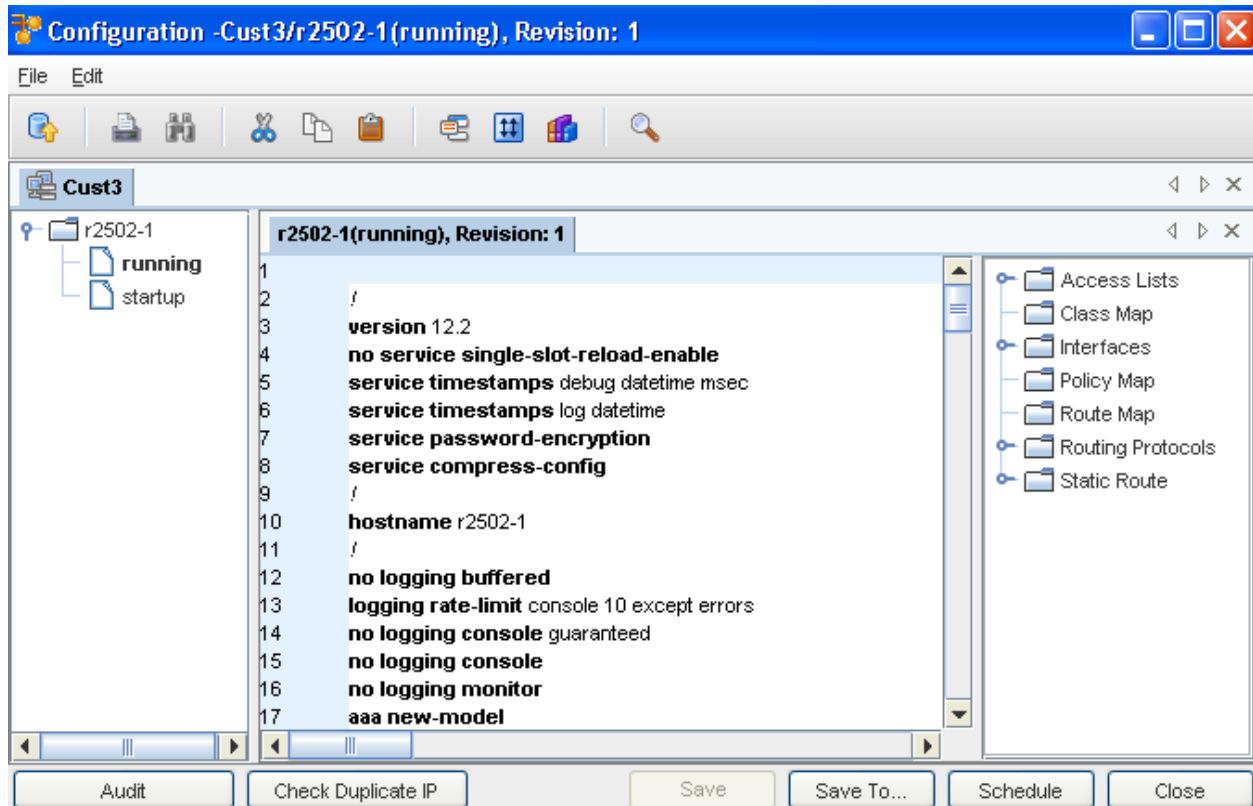
- 1 In the navigation pane, expand the **Interfaces** branch.

2 Click once on any item. In the content area. The clicked item is located and then highlighted. As the Config file is edited, the appropriate locators sections refresh to include the new details.

To edit a config file,

1 [The Config Editor Window](#)

2 In the content area, manually enter **changes** to the file.



Once changes are completed, you have the following options:

- **Audit** the configuration
- Check to see if there is an existing, **Duplicate IP**
- **Save** the file as a new workspace, or into an existing workspace
- **Save To...** as a .txt file that is located on your local computer or network
- **Save** the Config, then **Schedule** it for Push to the network
- **Close** the editor

## The Configlet Editor

### The Configlet Editor Window

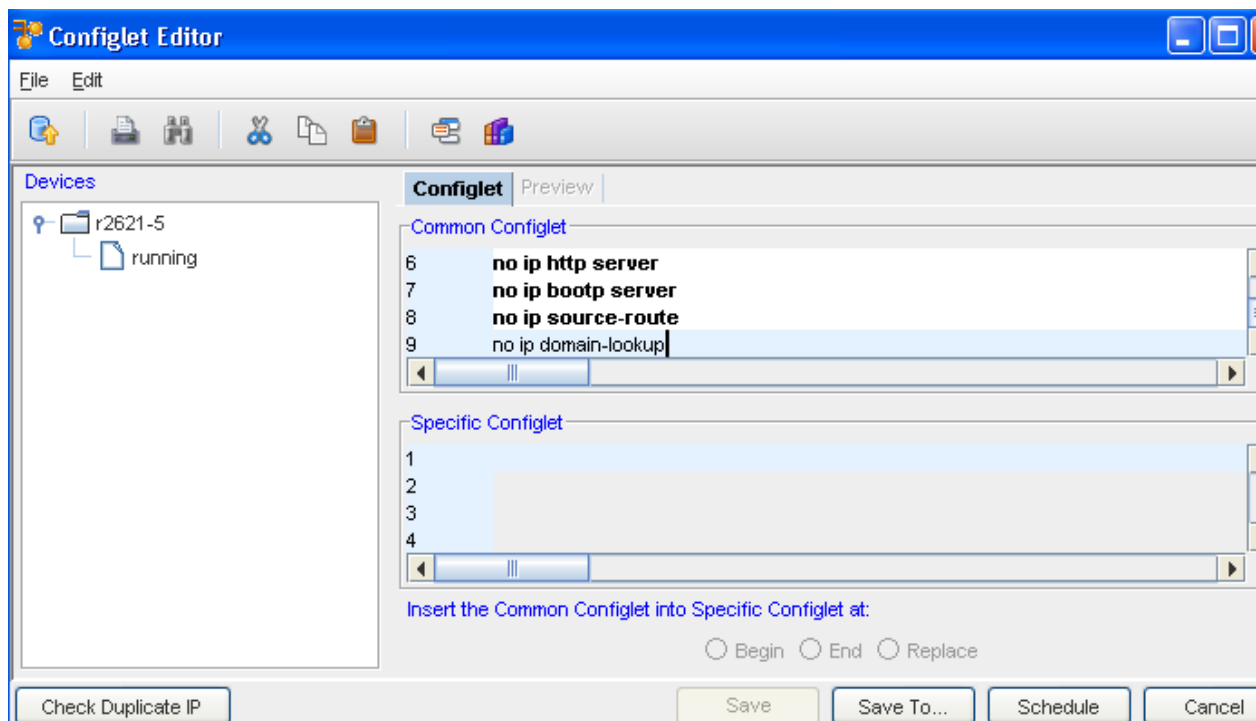
The Configlet Editor is used to edit whole or partial configurations that are Pushed to the network. When a single device is selected, one editor window opens. If more than one device is selected, the single editor session contains the selected devices listed in the Devices Column.

You can access the Configlet editor:

- From the Table layout in the Devices View, or, if you are using the Diagram view, select the **Devices**.
- In either layout, right-click on the **last selected device**. The right-click menu opens.

**Note** In a Table layout, a series of devices can be selected by holding down the Shift-key while selecting devices. **Or**, in a Table or Diagram layout, multiple devices can be selected by holding the Ctrl key while selecting devices.

Select **Editors**, then **Configlet**. The Configlet Editor window opens. Or, in the menu bar, click the **Configlet** icon.



The following components are available in the Configlet Editor window.

### Application Menu Bar Options

The menu options are:

File	Provides access to editor tasks
Save or Save To	Allows you to save the Configlet file as a new workspace, or as a .txt file
Schedule	Opens the Schedule Job window for scheduling when the Config is pushed to the network










Update Devices	Opens the Update Devices widow and allows you to update the Device List, and display the devices as tabs
Cancel	Cancels any changes made to the Config, and closes the Config Editor window
<hr/>	
Edit	Menu options for making changes to the Config file
Undo	Allows you to reverse any action completed in the editor window
Redo	Works with the undo feature, and allows you to "put back" your changes
Cut	Allows you to remove selected text
Copy	Allows you to copy selected text
Paste	Allows you to deposit the copied or cut text into another location
Select All	Allows you to select all the text on a page for copying
Find	Opens the Find and Replace feature
Go to	Allows you to jump to a specific line number




### Toolbars

The icons located on the segmented toolbars reflect actions that can be completed when using the editor.

Update Device List	Allows you to select or remove devices from the list
	
<b>Print</b>	Allows you to print the contents of the Config Editor (as shown)
	
<b>Search</b>	Opens the Find window, allowing you to find and replace details in the config
	
<b>Cut</b>	Allows you to select details in the content area and Cut text. Cut text can then be copied elsewhere in the content area, or copied into other editor sessions
	
<b>Copy</b>	Allows you to Copy any selected details, and Copy them elsewhere in the content area, or Copy into other editor sessions
	
<b>Paste</b>	Used with either the Copy or Cut feature to insert information into the content area of any open editor session
	

**Template**  Allows you to insert a saved template

**Insert Reference Variable**  Allows you to select and insert a Reference Variable

## Editor Content Area

Contains the content of the Config that is being pushed to the devices listed in the navigation pane.



<b>Buttons</b>	Provides access to editor tasks
<b>Audit</b>	Opens the Select item window, where you can select items
<b>Check Duplicate IP</b>	Allows you to check if a Duplicate IP is in existence
<b>Save To</b>	Allows you to save the Config file and the related device to a new workspace, or as a .txt file
<b>Schedule</b>	Opens the Schedule Job window for scheduling when the Config is pushed to the network.
<b>Cancel</b>	Cancels any changes made to the Config(s), and then closes the Config Editor window

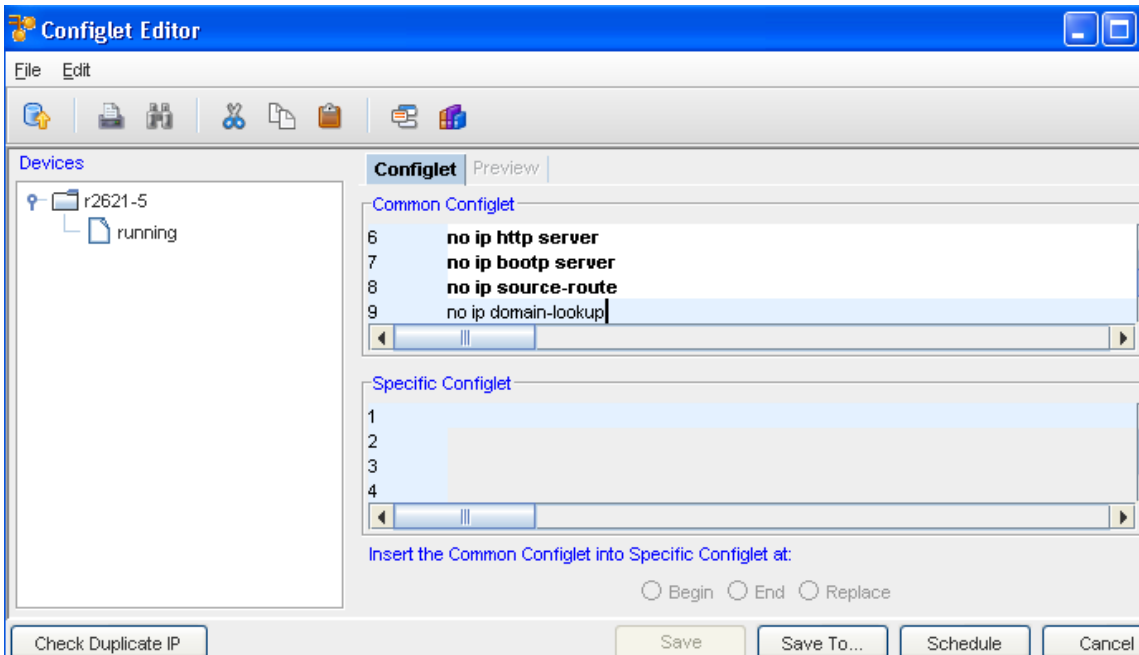
- [Using Reference Variables](#)
- [Additional Reference Variables](#)
- [Using IP Address Ranges](#)
- [Inserting Template Variables](#)
- [Inserting Reference Variables](#)
- [Updating Devices](#)
- [Using Find and Replace in Editors](#)
- [Scheduling a Job in Editors](#)
- [Saving in Editors](#)
- [Previewing Changes in Editors](#)

## Creating a Configlet

After determining which devices will receive the Configlet update, you can then create the configlet.

- 1 To update the listing of devices, Click **File -> Update Devices**, and then select the devices you want to add to this configlet.
- 2 In the Configlet Editor window, enter the **content of the configlet** in the Edit Configlet pane.

- 3 You can use the Insert template  and Insert Variables  icons to complete the content of the **Common Configlet** and the **Specific Configlet** sections.
- 4 Once the content is included, you must make the decision on where the Specific Configlet is to be placed within the Common Configlet.



- 5 Select Begin, End or Replace.

Since a configlet is not a full config file, once the Configlet is ready, you can then complete these tasks:

- Check for a **Duplicate IP**
- **Save** to a Workspace or file
- [Using the Scheduler.](#)
- **Cancel** the selections you have made, and leave this window

## Editing Configlets

Since a Configlet is partial text that is used to update a device's full Config file, the Configlet itself is an edit.

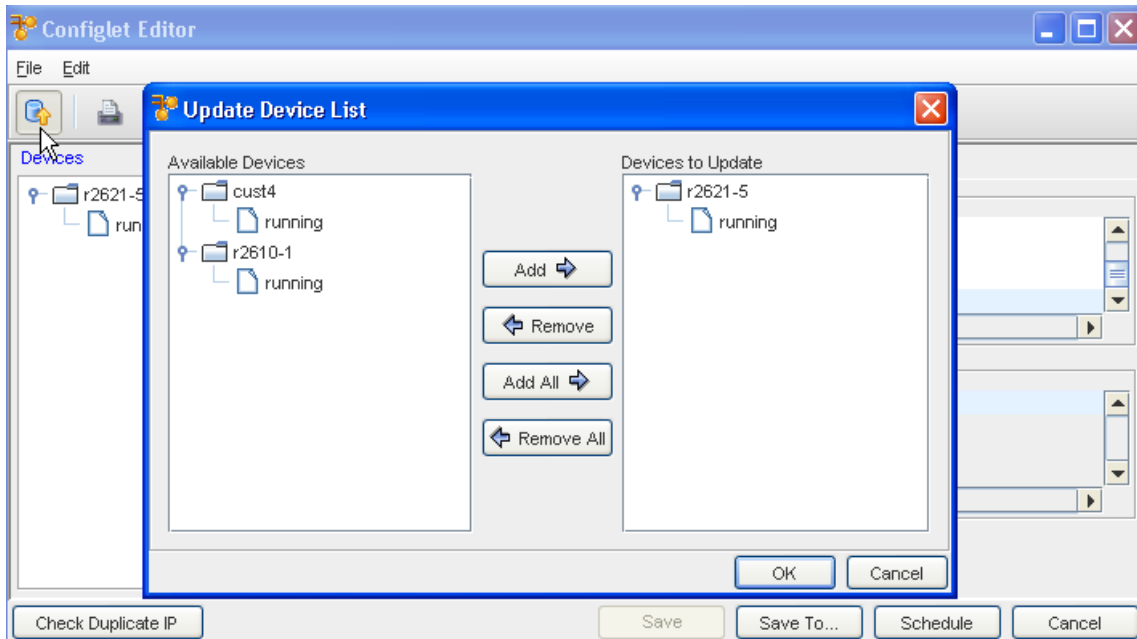
If there are changes to a Configlet that has been successfully pushed to the network, the change would entail creating a **new Configlet**, correcting the content of the original Configlet, and then scheduling it for Push to the network.

## Updating Devices Affected by a Configlet

The Configlet Editor lists the selected devices in the navigation pane. If additional devices are needed to be included in the Devices list, after the Configlet Editor is opened, you have the opportunity to edit the devices list.

To edit the list of devices affected by a configlet,

- 1 In the Configlet Editor window, click **File**, then **Update Devices**. You can also use the Update Devices icon.



The Update Devices List window opens. The Update Devices List window has two columns:

- **Available Devices** - these are the devices in a workspace or on the networks that will not be affected by the configlet push
- **Devices to Update** - these are the selected devices that are updated with the Configlet push

Either list can contain both virtual and network devices.

- 2 In the Available Devices column, select the **Devices** to be updated when the Configlet is pushed.

---

**Note** When using a Configlet to edit the Devices list, a series of devices can be selected by holding down the Shift-key while selecting the devices. You can also select multiple devices by holding down the Ctrl key while selecting the devices.

---

- 3 Click **Add**. The selected devices are then moved into the Devices to Update column. To move **all** of the devices listed into the Devices to Update column, click **Add All**.
- 4 If devices are not being removed from the Devices to Update column, click **OK**. The Update Devices List window closes. Or, if you are removing devices from the Devices to Update column so they are not affected by the pushed configlet, select the **devices**.

- 5 Click **Remove**. The selected devices are moved to the Available Devices column. To remove **all** the devices into the Devices to Update column, click **Remove All** .
- 6 When finished making changes (to the devices reflected in one or both columns), click **OK**. The Update Devices List window closes. The Configlet Editor is once again active.

The Devices column now reflects an updated list of devices that will be affected by the configlet push.

## The Interface Editor

### The Interface Editor Window

The Interface Editor is used to **make changes to multiple interfaces on multiple devices** . The editor uses [Creating a Configlet](#) to insert the changes. The changes affect the selected Interfaces and the device Global area.

The Interface Editor works in two ways:

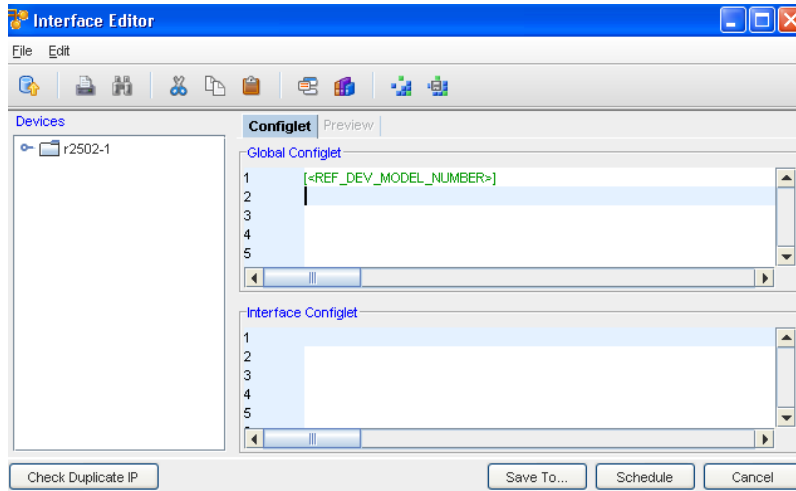
- Allows you to filter a devices interface's to include only the interfaces that are affected by the Configlet
- Allows you to make changes to devices globally, which affects all interfaces on multiple devices

The Interface Editor is accessible:

- In all **device views** . This includes, the default view of Devices, Sites, and Favorites
- By **right-clicking on a device** , and selecting **Editor -> Interface** from the **menu** toolbar

To open one or more interfaces in the Interface Editor,

- 1 If you are using the Table layout to view devices, select the **devices** from the table.
- 2 In the Editor menu toolbar, click **Interface**. Or, if you are using the diagram view, select the **devices**.
- 3 Right-click on the **last selected device**. The right-click menu opens.
- 4 Select **Editors**, then **Interfaces**. The Interface Editor window opens.



The following components are available in the Interface Editor window.

### Application Menu Bar Options

The menu options are:

<b>File</b>	Provides access to Editor tasks
<b>Load Collection</b>	Takes you to the Load Collection window where you can "name" the collection of Interfaces
<b>Save Collection As</b>	Allows you to Save the Collection of pre-defined interfaces to a device
<b>Save</b>	Allows you to save this config
<b>Save To</b>	Allows you to save the Config file as a new file, or as a .txt file
<b>Schedule</b>	Opens the Schedule Job window for scheduling when the Configlet is pushed to the network
<b>Update Devices</b>	Opens the Update Devices widow and allows you to update the Device List, and display the devices as tabs
<b>Cancel</b>	Cancels any changes made to the Configlets, and closes the Interface Editor window
<b>Edit</b>	Menu options for making changes to the Config file
<b>Undo</b>	Allows you to reverse any action completed in the editor window. For example, Typing, Cutting, Pasting or Removing of text.
<b>Redo</b>	Works with the Undo feature. Allows you to "put back" any changes that were completed using the undo feature.
<b>Cut</b>	Allows you to Remove selected portions of text in the editor window
<b>Copy</b>	Allows you to Copy any selected portion of text in the editor window
<b>Paste</b>	Allows you to Paste any portion of text that has been Cut or Copied from within the Configlet file, or from an external source
<b>Select All</b>	Captures the entire configlet file, for Cutting, Copying, or Pasting in another editor, or elsewhere in the current Config file

<b>Find</b>	Opens the Find and Replace feature as seen in the other editors
<b>Go To Line</b>	Allows you to jump to a specific line number in the Configlet file

## Devices Column











The navigation pane contains the devices and interfaces that are affected by the configlet push.

## Interface Tool bar



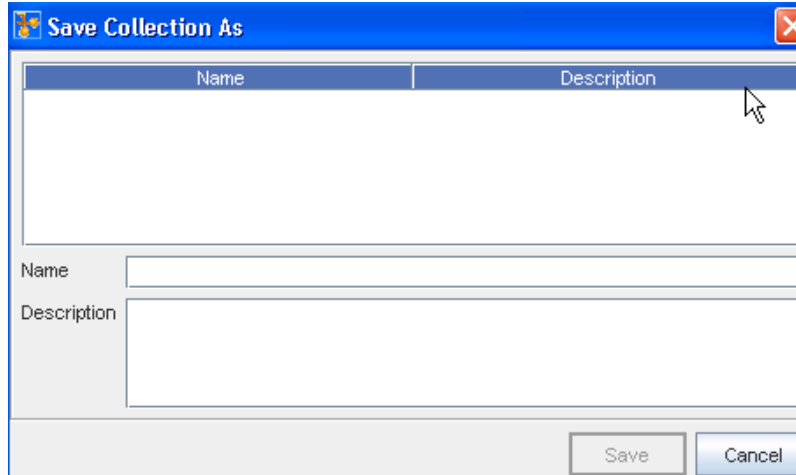
## Toolbars


The icons located on the segmented toolbars reflect actions that can be completed when using the editor.

<b>Update Device List</b>	Allows you to select or remove devices from the list
	
<b>Print</b>	Allows you to print the contents of the Config Editor (as shown)
	
<b>Search</b>	Opens the Find window, allowing you to find and replace details in the config
	
<b>Cut</b>	Allows you to select details in the content area and Cut text. Cut text can then be copied elsewhere in the content area, or copied into other editor sessions
	
<b>Copy</b>	Allows you to Copy any selected details, and Copy them elsewhere in the content area, or Copy into other editor sessions
	
<b>Paste</b>	Used with either the Copy or Cut feature to insert information into the content area of any open editor session
	
<b>Template</b>	Allows you to insert a saved template
	
<b>Insert Reference Variable</b>	Allows you to select and insert a Reference Variable
	
<b>Load</b>	Allows you to load the collection of the Device Interfaces
	
<b>Save Collection AS</b>	Allows you to Save Collection of the Device Interfaces
	

## Save Collection As

Whatever filters are (previously) applied for the interfaces, a "snapshot" is taken of those selected filters. If you want to use those, and only those filtered criteria, and save yourself time in updating devices and making changes to existing filter options, you can Save those interfaces as a "collection" to use again in the Interface Editor. When you use the **Save As** feature, you are anticipating that you will use this collection in the future.



- 1 Select the **Save Collection As**  icon.
- 2 Enter the **Name** and a **Description**. You can also select any existing Names to use if applicable.
- 3 Click **Save** after entering or selecting the Name.


## Load Collection

Use the **Load**  icon, or from the **File** option, select **Load Collection**.

From this section you can load a pre-determined "set" of interfaces (as determined by what is saved). To avoid having to filter devices, or update the devices listed, you can select a device and the device's interfaces.

- 1 In the Interface Editor window, click **Load**.
- 2 In the Load Collection window, select a name from the **previously Saved Device and interfaces** .

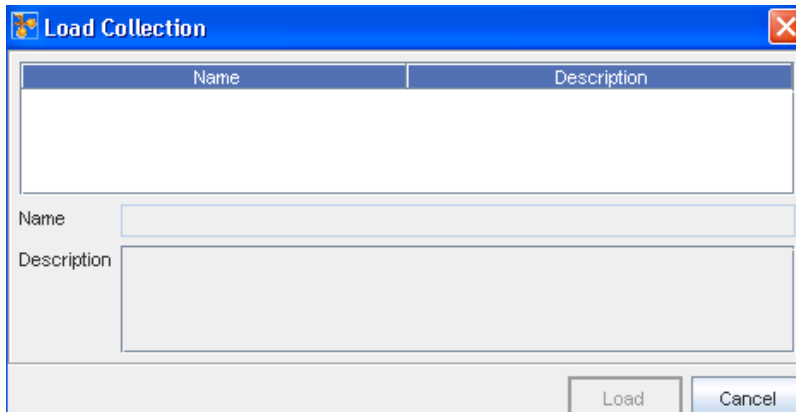
---

**Note**  This is where a good Description (in the Save As action) will help in determining the "collection" of what you want to load .

---

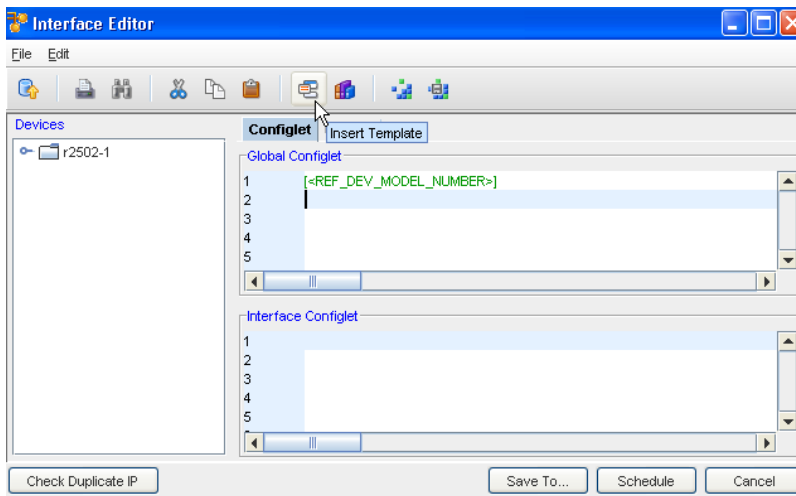
- 3 Select Load after making your selection.





### Edit Configlet Section

Within each of the sections; Interface and global, you can access the [Inserting Template Variables](#) and [Inserting Reference Variables](#).



### Editor Content Area

Contains the content of the Config that is being pushed to the devices listed in the navigation pane.

<b>Buttons</b>	Provides access to editor tasks
<b>Check Duplicate IP</b>	Allows you to check if a Duplicate IP is in existence
<b>Save To</b>	Allows you to save the Config file and the related device to a new workspace, or as a .txt file
<b>Schedule</b>	Opens the Schedule Job window for scheduling when the Config is pushed to the network
<b>Cancel</b>	Cancels any changes made to the Config(s), and then closes the Config Editor window

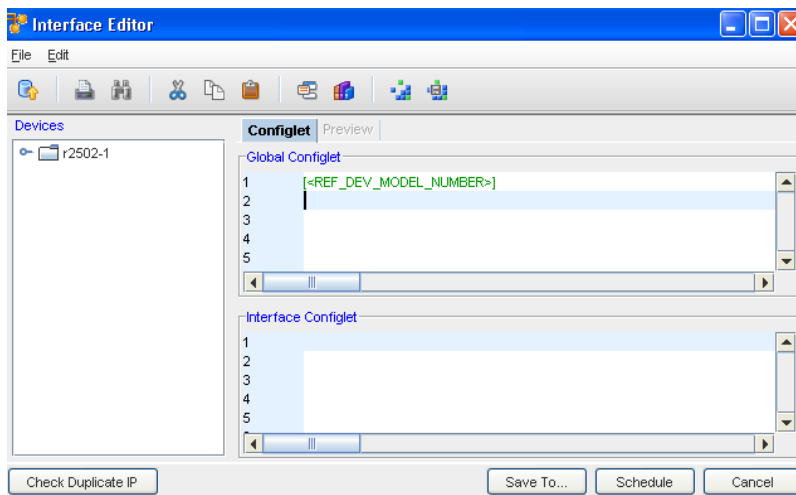
- [Using Reference Variables](#)
- [Additional Reference Variables](#)
- [Using IP Address Ranges](#)

- [Inserting Template Variables](#)
- [Inserting Reference Variables](#)
- [Updating Devices](#)
- [Using Find and Replace in Editors](#)
- [Scheduling a Job in Editors](#)
- [Saving in Editors](#)
- [Previewing Changes in Editors](#)


## Creating Interface Configlets

Once you have selected the devices and [The Interface Editor Window](#), you can select filter attributes, determine which devices and interfaces will be affected by the Configlet, and enter Reference Variables and templates.

- 1 In the **Interfaces Configlet** content area, enter the **configlet** that will affect the interfaces in the Devices column.



- 2 If creating a Configlet that will affect a device (in its entirety, not just its interfaces) in the Global Configlet content area, enter a Configlet.

- 3 Use the **Ref Var**  icon to insert an existing [Using Reference Variables](#).



- 4 To use a template when creating an interface or Global Configlet, click the respective

**Template**  icon. The Select Item window opens.

- 5 By default, the Select Item window opens to the network specific templates, but you also can choose System and Module templates.

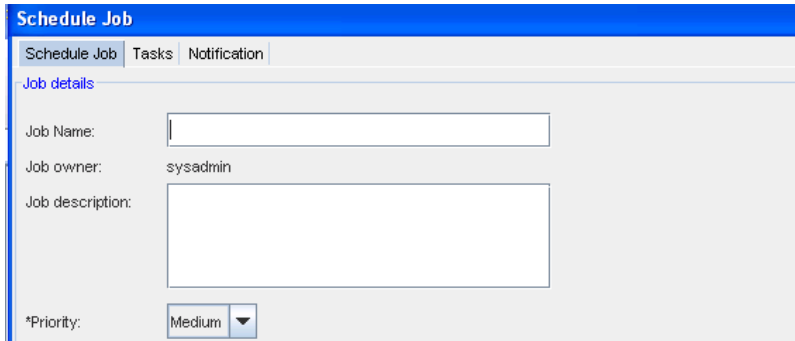
- 6 Navigate to the folder location of the template. Select the **template**.

- 7 Click **Select Item**. The Select Item window closes. The selected template is inserted into the Configlet.

- 8 You can also Load a Collection of Device Interfaces  , and then save the Collection of Device Interfaces  using the appropriate icons.

Now, you can select to **Schedule the Interface Editor window** .

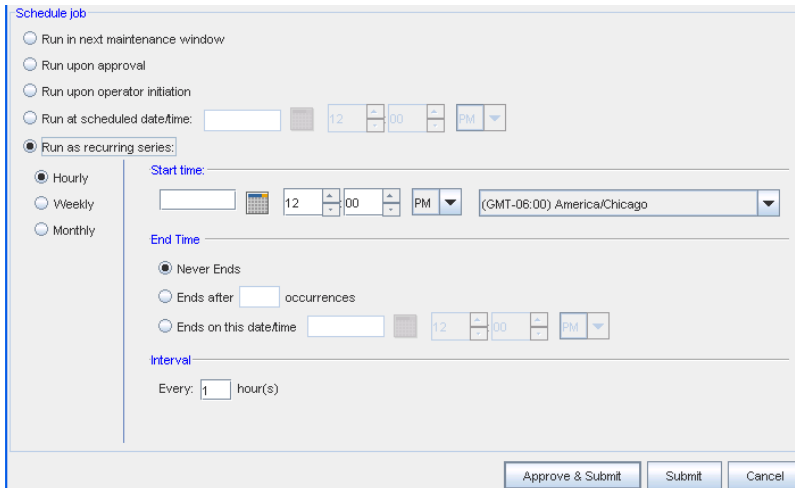
- 9 When you are ready to schedule, click the **Schedule Job tab**.



The screenshot shows the 'Schedule Job' window with the following details:

- Job Name:** [Empty text box]
- Job owner:** sysadmin
- Job description:** [Empty text area]
- \*Priority:** Medium (dropdown menu)

- 10 Enter the **Job Name** . You can also enter a Description.
- 11 From the drop-down list, select a **Priority level**.



The screenshot shows the 'Schedule job' window with the following options:

- Run in next maintenance window
- Run upon approval
- Run upon operator initiation
- Run at scheduled date/time: [Date/Time picker]
- Run as recurring series:
  - Hourly: Start time: [Time/AM-PM], [Timezone dropdown]
  - Weekly
  - Monthly
- End Time:**
  - Never Ends
  - Ends after [Occurrences] occurrences
  - Ends on this date/time [Date/Time picker]
- Interval:** Every: [1] hour(s)

Buttons at the bottom: Approve & Submit, Submit, Cancel

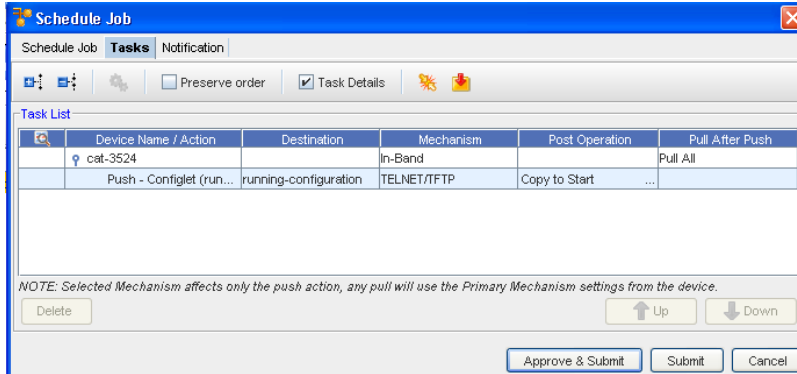
- 12 At the Schedule job section, by default, all jobs are scheduled to **Run upon approval** . All selections in the following example are displayed as being active in the schedule for viewing purposes only. With adequate permission, you can click the Submit button located at the bottom of the window.


Note that you can select to have the job **Run in the next maintenance window**.

- 13 If you select the **Run upon operator initiation** option, and Submit the job for approval, this keeps the job in a pending state after approval . After this, any user, with Schedule permissions, can then execute this job.
- 14 To set a specific time, select **Run at scheduled date/time** . The related date and time fields activate.
- 15 Enter a **date**. For assistance, use the Calendar icon to open a monthly calendar.

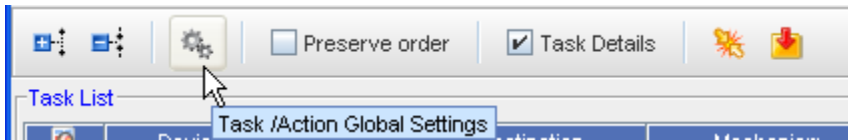
- 16 Select the time. The hour, minute and AM/PM setting must be designated.
- 17 If this option is okay, click **Submit**.
  - To set a recurring schedule, select **Run as recurring series** . The recurring setting options activate.
  - Set the recurring options: Frequency, Start and End Times, and Time Interval. The job is sent to the Schedule Manager, and the Schedule Job window closes.

You can also work with the **Tasks** window.

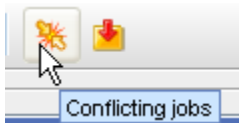


- 18 In the Schedule Job window, click the **Tasks** tab. You can view the tables in either an expanded or collapsed view. 

- 19 You can access the **Task / Global** window.




- 20 You can Preserve the order the tasks are currently listed in, and also access the Task Details.
- 21 You can check to see if there is a conflicting job, or you can access the Command Editor and add Commands.



The **Notification** tab can also be accessed.

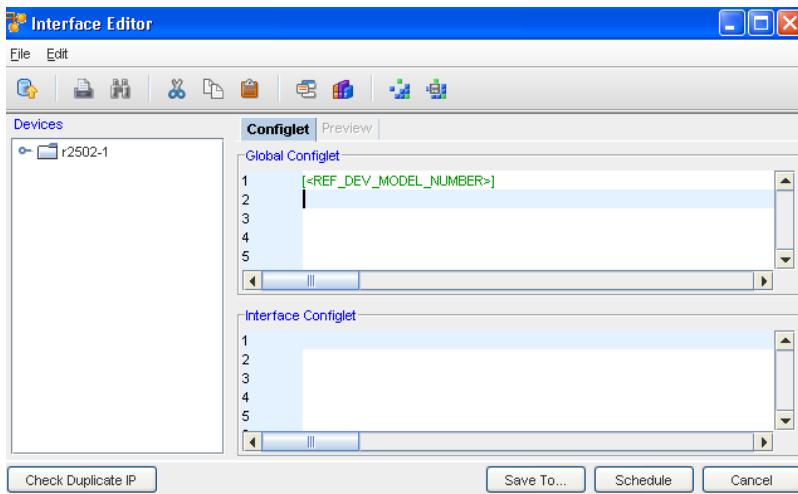
## Editing Interfaces

An Interface Config is used to send a scriptlet, written in the router's command-line language (for example, IOS for Cisco devices) to a device. The Interface config sends out a request, and also requests a responds regarding actions to a device.

**Note**  Once sent, an Interface config cannot be edited. If the config failed, you must then create and schedule a new Interface config.

## Interface Editor - Updating Devices

- 1 In the Interface Editor window, click the **Update Devices**  icon.



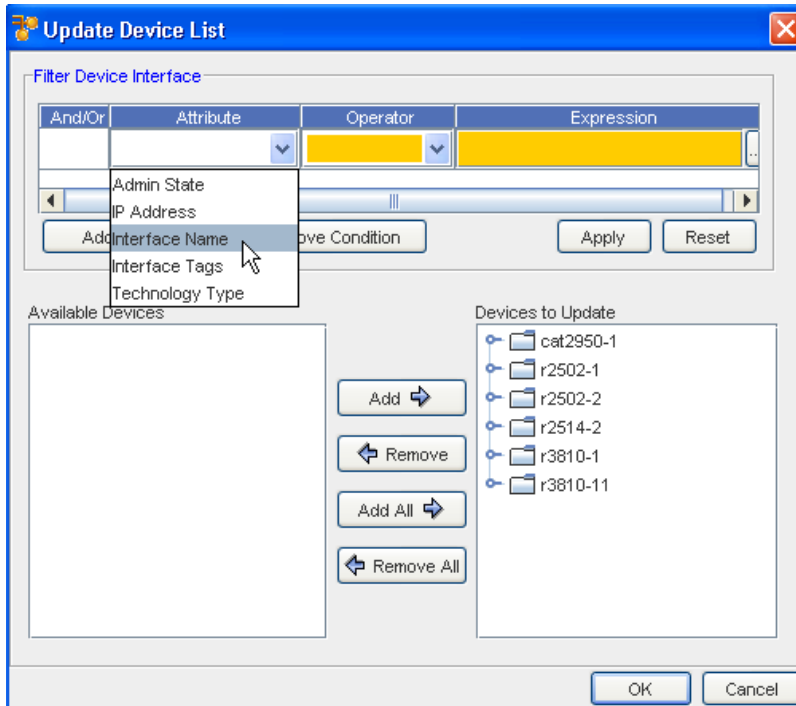
The **Update Device List** window opens. The Update Device List contains two sections:

- The Filter Device Interface options
  - The **Available Devices** section, which contains all devices in the opened view, and the **Devices to Update** column
- 2 From this section you can work with filters and their attributes by Adding or Removing conditions.
  - 3 You can also Apply the filters conditions, or you can select Reset to remove any existing attributes.

### Filter Device Interface section

To Add Condition,

- 1 To Add a Condition, click the **Add Condition** button. The window opens allowing you to add conditions from the list. You can select from And/or, select an Attribute and an Operator, and include an expression.



- 2 From the **And/Or** column, click the drop-down arrow to make your selection.
- 3 From the **Attribute** drop-down arrow, make your selection.
- 4 Make the **Operator** selection from the options in the drop-down.
- 5 Click the **Expression** column to add the Interface Name to the filter.
- 6 Click **Apply** when you have completed selecting the Interface attributes.
- 7 Now click **Ok** to return to the Interface Editor window.

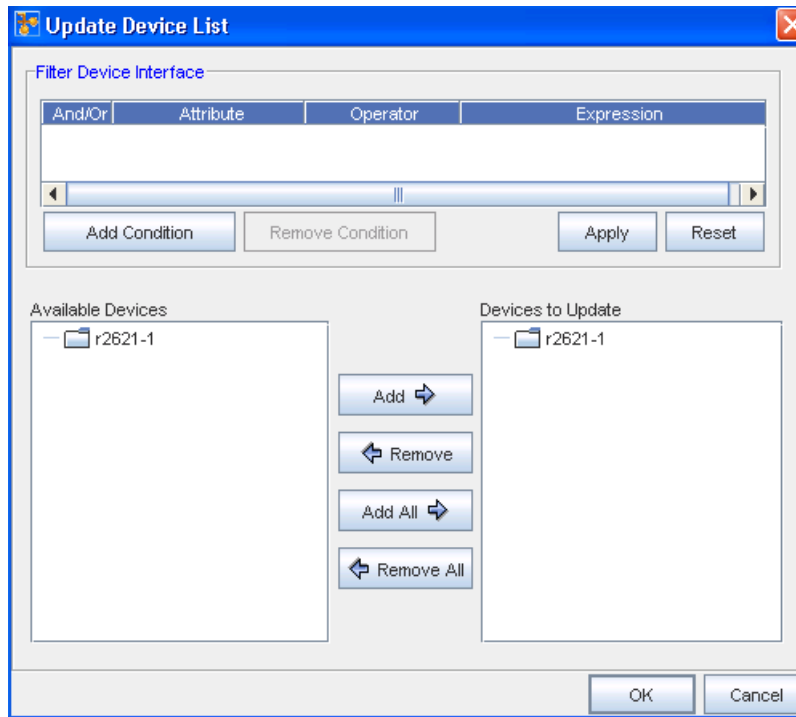
To Remove a Condition,

- 1 Select the entire line of Conditions from the list to highlight the condition you want to remove.
- 2 Once highlighted, click the **Remove Condition** button.
- 3 Click **Reset** when you have removed the condition.
- 4 Click **Ok** to return to the Interface Editor window.

### Available Devices and Devices to Update section

To Add Devices to Update,

From the bottom section of the Device List window, you can work to add devices to be updated.



- 1 From the listing of the Available Devices, add one or all of these devices using the **Add** or **Add All** arrows.
- 2 The devices you selected are now in the **Devices to Update** section.
- 3 If you need to remove devices from the **Devices to Update** column, and return them to the Available Devices column, highlight the Device then use the **Remove** arrow. You can remove all the devices using the **Remove All** arrow.
- 4 Click **OK** to return to the Interface Editor window.

## The Command Editor


### The Command Editor Window

The intent of the Command is not to change or update a device's configuration, although a Command can be used for this purpose. The intent is to provide access to device-level information for completing actions, such as:

- Providing a verification if a previous configuration change was completed correctly. For example, sending a "show interfaces" command to see that a new interface was successfully added.
- Completing tasks on the router for verifying the integrity of the network. This includes completing pings, tracers, and show routes.
- Completing router verification and diagnostics. This includes running internal diagnostics on a router, rebooting a router, and reloading alternate configurations.

Once a command has been pushed and scheduled on the device server, it is sent via a new DASL Device Driver. These script extensions work exactly like the regular PUSH sections, except they do not enter "conf t" mode prior to sending the commands to the device.

The Command Editor is accessible:

- When the Command  icon is active. For example, in a workspace.
- By **right-clicking on a device** and selecting **Editor** -> **Command** from the menu. The right-click menu feature is used in the navigation pane and accessible on any device to provide shortcut access to other features. For example: Editors, Wizards, Cut-Through functions, and more.

A Command can be created for one or more devices. The Command is then scheduled for all devices that are affected by the Command.

A Command is used to send a scriptlet, written in the router's command-line language (for example, IOS for Cisco devices) to a device that is then executed on the device, and the results returned to the user.

To open one or more Command files,

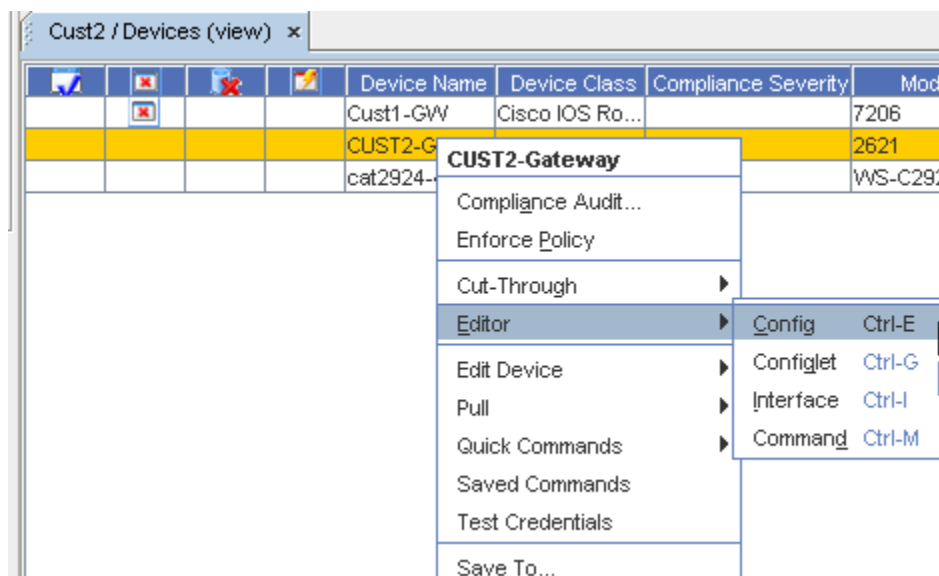
- 1 If you are using the Table layout to view devices, select **devices** from the table. Or, if you are using the Diagram view, select the **devices**.

---

**Note** In a Table layout, a series of devices can be selected by holding down the Shift key while selecting devices. Or, in a Table or Diagram layout, select multiple devices can be selected by holding the Ctrl key while selecting devices.

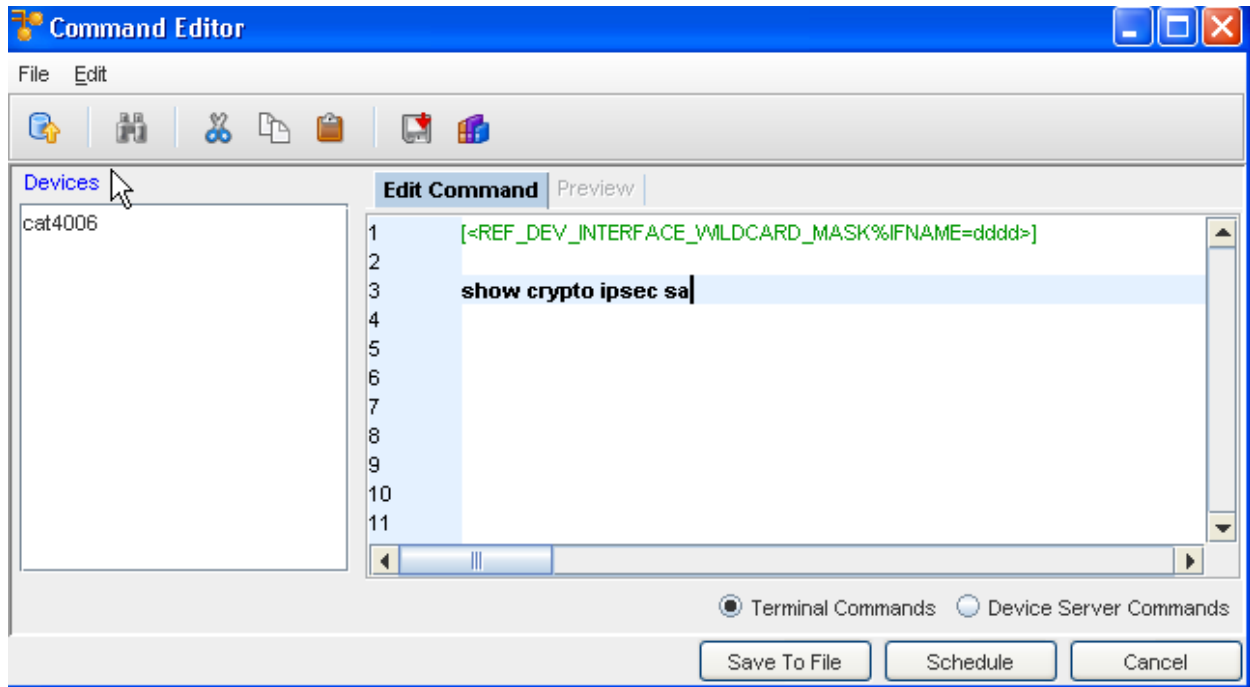
---

- 2 Select **Editors**, then **Command**.



When a single device is selected, one editor window opens. If more than one device is selected, the single editor session contains the selected devices listed in the Devices Column.





The following components are available in the Command Editor window.

### Application Menu Bar Options








The menu options are:

File	Provides access to editor tasks
Update Devices	Opens the Update Devices window and allows you to update the Device List, and display the devices as tabs
Schedule	Opens the Schedule Job window for scheduling when the Config is pushed to the network
Cancel	Cancels any changes made to the Config, and closes the Config Editor window
Edit	Menu options for making changes to the Config file
Undo	Allows you to reverse any action completed in the editor window
Redo	Works with the undo feature, and allows you to "put back" your changes
Cut	Allows you to remove selected text
Copy	Allows you to copy selected text
Paste	Allows you to deposit the copied or cut text into another location
Select All	Allows you to select all the text on a page for copying
Find	Opens the Find and Replace feature
Go to	Allows you to jump to a specific line number



## Toolbars

The icons located on the segmented toolbars reflect actions that can be completed when using the editor.

<b>Update Device List</b>	Allows you to select or remove devices from the list
	
<b>Search</b>	Opens the Find window, allowing you to find and replace details in the config
	
<b>Cut</b>	Allows you to select details in the content area and Cut text. Cut text can then be copied elsewhere in the content area, or copied into other editor sessions.
	
<b>Copy</b>	Allows you to Copy any selected details, and Copy them elsewhere in the content area, or Copy into other editor sessions
	
<b>Paste</b>	Used with either the Copy or Cut feature to insert information into the content area of any open editor session
	
<b>Command</b>	Allows you to insert a Command
	
<b>Insert Reference Variable</b>	Allows you to select and insert a Reference Variable
	

## Edit Commands

You must select either **Terminal Commands** or **Device Server Commands** by clicking within the appropriate radio button.

<b>Buttons</b>	Provides access to editor tasks
<b>Save To File</b>	Allows you to save this to a file
<b>Schedule</b>	Opens the Schedule Job window for scheduling when the Command is pushed to the network
<b>Cancel</b>	Cancels any changes made to the Commands, and closes the Command Editor window

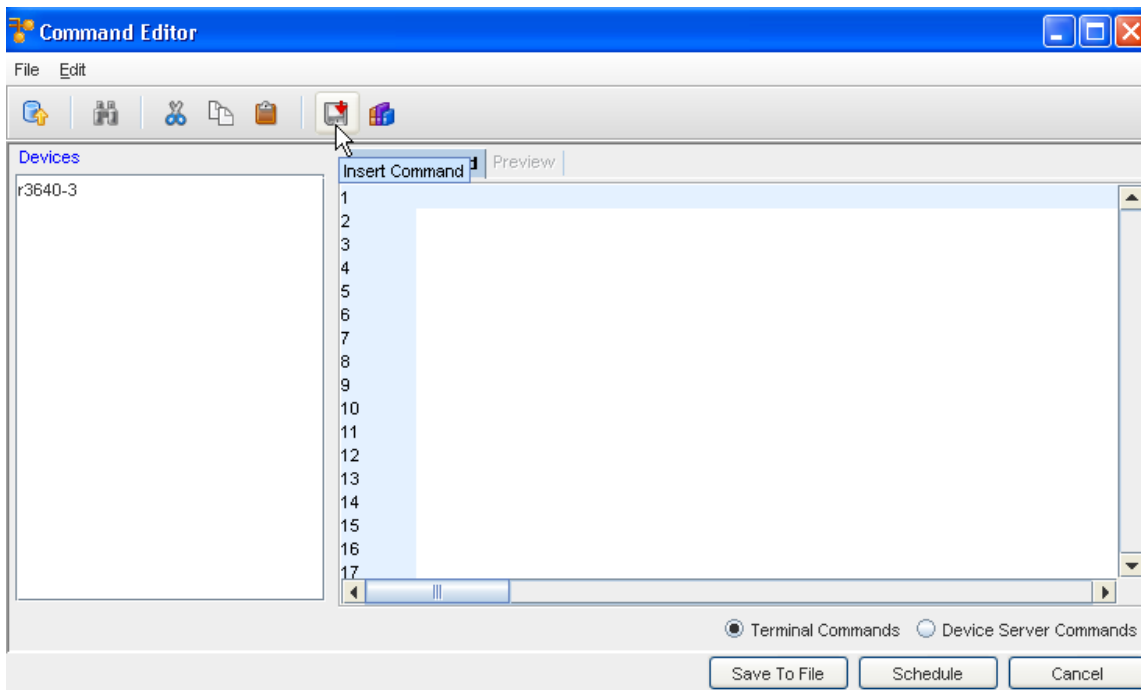
- [Using Reference Variables](#)
- [Additional Reference Variables](#)
- [Using IP Address Ranges](#)
- [Inserting Template Variables](#)

- Inserting Reference Variables
- Updating Devices
- Using Find and Replace in Editors
- Scheduling a Job in Editors
- Saving in Editors

## Creating a Command

The **Command Editor** can be accessed when the Command icon is active in the Devices view.

- 1 In the **Command Editor** window, enter the **content** of the Command in the Edit Command pane.



You can also use the command icon to select a command.

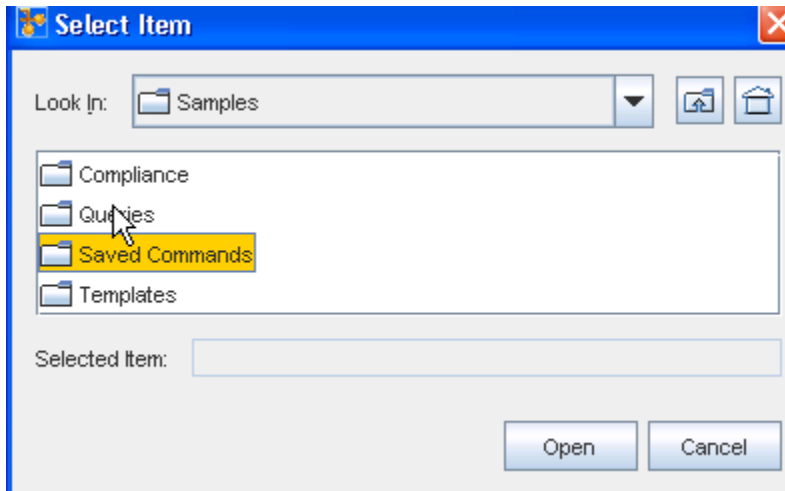
- 2 Click the **command icon**  .

---

**Note** By default, the Select Item window opens to network specific templates.

---

- 3 Navigate to the **folder location** of the command.
- 4 Select the **command**.



- 5 Click **Select Item** . The Select Item window closes. The selected commands are inserted into the Command.
- 6 Back at the Configuration window, you can click the [Using Reference Variables](#) icon.
- 7 You must also determine if these are Terminal or Device Server Commands, and mark the radio button accordingly.

- 8 You can also use the Insert Reference Variables icon  and insert an appropriate variable.

Since a config is not a full config file, once the Command is ready, you can then complete these tasks:

- **Save the Command as a .txt file, located on your hard drive or network**
- Save as a Workspace
- Schedule the job
- Cancel your activity on this window

---

**Note** Clicking the Device (under Devices in the Command Editor) allows you to then select Preview to view the text of the command.

---

## Editing a Command

A Command is used to send a scriptlet, written in the router's command-line language. For example, IOS for Cisco devices, to a device. The Command sends out a request and requests a response regarding actions to a device.

---

**Note** Once sent, a Command cannot be edited. If the Command fails due to an error, you must create and schedule a new Command.

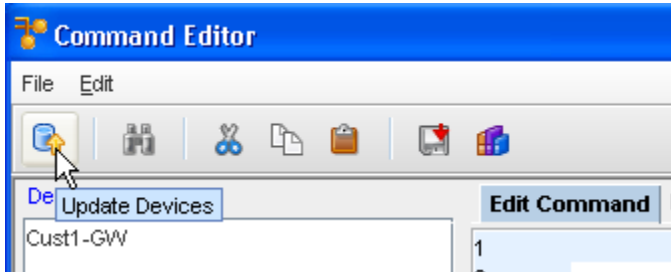
---

## Updating Devices Affected by Commands

The Command Editor lists the affected devices in the navigation pane. If additional devices need to be included to the Devices list after the Command Editor is opened, you can edit the devices list.

To edit the list of devices affected by a Command,

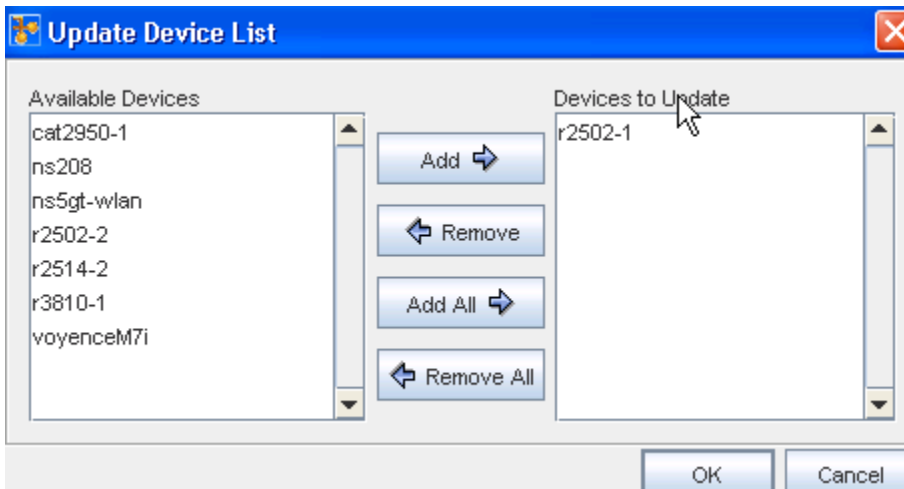
- 1 In the Command window, click **File** then click **Update Devices**. You can also use the Update Devices icon to get the Update Device List.



The Update Devices List window opens. The Update Devices List has two columns:

- **Available Devices** - are the devices in a workspace or on the networks that will not be affected by the Command push
- **Devices to Update** - are the selected devices that are updated with the Command push

Either list can contain virtual and network devices.



- 2 In the Available Devices column, select the **devices** that are to be updated when the Command is pushed.
- 3 Click **Add**. The selected devices are moved to the Devices to Update column.
- 4 If devices are not being removed from the Devices to Update column, click **OK**. The Update Devices List window closes. Or, if you are removing devices from the Devices to Update column, so the pushed Command will not affect them, select the **devices**, and then click **Remove**. The selected devices are moved to the Available Devices column.

- 5 When you have completed making changes to the devices reflected in one or both columns, click **OK**. The Update Devices List window closes. The Command Editor is now active.

The Devices column reflects an updated list of devices that will be affected by the Command push.

## Scheduling Jobs

### Using the Scheduler

When viewing the Schedule Manager, keep in mind that it now automatically refreshes when new jobs are added, or when there is a change in a job status. You always get the latest, real time view of the Schedule Manager.

When a configuration change is ready to be scheduled to one or more devices in the Network, typically on completion of an Editor session, the scheduler is opened. The scheduler allows you to define when a job is run, and enforces workflow approvals.

The Scheduler allows you to designate when jobs are **pushed** to the network. Access to the Schedule option is available at the bottom of each editor window.

The Scheduler allows you to complete the following tasks:

- Set the Priority of a Job
- Set Run Times for all Jobs
- Set Recurring Job Schedules
- Approve Scheduled Jobs (user-permissions required)
- Submit Jobs for Approval
- Send Notifications to Other Users Regarding Job
- Review Job Tasks
- View Data Fields

When opened, the Schedule Job window contains three tabs:

<b>Schedule Job</b>	Contains general job tasks details and date configuration settings
<b>Tasks</b>	Contains the task details of the job. Including the content of the <b>push</b> and the devices that are affected. Depending on how this is accessed, this tab may not be available on each Schedule Job window.
<b>Notification</b>	Contains settings and selections for who, when, and why notifications are sent while the job is processing
<b>Data Fields</b>	Contains the Data Fields for this selected device

For a job to be scheduled, details on the Schedule Job tab must be completed. Details on the Tasks and Notification tabs need not be completed to submit the job.

## Scheduling a Run Time

Regardless of how the Schedule Job window is accessed, the method of scheduling jobs is exactly the same. All required fields must be populated. Any required fields not populated will generate errors.

For more information on the various settings, see [Using the Scheduler](#).

The screenshot shows the 'Schedule Job' window with the following sections:

- Job details:**
  - \*Job Name: [Text input field]
  - Job owner: sysadmin
  - Job description: [Text area]
  - \*Priority: Medium (dropdown menu)
- Schedule job:**
  - Run in next maintenance window:
  - Run upon approval:
  - Run upon operator initiation:
  - Run at scheduled date/time: [Date/Time picker] PM
  - Run as recurring series:
    - Hourly: 
      - Start time: [Time picker]
    - Weekly: 
      - [Day of week picker]
      - Start time: [Time picker]
      - End Time: (GMT-06:00) America/Cr
    - Monthly:
  - Never Ends: 
    - Ends after [Number] occurrences:
    - Ends on this date/time: [Date/Time picker] PM
  - Interval: [Text input field]

Buttons at the bottom: Approve & Submit, Submit, Cancel.

In the Job details section of the Schedule Job tab,

- 1 Enter the **Job Name** .
- 2 You can also enter a job **Description**.
- 3 From the **\*Priority** drop-down list, select a **Priority level** .

This level determines the execution priority of your job in the Device Server. For most jobs, select the Medium priority. (This is the default.) This will run on a normal schedule. For jobs such as Cut-Through, you should select High as the priority as this task is completed in real time and needs the highest priority. A Low priority can also be selected if you have numerous jobs to run.

Scheduling a job,

- 1 At the Schedule job section, by default, all jobs are scheduled to **Run upon approval** . All selections in the following example are displayed as being active in the schedule for viewing purposes only. With adequate permission, you can click the Submit button located at the bottom of the window.
- 2 Note that you can select to have the job **Run in the next maintenance** window.
- 3 If you select the **Run upon operator initiation** option, and Submit the job for approval, this keeps the job in a pending state after approval . After this, any user with Schedule permissions can then execute this job.
- 4 To set a specific time, select **Run at scheduled date/time** . The related date and time fields activate.
- 5 Enter a **date**. For assistance, use the Calendar icon to open a monthly calendar.
- 6 Select the time. The hour, minute, and AM/PM settings must be designated.
- 7 If this option is okay, click **Submit**.
- 8 To set a recurring schedule, select **Run as recurring series** . The recurring setting options activate.

---

**Important** When the **recurring schedule** is selected, the new time zone drop-down options are available. Make your selection from the drop-down options. The time zone you select must be the **client's time zone**. The new time zone field will be propagated with the client time zone automatically when creating a new Maintenance Window or recurring scheduled job.

---



The screenshot shows a configuration window for scheduling a recurring series. At the top, there are two radio buttons: 'Run at scheduled date/time:' (unselected) and 'Run as recurring series:' (selected). Below the 'Run as recurring series:' option, there are three radio buttons for frequency: 'Hourly' (selected), 'Weekly' (unselected), and 'Monthly' (unselected). The 'Start time' section includes a date picker, a time field set to '12:00', a PM/AM selector set to 'PM', and a time zone dropdown menu set to '(GMT-06:00) America/Chicago'. The 'End Time' section has three radio buttons: 'Never Ends' (selected), 'Ends after' (unselected) with a text input field, and 'Ends on this date/time' (unselected) with a date and time picker. The 'Interval' section has a label 'Interval' and a text input field 'Every: 1' followed by 'hour(s)'. The window has a light gray background and a blue border.

9 Set the recurring options: Frequency, Start and End Times, and Time Interval.

10 If this option is okay, click **Submit**. The job is sent to the Schedule Manager and the Schedule Job window closes.

The **Cancel** button takes you out of this window, and back to the previous window you opened.

To review the process of a job, see the [Schedule Manager Overview](#)

## Using the Schedule Tab

The Schedule Job tab is divided into two sections:

- Job Details
- Schedule Job

The following fields are available used when scheduling a job. Required fields are identified by an asterisk.

Job Details,

- Enter the **Job Name** . The job name is how you will refer to the job in the job history. The Job Owner is System generated from the user creating the job.
- enter a **Job Description** . Add any comments in this area for outlining job significance and additional details that other users would find helpful during a review of job history and tasks.
- Select a **Priority Setting** . This allows the job to run ahead of other scheduled jobs, depending on the priority setting. Priority settings are: Low, Medium and High

Schedule Job,

---

**Note** The following graphic has been edited so that all options are active. When viewing the actual application, only the selected option is available.

---

The following fields are available used when scheduling a job. Required fields are identified by an asterisk.

Scheduling a job,

- 1 At the Schedule job section, by default, all jobs are scheduled to **Run upon approval** . All selections in the following example are displayed as being active in the schedule for viewing purposes only. With adequate permission, you can click the Submit button located at the bottom of the window.
- 2 Note that you can select to have the job **Run in the next maintenance** window.
- 3 If you select the **Run upon operator initiation** option, and Submit for approval, this keeps the job in a pending state after approval. After this, any user, with Schedule permissions, can then execute this job.
- 4 To set a specific time, select **Run at scheduled date/time** . The related date and time fields activate.
- 5 Enter a **date**. For assistance, use the Calendar icon to open a monthly calendar.
- 6 Select the time. The hour, minute and AM/PM setting must be designated.
- 7 If this option is okay, click **Submit**.
- 8 To set a recurring schedule, select **Run as recurring series** . The recurring setting options activate.
- 9 Set the recurring options: Frequency, Start and End Times, and Time Interval.

---

**Note** When the **recurring schedule** is selected, the new time zone drop-down options are available. Make your selection from the drop-down options. The time zone you select must be the **client's time zone**. The new time zone field will be propagated with the client time zone automatically when creating a new Maintenance Window or recurring scheduled job.

---

10 If this option is okay, click **Submit**. The job is sent to the Schedule Manager and the Schedule Job window closes.

The **Cancel** button takes you out of this window, and back to the previous window you opened.

## Reviewing Job Tasks

The Schedule Job Tasks tab allows you to review the job that is scheduled for **push or pull**. See: [Using the Scheduler](#).

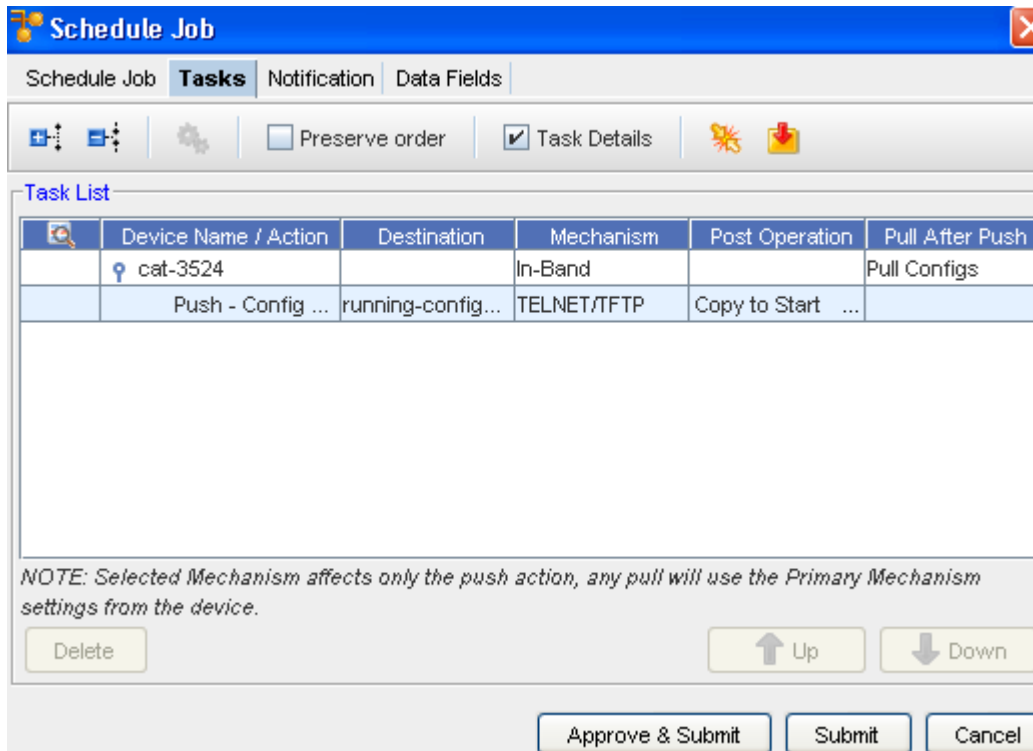
---

**Note** Depending on the module where the Schedule Job window is accessed, the Tasks tab may not be available.

---

The **Tasks tab** allows you to complete the following:

- Set a device order
- Designate a Run Type
- Identify Conflicting Scheduled Pushes or Pulls
- Insert a Command on-the-fly, into the content area of the scheduled job (Configlet, Config, Command or Interface)
- Complete a Modem Push
- Remove any Device from the Scheduled Update List



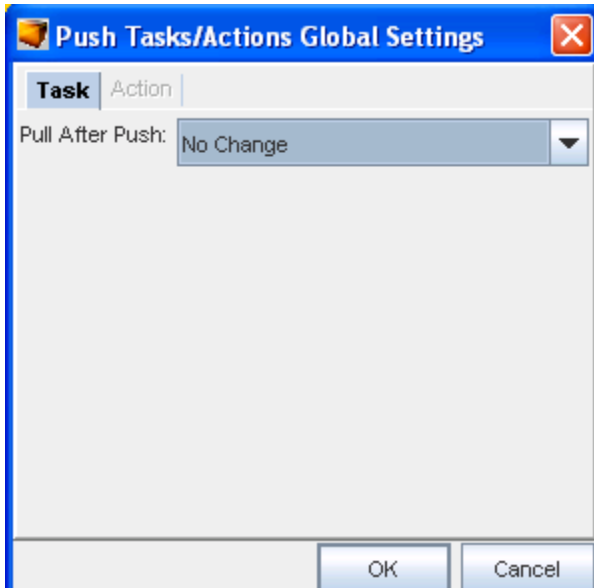
## Feature Toolbar

The first area of the Tasks tab is the toolbar. There are several actions that can be completed:

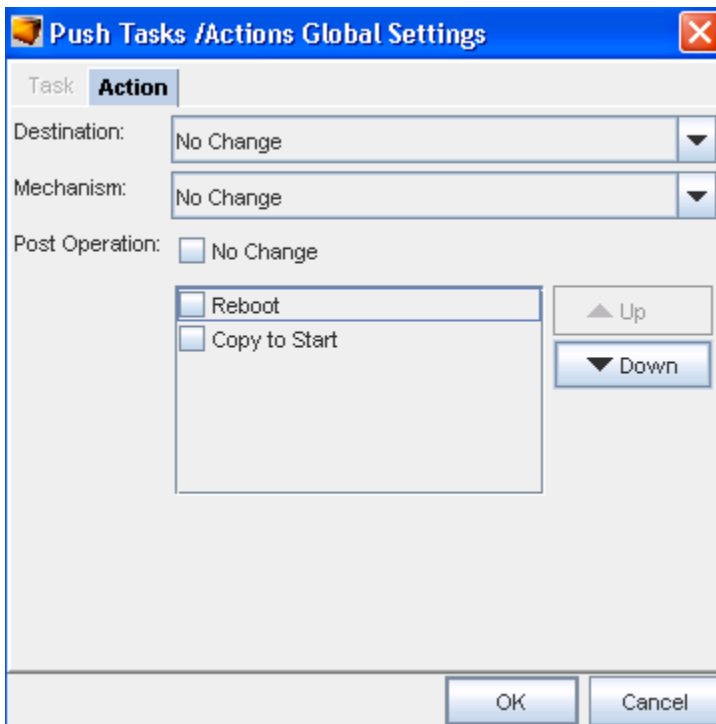
Icon	Description
	Expand the list
	Collapse the list
	Task/Action Global Setting
<input checked="" type="checkbox"/> Preserve order	Used to preserve the listed order
<input checked="" type="checkbox"/> Task Details	When a task is selected (under the Device Name) the task information is displayed. For example is this graphic the check box is checked and the details for that task ( <b>Config for running</b> ) are displayed.
	Prior to submitting any job, you can verify if there are any jobs that conflict with the job you are now scheduling
	Opens the Command Editor allowing you to create and insert a Command on-the-fly, into the scheduled job

## Content Area

The content area contains the body of the file being sent. This is the final opportunity, before push, that you are able to view the contents of the file being pushed.



When viewing the information contained within the Task tab, you can select the Global Settings icon and change the devices mechanism all at one time, rather than clicking each device listed, and changing the mechanism individually.

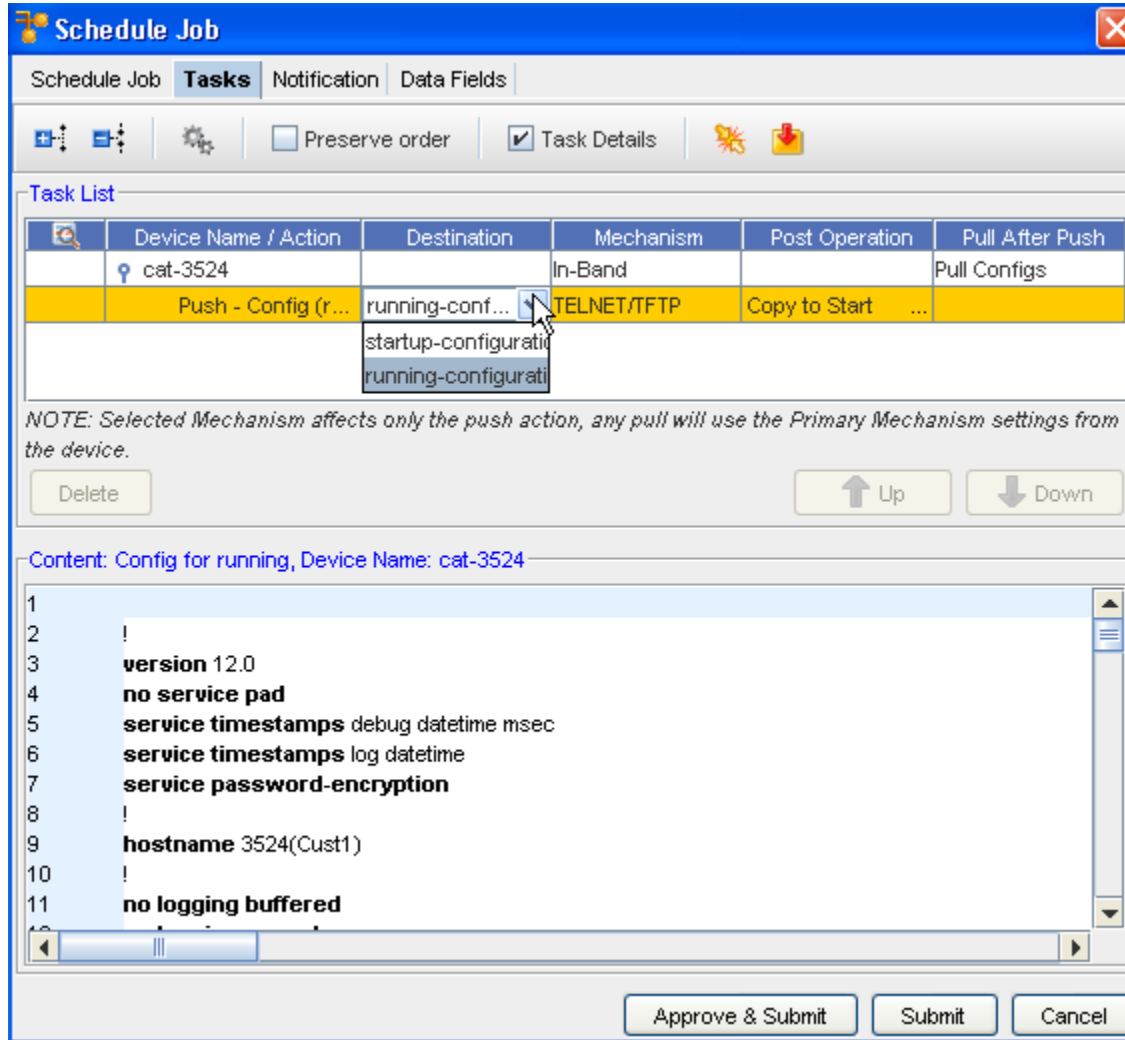


## Using the Task Tab

The Task tab details the actions that are scheduled for each device within a job. The listed devices can be moved to change the order in which each device receives its updates.



The **Tasks** tab on the Schedule Job window is divided into two sections:

- Task List with additional device information
- Content of the configuration for the running device



The first area of the Tasks tab is the toolbar. There are two actions that can be completed:

Icon	Description
	Expand or Collapse the list
	Task / Action Global Setting
<input checked="" type="checkbox"/> Preserve order	Preserve Order of the list
<input checked="" type="checkbox"/> Task Details	When a task is selected (under the Device Name) the task information is displayed. For example is this graphic the check box is checked and the details for that task ( <b>Config for running</b> ) are displayed.

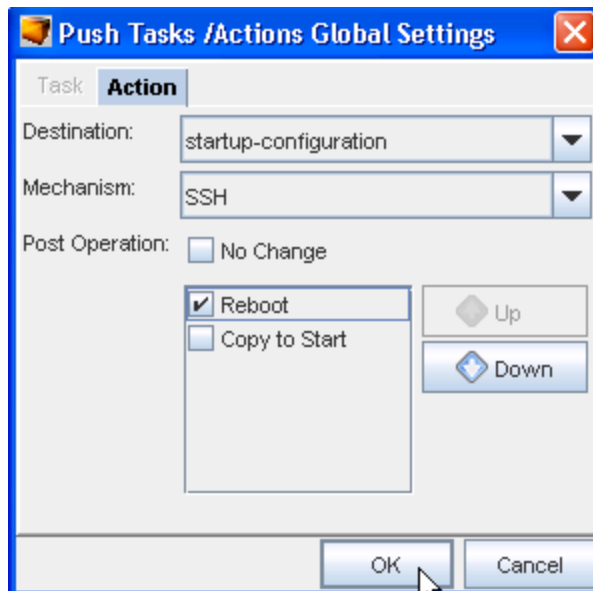
Icon	Description
	Prior to submitting any job, you can verify if there are any jobs that conflict with the job you are now scheduling.
	Opens the Command Editor allowing you to create and insert a Command on-the-fly, into the scheduled job

### Expand or Collapse

Use these icons to expand or collapse the task list.

### Task/Action Global Setting

When this is selected, the Push Task/Action Global Setting window opens, and allows you to make selections on Destination, Mechanism, and Post Operation settings.



### Preserve Order

Click this check box to preserve the order of the tasks list.

### Task Details

Click this check box to view additional details on the tasks.

### Conflict Resolution

- Before submitting a job, any job can be checked for Conflicts.
- A Conflict can occur if a previous job had been scheduled, but not yet executed for a device in the current job. Conflicts should be resolved before scheduling to ensure overwrites of changes do not occur.

### Commands

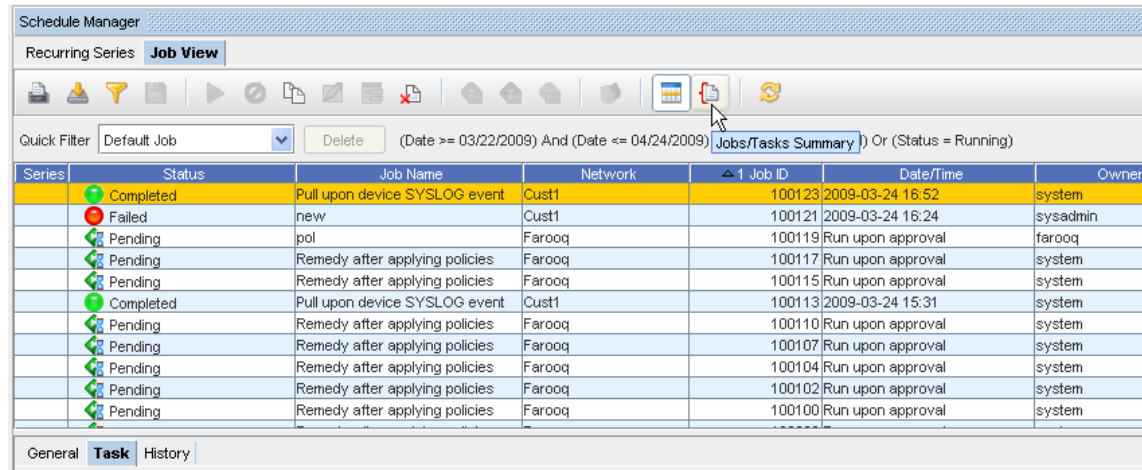
- Commands can be inserted into any scheduled job (via the Command Editor), and executed before or after configlet or config tasks.




- Commands help to validate the state of the device during job execution.
- The Command icon opens the Command Editor. Duplicate Commands are created for each device in the job.

## Reviewing Job/Status Summary

With the Schedule Manager displayed, you can select to review a Job/Status summary.



- 1 Select a **job** from the list, and then select the **Jobs/Tasks Summary**  icon.
- 2 The Job/Status summary information is presented in the left portion of the Schedule Manager window.
- 3 Click again on the Summary icon to close this Job/Summary window.

## Using the Notification Tab to Send an Email

The **Notification tab** allows you to select users or groups within your network, and users that are external to the application. You can then send email's regarding the state (status) of the job as it is processed. By default, all users and groups that have access to the Network are listed here. They do not receive email unless they are added to the Notification State column.

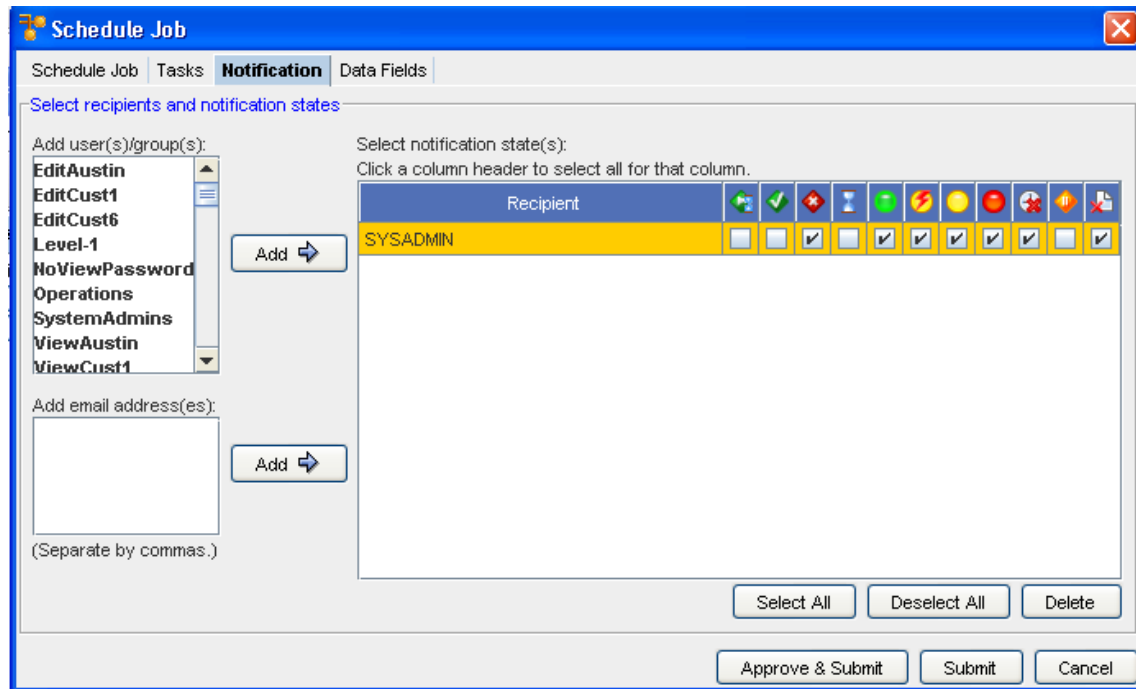
Any external email addresses can be added by entering names in the Add Email Address field, and adding these names to the Notification list.

---

**Important** You must add at least one email address to the Notification tab while scheduling a Report.

---

As jobs are being pushed to the network they have various states. Depending on the success of the push, the states (or status) the device goes through vary.



The Notification tab contains three sections.

- Add users/groups
- Add email Addresses
- Select Notification States

**Note** The Select All, De-select All, and Delete buttons can be used in the Notification States section to work with the list of recipients.

## Add users/groups

The Add user/group section allows you to select users or groups from all the available Network Configuration Manager users.

## Add email addresses

The Add email addresses section allows you to enter a comma delimited list of external user's email addresses.

## Notification States

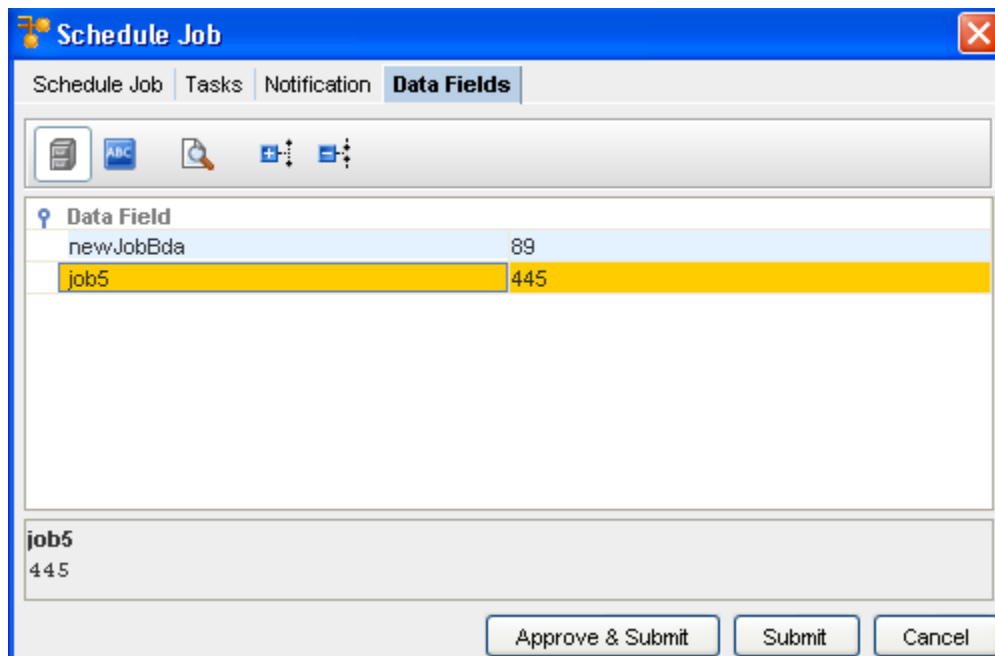
When users are added (using one of the methods listed above) each job state is available for selection for each user. Depending on the user or group, the check boxes allow you to select notification status, based on the user or group's needs.

To send an email notification to users and/or groups,

- 1 On the Notification tab, select the **users** from the Add user/group column. Or if you are adding external email addresses, enter the email addresses in the Add email addresses text field. A comma ( , ) must be used to separate each email address.
- 2 In the Notification State section, select the **job states** for each user/group, for which an email will be sent. At the bottom of the window is the option to **Select All** job states. This option checks all the check boxes, for all the listed users/groups. Or, to reset all users/groups, click **Deselect All**.
- 3 When finished with the job details, click **Submit**. for the job to be submitted to the Schedule Manager. Or, if you have been granted adequate permissions, click **Approve & Submit**. The job will be scheduled to run based on the settings that were defined in the [Using the Scheduler](#).

## Viewing Data Fields

The Data Fields tab allows you to view the Data Fields for a specific job or schedule.



## Working with the Schedule Manager

### Schedule Manager Overview

The Schedule Manager provides a view into **all jobs scheduled** , and their **job status** within Network Configuration Manager.

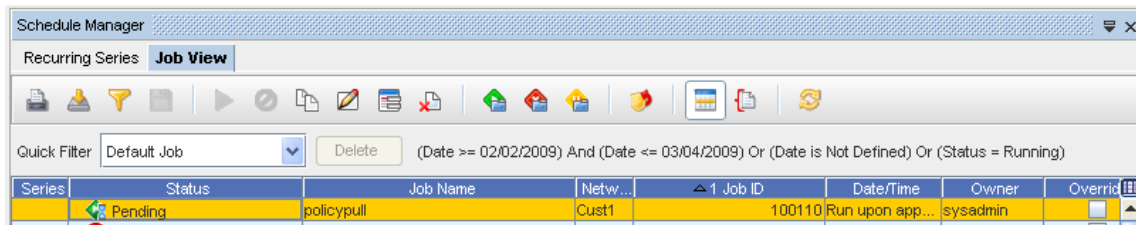
When any changes have been made to the Schedule Manager, such as Jobs Added, Jobs Changed, or Jobs Removed, the Schedule Manager view is automatically refreshed (updated) to reflect these change.

You can access the Schedule Manger from the **Tools** option in the menu bar.

**Note** Security Permissions apply, so you cannot view jobs you do not already have permission to view.

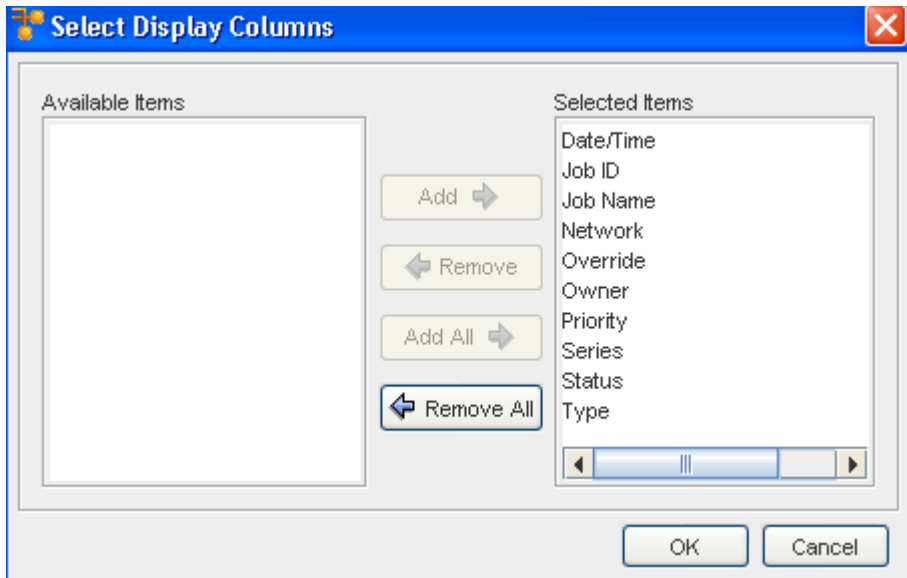


The Scheduler Manager has separate sections detailing information pertaining to various jobs. These include the **Job View** and the **Recurring Series** . The Recurring Series tab displays primary information for recurring jobs.



Within the **Job View** tab contents, the first section of the Schedule Manager details each job's information. The various columns give you specific job information.

- 1 To view even more job information, right-click on any column heading to see the available column options in the **Select Display Columns** window. Move column headings between the **Available Items** and **Selected Items** to view more or less job information displayed within the Schedule Manager.
- 2 After making your selections, click **OK**.



**Note** If you have previously defined filters, use the Quick Filter drop-down arrow to see the selections of filters, then make a selection from the list. To designate a new filter, click the Apply icon, and then define your filter criteria.

This **Status** tab displays the current status of each job. Jobs fall into the following categories:


- Completed
- Approved
- Rejected
- Running
- Failed
- Pending
- Completed/Warning
- Cancelled
- Partially Completed
- Hold



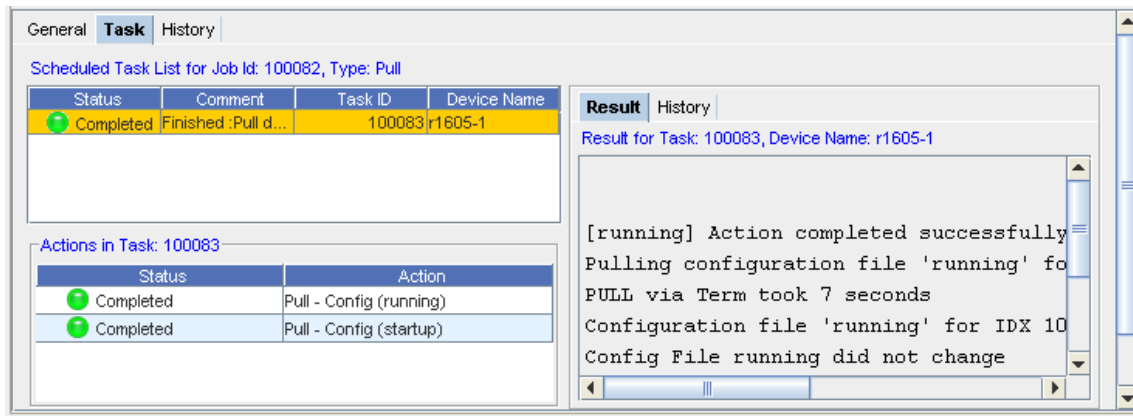
**Note** The tool bars displayed in Job View and Recurring Series include some different icons. To review the icons in the Recurring Series that differ from those in the Job View see: [Recurring Series](#).

Once a job displays in the Schedule Manager, the following tasks can be completed:

- Printing a copy of a Job
- Exporting a Job (copy)
- Filtering the Job Listing
- Quick Filter
- To Save the Current Filter
- Executing a Job
- Canceling a job
- Copying a Job
- Copying a Job
- Adding a Data Field
- Deleting a Job
- Changing the Job Status
- Schedule Manager (Override) Update Credentials
- Job Details
- Reviewing Job/Status Summary
- Refreshing a Job List

- 3 Within the **Job View** tab, view more information by clicking the **Details**  icon. The bottom section of the Schedule Manager displays the **details** of a job, including the **General** and **Task** information for the job selected from the list.

### Schedule Manager tool bar options



The screenshot shows the 'Task' tab of the Schedule Manager. It displays a 'Scheduled Task List for Job Id: 100082, Type: Pull' with one task: 'Completed' status, 'Finished :Pull d...' comment, '100083' Task ID, and 'r1605-1' Device Name. Below this, 'Actions in Task: 100083' are listed in a table:

Status	Action
Completed	Pull - Config (running)
Completed	Pull - Config (startup)

To the right, the 'Result' tab shows the following log output:

```

Result for Task: 100083, Device Name: r1605-1

[running] Action completed successfully
Pulling configuration file 'running' fo
PULL via Term took 7 seconds
Configuration file 'running' for IDX 10
Config File running did not change
    
```

## Recurring Series

There are two tabs located within the Schedule Manager.

- The **Job View** is just that, a listing of the current jobs that have been scheduled to run, along with information pertaining to each job.
- The second tab at the top of the Schedule Manager is the **Recurring Series** tab. If there have been any jobs scheduled to run on a **Recurring Series**, those jobs are listed within this tab. The Recurring Series tab displays primary information for recurring jobs.





This tab is much like the Job View tab, giving you access to details, and providing the same information on each job through the General and Task tabs.

Notice that the tool bar options within the Recurring tab are more limited than those options on the Job View tab. This is because the recurring jobs are very specific. For example, you **cannot Execute or Cancel a recurring job**.

Note the following icons:

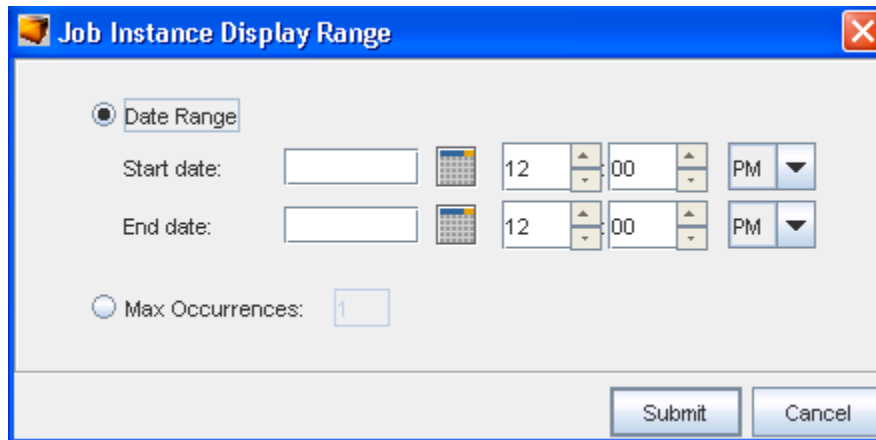


When the recurring **Series**  icon is selected, the original or primary recurring jobs are listed. These are the jobs that were originally created to run specifically at set intervals.

The **Instances**  icon, when selected, allows you to make changes in the "instances" you want to run **from** the originally scheduled job. Each time a scheduled recurring job runs, it creates an instance.


When the Instances icon is selected, the **Job Instant Display Range** window opens. From here, you can make changes to an "instance". For example, if you want the **Max Occurrences** to be 10, click the radio button, and insert the number **10**. Click **Submit** when you have made selections from this window. This tells the application that you want the original recurring job to run 10 instances.


You can also alter the **Date Range** of the "instance" by first clicking the Date Range radio button, then entering the day and the time for both the Start and End dates.



**Job Instance Display Range**

Date Range

Start date:   12  00  PM

End date:   12  00  PM

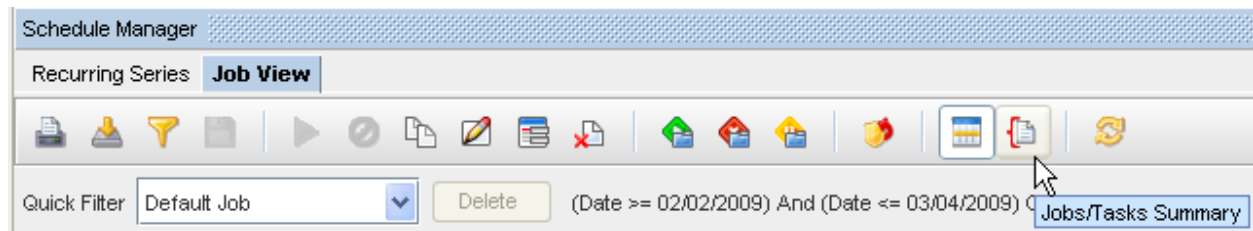
Max Occurrences:

Submit Cancel

## Viewing a Scheduled Job Summary

When viewing the Schedule Manager, keep in mind that it now automatically refreshes when new jobs are added, or when there is a change in a job status. You will always get the latest, real time view of the Schedule Manager.


To view a summary of the scheduled jobs and their current status, select the **Summaries** icon on the tool bar bar.



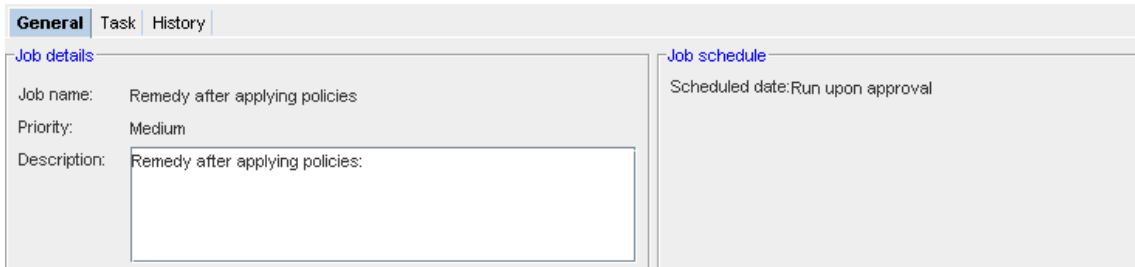
The Summary of jobs is displayed to the left of the listing of jobs. Notice that the summary includes the total count of the jobs, divided into status categories.

## General Tab

### Job View

- 1 With the **Details** icon  clicked and the details displayed on the Schedule Manager window, select the **General** tab.
- 2 You can view the information contained within the General tab for any job you have selected from the list.



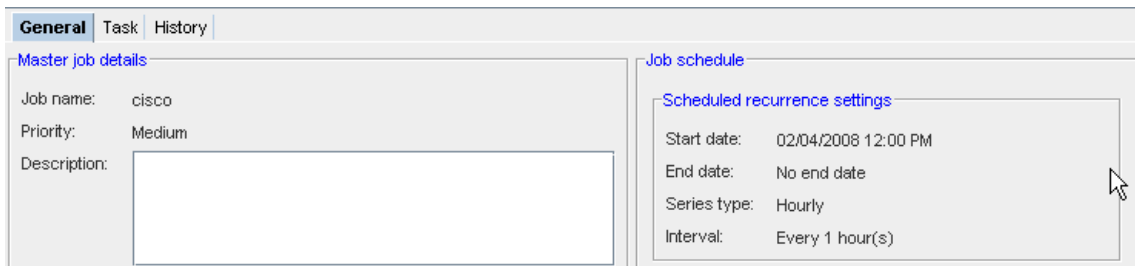


3 Switch to the **Task** tab, or the **History** tab for more detailed information.

### Recurring Series



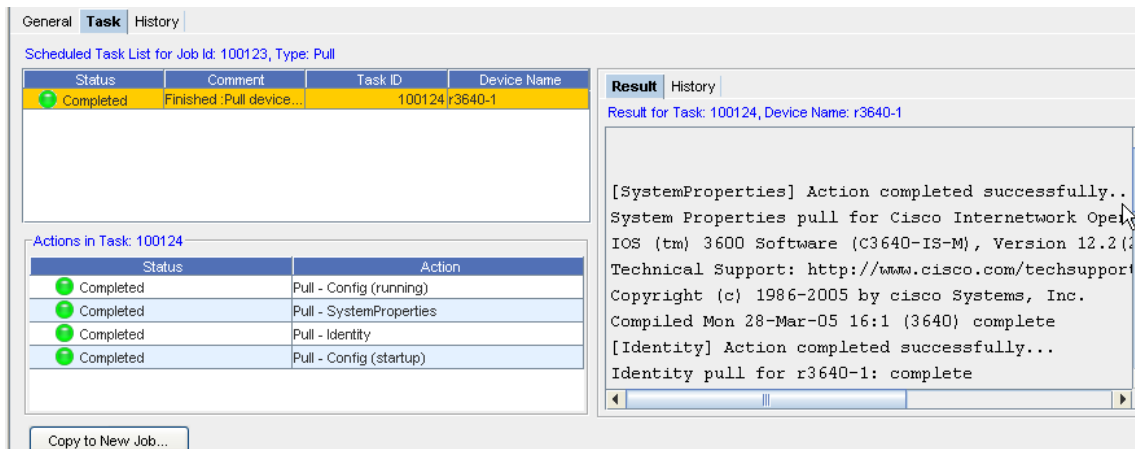
- 1 With the **Details** icon clicked and the details displayed on the Schedule Manager window, select the **General** tab.
- 2 You can view the information contained within the General tab for any job you have selected from the list.



3 Switch to the **Task** tab, or the **History** tab for more detailed information.

### Task Tab

- 1 To view more details concerning any job that has been scheduled, first select a job from the listing. In this example, **Job ID 100083** has been selected from the list.



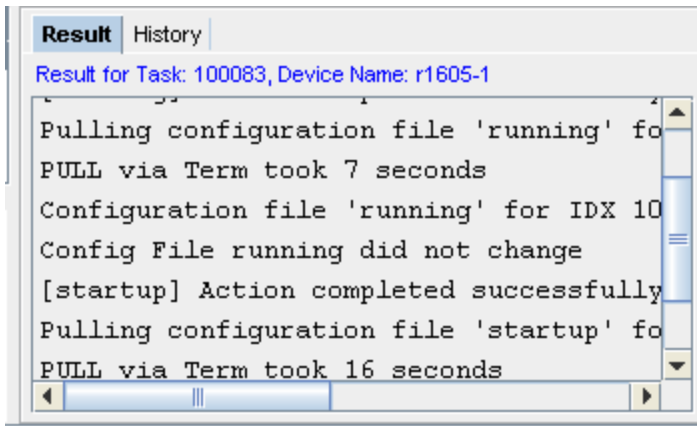
- 2 Within the **Task** tab, the **Scheduled Task List for Job Id:100083, Type: Pull** is displayed. This indicates that a Network push was requested. This push entails that all devices within that specific network are affected.
- 3 As you can now complete multi-config pushes, the **Actions in Task:** section details the results of each action associated to each task . View the **Result** tab to see the results for each action associated with the Network Push task.

---

**Note** The Actions in Task number will always be one number higher than the Job ID number.

---

- 4 The **Result** section details the results for the Task (shown here at 100057), and the Device as Router. Scroll through this section to view the actions results. The **Results** tab shows information **associated to the Action**.




---

**Note** **E rrors and warning** from Device Services (detailed in the Schedule Manager) are **color coded**. Errors are displayed in **red**, while warnings are in **orange**.

---

Within the contents of the Results tab, there may be symbols accompanying the contents.

The following symbols are used to help define the contents.

- 5 Next, click the **History** tab to view the history details of the task. The **History** tab displays information **associated to the Task** .

Result tab,

Symbol	Description
>>>	Indicates information is included
!!!	Indicates here is a warning
---	Indicates negative information
===	Indicates information set on device

History tab,

Comments	Time / Date
Completed successfully	2008-12-02 10:53
Finished :Pull device configurat...	2008-12-02 10:53
Task started on default Dec 02...	2008-12-02 10:53
Starting :Pull device configurati...	2008-12-02 10:53
Executing :Get Configuration Fi...	2008-12-02 10:53
Queued for execution	2008-12-02 10:53

Selected history comments

Completed successfully

Selected task comments,

From this section, you can view the **Selected History Comments** on the each task. Scroll to view all comments.

**Note** View the **Task** tab in the **Recurring Series** section as well to get additional job information for specific Recurring jobs.

## The History Tab

The History tab displays a history of the events taken place for a specific job. For example, in the following graphic, the job has gone through three separate events to complete successfully.

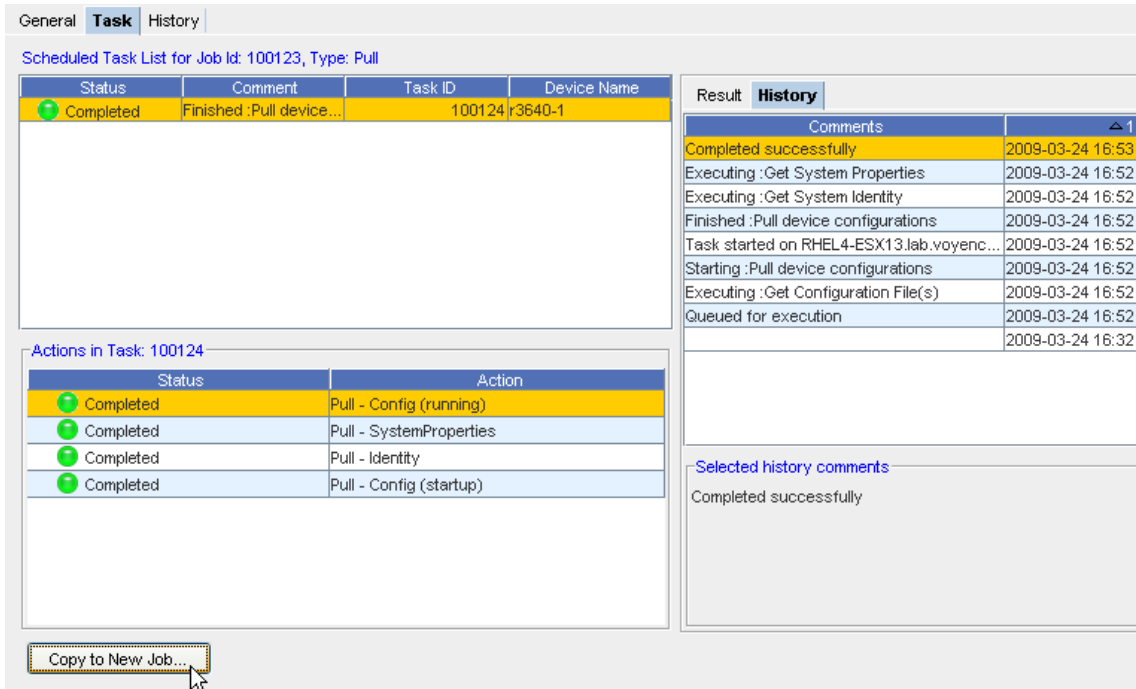
Time / Date	Comments
2008-02-04 05:18	Completed successfully
2008-02-04 05:17	Queued for execution
2008-02-04 04:57	Device Event :1.3.6.1.6.3.1.1.5.5:

Selected history comments

There may be comments (if added) you can also view from this tab.

## Additional Task

From the **Task** tab you can access an additional Task. For example, with the **Job View** displayed, and the **Task** tab selected, you can access the following task - **Copy to New Job** - for **Pull Only** jobs.




This takes you to the Schedule Copy Pull job window.

## Printing a copy of a Job

From the Schedule Manager window, you can access the icon to **Print a copy** of the job displayed.




1 Select the Job from the listing of jobs displayed.

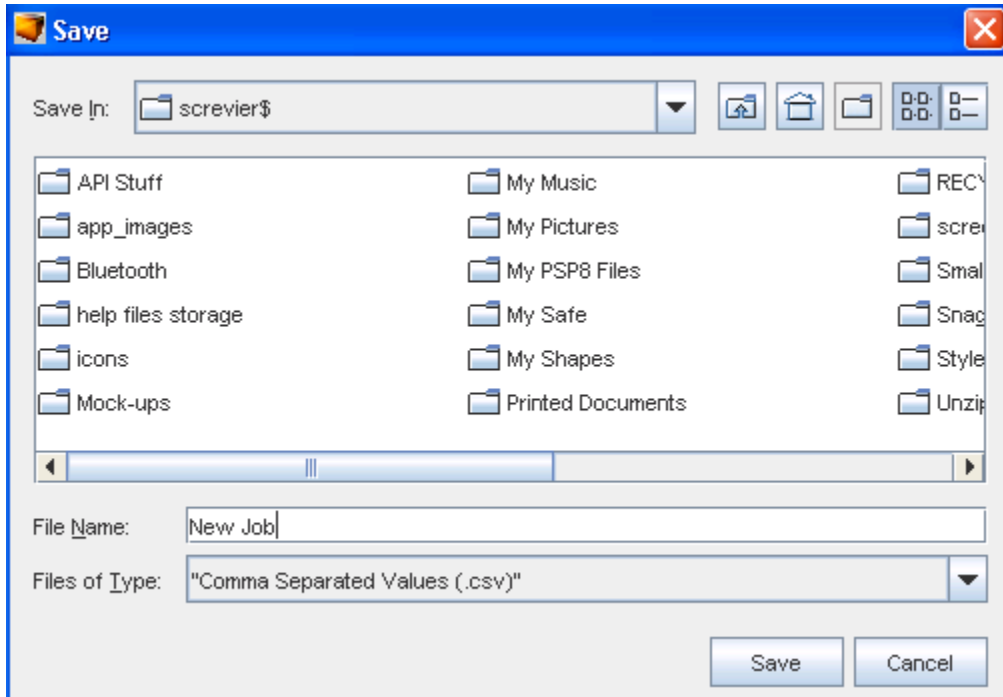
2 Click the **Print** icon  to use your browser's print facility. The printed copy contains the Status, Network, Job ID, and more.

## Exporting a Job (copy)

From the Schedule Manager window, you can access the icon to **Export a copy** of the job displayed.




- 1 With the list of jobs displayed, click the **Export** icon . The Save Job window opens.

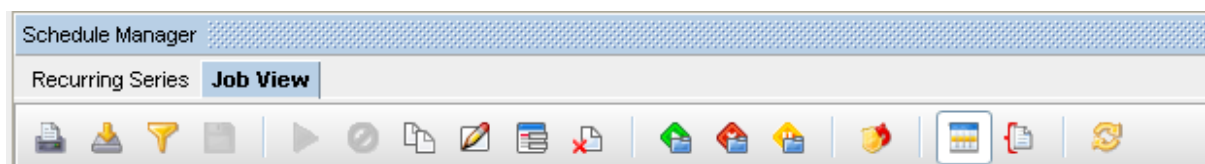


- 2 Determine **where** you want to export this job to, and the **File Name**, then click **Save** after making your selections.
- 3 You can also change the File Name, as well as designate the File Type when exporting a job. A copy of the job you exported is now stored in the format (Files of Type) you selected.

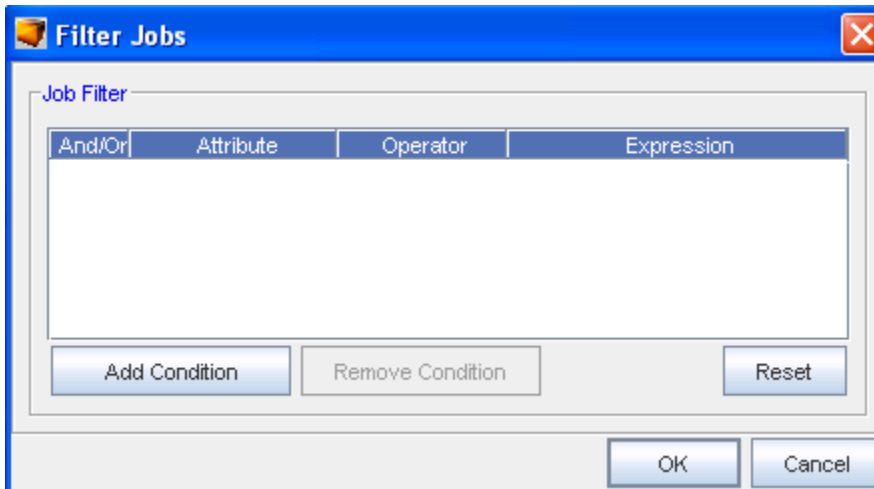
## Filtering the Job Listing

From the Schedule Manager window, you can access the icon to **Filter the list of jobs** displayed.

- 1 With the list of jobs displayed, select the Filter **Apply** icon  on the Schedule Manager window.



The Filter Jobs window displays.



- From here, use the **Add Condition** button to add another filter. Remember, you must have an Expression for each Attribute.

---

**Important** Click **Reset** to remove any existing filters.

---

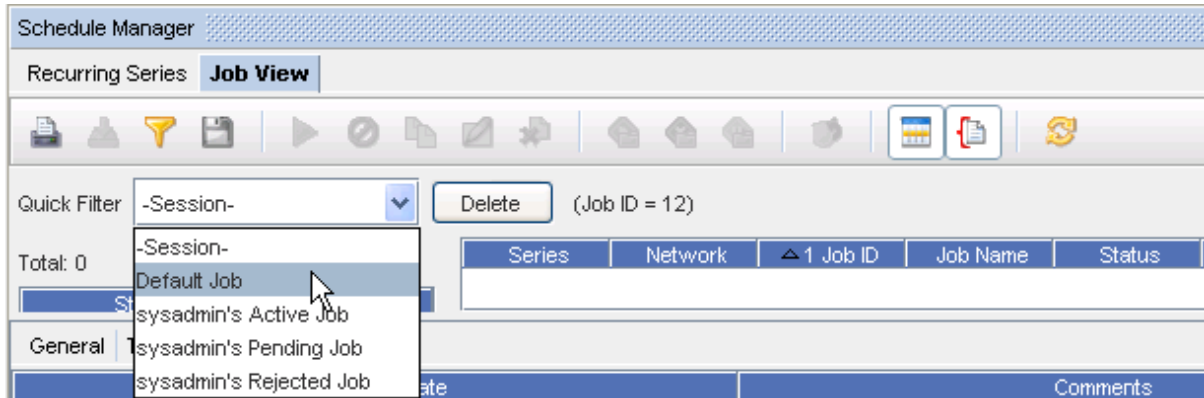
- You can also use the **Remove Condition** to have an existing conditional filter removed.
- Click **Ok** when you have made your filtering selections.
- You can Save the current Filters using the **Save** icon.

### To Save the Current Filter

If you have changed filters, (see the Filter Job window above) and used the **Apply** icon, you can now **Save** that new filter.



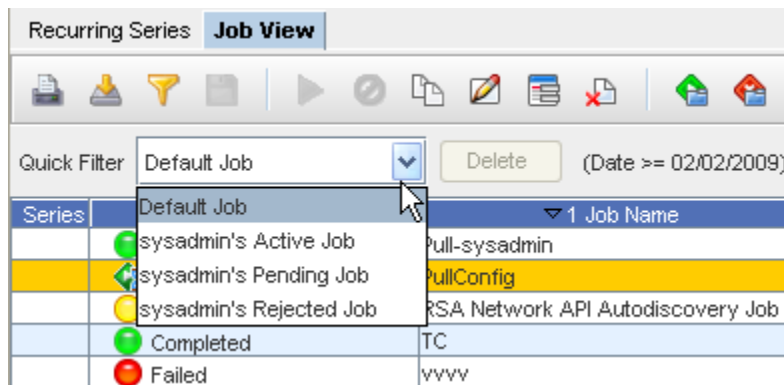
- Click the **Save** Filter icon, to name and save that filter,.
- The next time you want to select a filter, using the Quick Filter drop-down selections. The newly save filter is now in the listing, and can easily be selected.



- Using the Quick Filter drop-downs, you can also Delete a filter you have saved. Select a filter name from the list, then click **Delete**.

## Quick Filter

From the Schedule Manager, you can use the **Quick Filter** drop-down arrow options to determine what jobs you want displayed, by filtering.



You can use the Default to view all the Jobs in the Schedule Manager. You can also select from the following filters:

- Active
- pending
- Rejected

---

**Note** The Default is to show all jobs.

If you have perviously defined your own filters, you can use the **Delete** button to delete any selected user-defined filters from the Quick Filter drop-down options.

---

**Note** You cannot delete the system filters.

## Executing a Job

Use the **Execute** icon (where appropriate) to execute an existing job in the Schedule Manager listing. The job must have already been **scheduled and approved** , and you must have adequate permissions to complete this task.

- 1 Select the **job you want to Execute** from the listing of jobs.
- 2 Next, click the **Execute** icon.
- 3 Click **Ok** at the confirmation message.

## Canceling a job

Use the **Cancel** icon (where appropriate) to cancel a job in the Schedule Manager listing. You must have permission to cancel a job that has not yet run.



- 1 Select the **job you want to cancel** from the listing of jobs. Only Running jobs can be cancelled.
- 2 Next, click the **Cancel** icon.
- 3 Click **Ok** at the confirmation message.

## Copying a Job

Instead of recreating a job and tasks, an existing scheduled job can be copied, edited, and then scheduled as new.

Using the Schedule Manager, the following tasks can be completed:

- Copy an existing job, edit, and reschedule
- Edit an existing recurring job
- Delete an existing recurring job
- Filter the list to display specific job types
- Approve or reject recurring jobs
- Review the details of a recurring job

To copy a scheduled job,

- 1 From the menu bar, select **Tools - > Schedule Manager**.
- 2 On either the Job View or the Recurring Series tab, select a **job**. The grayed out icons in the toolbar now activate.



- Click the  **Copy icon** . The Schedule Copy Pull Job window opens.



The **Copied Job ID** number indicates that this job is a copy of an existing job.

- After you have entered the **new Job Name**, then go to the **Schedule Job** section of the window to Submit this job.

The screenshot displays the 'Schedule Job' configuration window. It is divided into two main sections: 'Job details' and 'Schedule job'.

**Job details:**

- Copied job ID: 100060
- \*Job Name: [Empty text box]
- Job owner: sysadmin
- Job description: [Empty text area]
- \*Priority: Low (dropdown menu)

**Schedule job:**

- Run in next maintenance window:
- Run upon approval:
- Run upon operator initiation:
- Run at scheduled date/time: [Empty] [Calendar icon] 12:00 PM
- Run as recurring series:
  - Hourly: 
    - Start time: [Empty] [Calendar icon] 12:00 PM (GMT-06:00) America/Chicago
    - End Time:
      - Never Ends:
      - Ends after [Empty] occurrences:
      - Ends on this date/time [Empty] [Calendar icon] 12:00 PM:
    - Interval: Every: 1 hour(s)
  - Weekly:
  - Monthly:

Buttons at the bottom: Approve & Submit, Submit, Cancel

- 5 If needed, click the [Using the Notification Tab to Send an Email](#) and add users, add email addresses, and select the notification states for users who need to be notified of the new job.

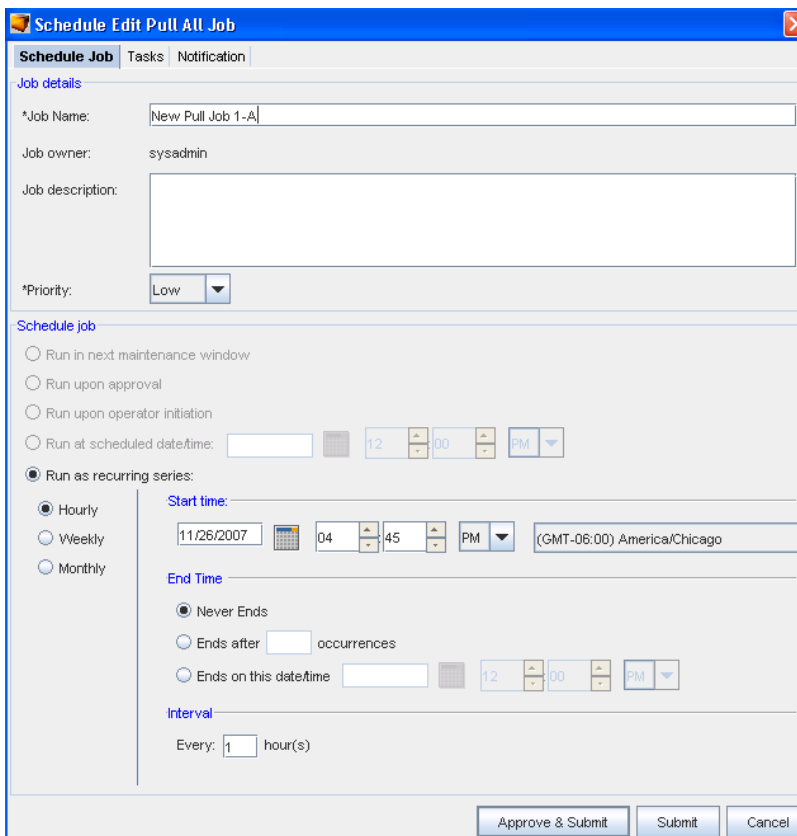
## Editing a Job

To edit a scheduled job,

- 1 From the menu bar, select **Tools - > Schedule Manager**.
- 2 On either the **Job** or the **Recurring Series** tab, select a **job**. The grayed out icons in the toolbar now activate. The job must be in a Hold, Pending, or Approved Status for you to complete an edit.




- 3 Click the **Edit**  icon. The **Schedule Edit** (for the job you selected) window opens.



- 4 At the Schedule Edit window, make any needed changes to the existing information, then at the **Schedule Job** portion of the window, make your selections for Submitting this job.
- 5 Click **Submit** when you have made your changes. You can click **Approve & Submit** if you have those permissions.

## Viewing and/or Updating Data Fields

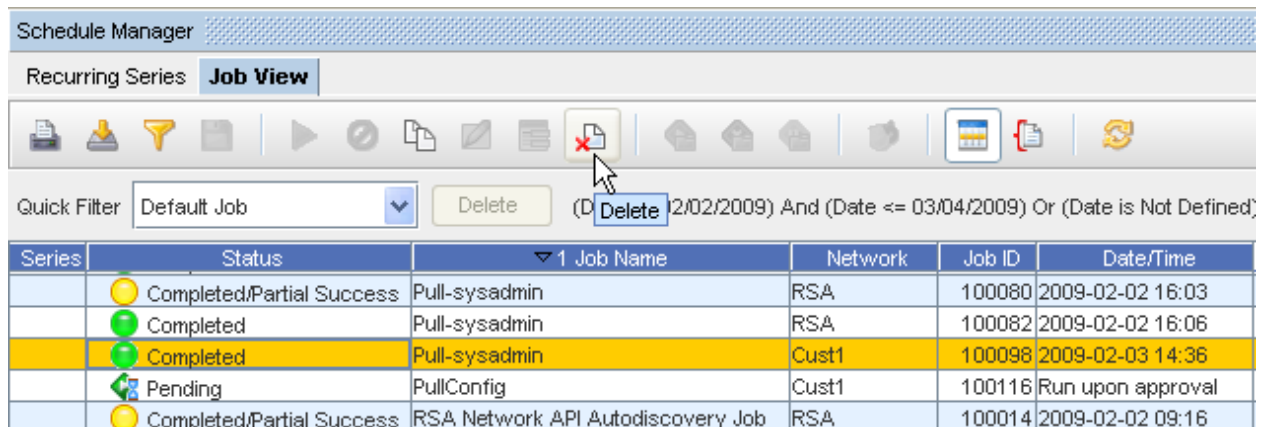
To view or update existing data fields,

- 1 From the menu bar, select **Tools - > Schedule Manager**.
- 2 On the **Job** tab, select a  job, and then click the **View and/or Update Data Fields** icon.
- 3 If data fields are present, you can then make any needed changes to them, or determine if you need to delete the data fields.



## Deleting a Job

Use the **Delete** icon (where applicable) to delete a job permanently from the Jobs list displayed in the Schedule Manager. You must have the correct permissions to complete a delete activity.



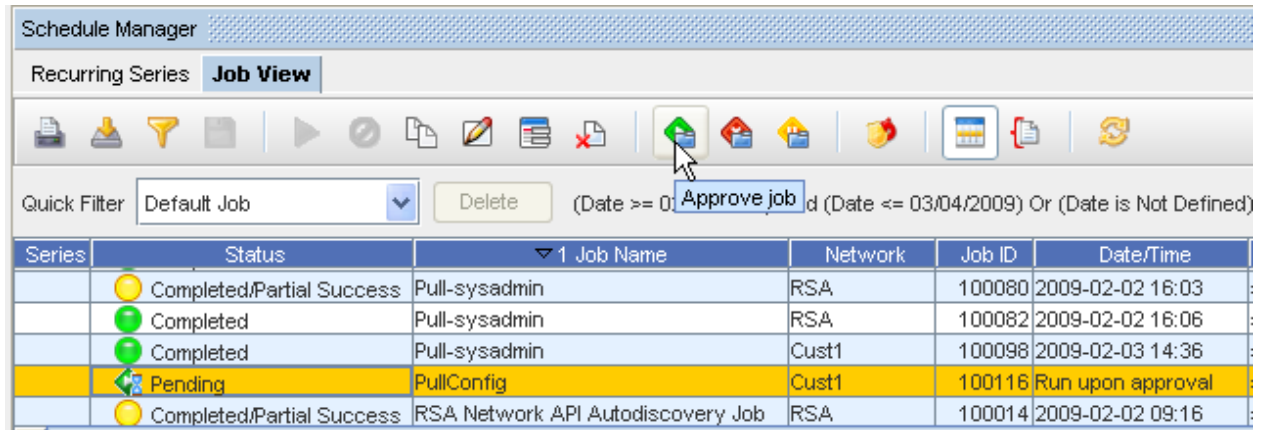
- 1 From the listing, **select the job** you want to delete.
- 2 Select the **Delete** icon from the tool bar.
- 3 Click **Ok** at the confirmation message.

## Changing the Job Status

If granted the appropriate permissions, you can change the status of an existing job.

- Review the listing of jobs within the Schedule Manager, and locate a job that is in **Hold or Pending status**.
- Highlight the job, then change the current status by selecting one of the options on the Schedule Manager tool bar. You can select:
  - Approve
  - Reject
  - Hold

**Approve**



**Reject**



**Hold**



**Note** Note that the Schedule Manager automatically refreshes whenever there is a change to a job.


## Jobs in the Hold Status

For jobs that are in the **Pending or Hold** status, you have several features available to assist you in getting these job details. You can select to Approve those jobs if you have the appropriate permissions, or reject those jobs.

## Schedule Manager (Override) Update Credentials


With this option, you have the ability to override the existing credentials for a job or other non-scheduled operations. Only those users with the **Override Credential** permissions are allowed to override the credentials.



- 1 From the listing, **select the job** you want to override and Update the Credentials on.
- 2 Select the  **Update Credentials** icon from the tool bar.
- 3 At the **Job Credentials Input** window, you must enter the appropriate information needed to update (override) the credential.
- 4 Click **Ok** when you have completed updating the credential.

**Note** Note that the Schedule Manager automatically refreshes whenever there is a change to a job.

## Job Details


- 1 From the Schedule Manager tool bar, use the **Details**  icon to show or hide the **Job details** section of the Schedule Manager window. Once clicked, the General and Task tabs display in the lower portion of the work area, along with the Result, History, and Content tabs offering even more job information on the job and tasks.



- 2 Clicked the icon once again, and the tabs (containing the job detail tabs) are no longer displayed.

## Reviewing Job/Status Summary

With the Schedule Manager displayed, you can select to review a Job/Status summary.

- 1 Select the **Summaries**  icon. The Job/Status summary information is presented in the left portion of the Schedule Manager window. This summary displays the total number of jobs, as well as the job count per status.



- 2 Click the **Summaries** icon again, to close this Job/Summary window.

## Refreshing a Job List

Once you have made changes to the existing list of jobs displayed in the Schedule Manager (for example, if you deleted jobs from the list), note that the Schedule Manager **automatically refreshes** whenever there is a change to a job.

You can also use the **Refresh**  icon to refresh the Schedule Manager.



## Working with the Data Field Manager

### Introducing the Data Field Manager

---

**Note** You must have System Administration privileges to work with the Device Data Fields. You must also have View Permissions to view the data fields information.

---

Data Fields are used to create attributes, and to assign values to devices.

- 1 From the **Tools** menu, select **Data Field Manager** .

Tools	Window	Help
Networks Navigation	F6	
Dashboard	F8	
Automation Library	F3	
Schedule Manager	F7	
QS Inventory	F9	
Event Manager	F11	
Data Field Manager		
Metadata	F12	
System Administration	F4	
EMC M&R		
Change Audit	Ctrl-U	
Global Device Search	Ctrl-S	
Single Device Auto Discovery		
Template Merge		
Change Password		
Change RSA Tokens PIN		

- 1 At the **Data Field Manager** window, you can complete the following tasks:
- 2 Add a new Data Field
- 3 Edit an existing Data Field
- 4 Remove a selected Data Field
- 5 Refresh the Data Field view

## Working in the Data Field Manager

---

**Note** You must have System Administration privileges to work with the Device Data Fields. You must also have View Permissions to view the data fields information.

---

Data Fields are used to create attributes, and to assign values to devices.





- 1 From the **Tools** menu bar, select **Data Field Manager** .



- 2 At the **Data Field Manager** window, you can complete the following tasks:
- 3 Add a new Data Field
- 4 Edit an existing Data Field
- 5 Remove a selected Data Field
- 6 Refresh the Data Field view

### Using the icons



Icon	Usage
	Add an additional data field
	Edit an existing selected data field
	Delete a data field from the list
	Refresh the view

## Adding a Data Field

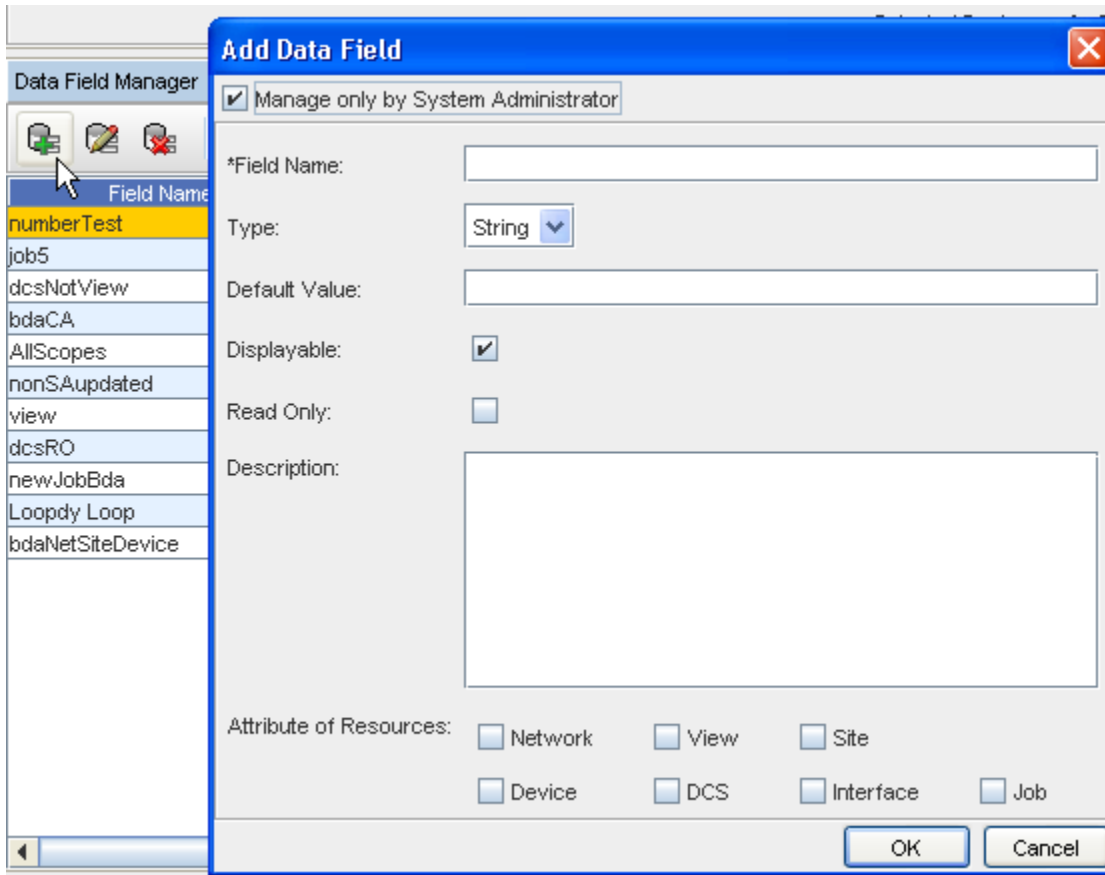
Data Fields are used to create attributes, and to assign values to devices.

- 1 From the **Tools** menu bar, select **Data Field Manager** .



Tools	Window	Help
Networks Navigation	F6	
Dashboard	F8	
Automation Library	F3	
Schedule Manager	F7	
QS Inventory	F9	
Event Manager	F11	
Data Field Manager		
Metadata	F12	
System Administration	F4	
EMC M&R		
Change Audit	Ctrl-U	
Global Device Search	Ctrl-S	
Single Device Auto Discovery		
Template Merge		
Change Password		
Change RSA Tokens PIN		

- At the **Data Field Manager** window, click the **Add** icon to open the Add Data Field window.



- Click the **Edit only by System Administrator** check box if you want this field to only be edited by the System Administrator.
- Enter a Field Name, and then use the drop-down to select a Type.
- Next, enter a **Default value**.

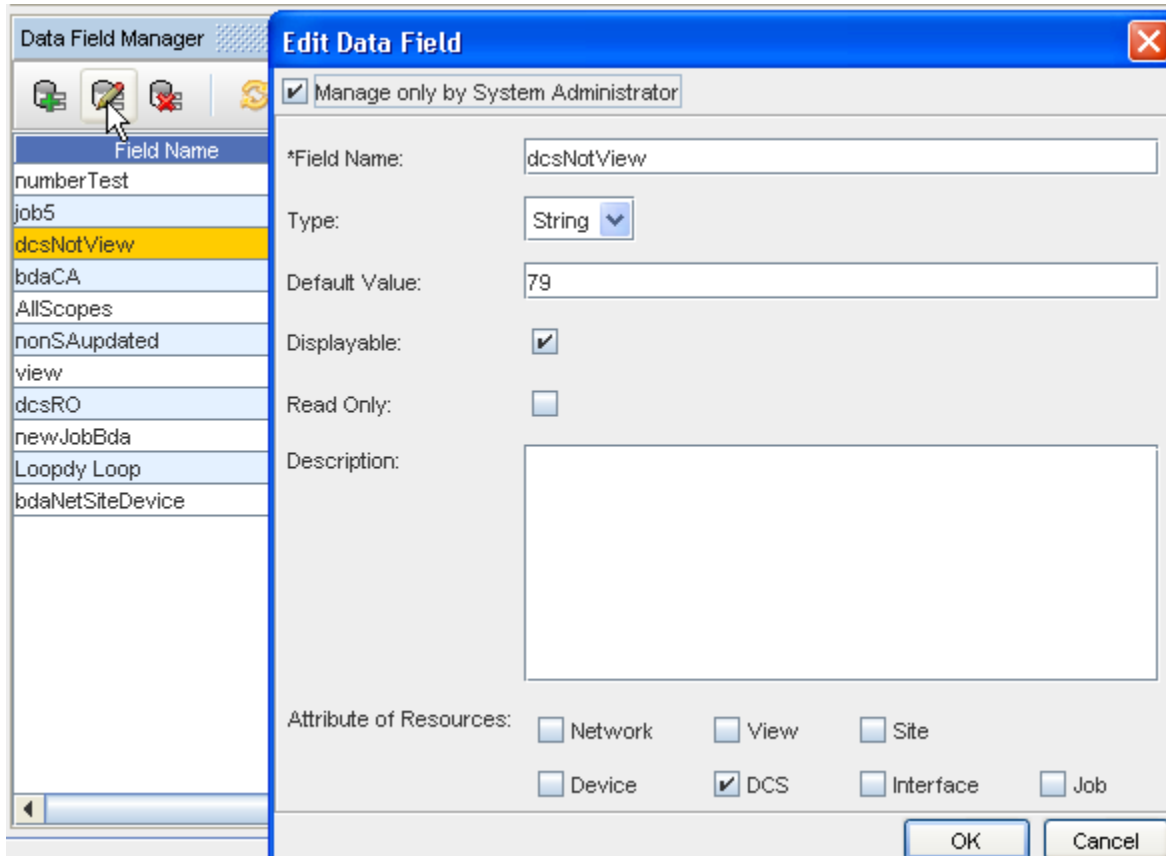
- 6 Click the check box if you want this field to be displayed (click **Displayable**).
- 7 Click the check box if you want this to be **Read Only**.
- 8 Select if this field is to be **Viewable** and/or **Editable**.
- 9 Enter a **Description** if needed.
- 10 Next at the Attribute of Resources portion of the window, check the appropriate check boxes where you want the Data Field to be associated with.
- 11 Click **Ok**.
- 12 The new data field is now added to the list of existing fields in the window.

## Editing a Data Field

- 1 From the **Tools** menu bar, select **Data Field Manager** .



- 2 At the **Data Field Manager** window, **highlight** the field you want to edit, then click the **Edit** icon to open the Add Data Field window.



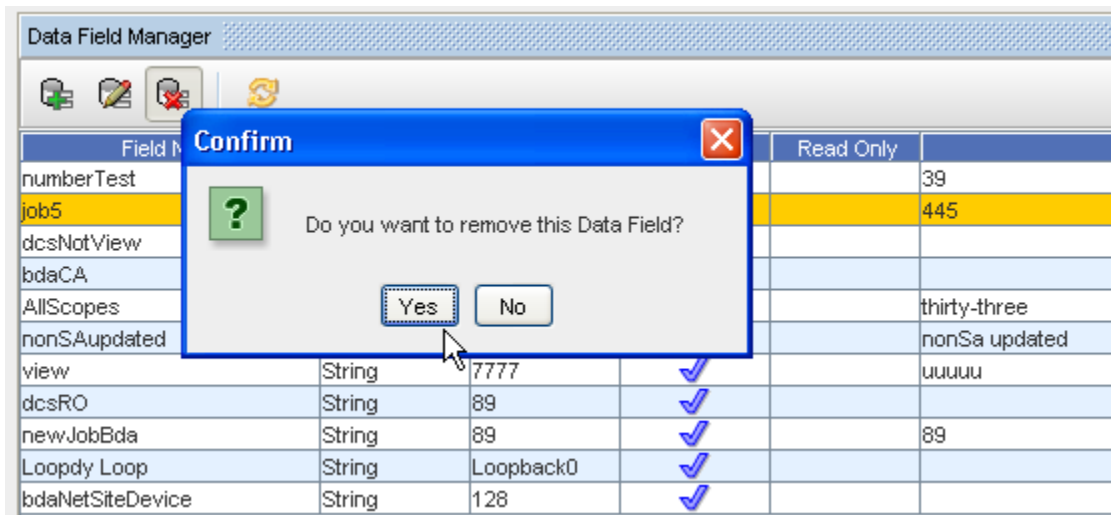
- At the Edit Data Field window, make any changes to the existing content, then click Ok. The field is now edited, and your changes are saved.

## Deleting a Data Field

Data Fields are used to create attributes, and to assign values to devices.

Tools	Window	Help
Networks Navigation	F6	
Dashboard	F8	
Automation Library	F3	
Schedule Manager	F7	
QS Inventory	F9	
Event Manager	F11	
Data Field Manager		
Metadata	F12	
System Administration	F4	
EMC M&R		
Change Audit	Ctrl-U	
Global Device Search	Ctrl-S	
Single Device Auto Discovery		
Template Merge		
Change Password		
Change RSA Tokens PIN		

- 1 From the **Tools** menu bar, select **Data Field Manager** .
- 2 At the **Data Field Manager** window, **highlight** the field you want to delete, then click the **Delete** icon.



- 3 Click **OK** at the confirmation message.

# SYSTEM ADMINISTRATORS - Getting Started

# 6

This chapter includes the following topics:

- Getting Started - System Administrator Tasks
- Getting Started - System Administration Overview
- System Administration Best Practices
- System Administration Tasks and Procedures
- System Administration User Rights
- Working with Global Settings
- Working with Network Settings
- Working with Networks
- Working with Devices (Devices View)
- Working with Sites
- Working with Views
- Working with Tools
- Working with the Schedule Manager
- Scheduling Jobs
- Working with the Event Manager
- Using the Command Line Interface (Bulk Import)
- Working with the DNS Wizard
- RSA

## Getting Started - System Administrator Tasks

As the **System Administrator**, you have the authority to grant user permissions and access to various tasks and views within the application.

The first task you may want to accomplish is **creating a Network** .

**See:**

[Working with Networks](#)

[Creating a New Network](#)

[Assigning Device Servers](#)

## System Administrators

Tasks to be completed by the System Administrator include:

- Working with the System Administration tools on a **Global** Level, including:
- Working with System Users
- Working with System Groups
- Working with Permissions
- Working with the RSA Token Viewer
- Working with Authentication Servers
- Working with Maintenance Windows
- Working with Device Classes
- Using the Diagnostic Tool
- Working with Networks
- Working with Devices
- Working with Sites
- Working with Views
- Working with the Schedule Manager
- Scheduling Jobs
- Working with the Event Manager
- Using the Command Line Interface
- Using Backup and Restore

## Getting Started - System Administration Overview

The System Administration module is where you complete tasks that affect system **Global Settings, Networks** , and **User Management**. This includes:

- Configuring Device Communication Mechanisms and Credentials
- Managing Device Servers, and Out-Of-Band Management Servers
- Managing Networks

- Managing Users and Groups
- Managing Credentials
- Defining Security policies between users, groups, and networks
- Associating Devices and Users to Networks
- Using the Command Line Interface (for bulk import)
- Managing Privilege Passwords
- Setting up Locking parameters
- Working with RSA Token Viewers

There are three types of users that are granted access to the System Administration module. They are:

- System Administrators
- Network Administrators
- User Administrators

**Systems Administration** functions are intended for access by any user that has been given NCM system administrator, network administrator, or user administrator privileges. The system administrator can create or delete networks, manage device servers and devices, create/edit system users, and create authorization policies between users, groups, and networks. System Administrators can see and alter information about any network in the NCM application.

**Network Administration** functions are limited to those networks to which you are assigned, or that you create. Network Administrators cannot see or manage any networks that they do not have specific permissions to access, manage users, groups, and network authorizations, or edit system global information.

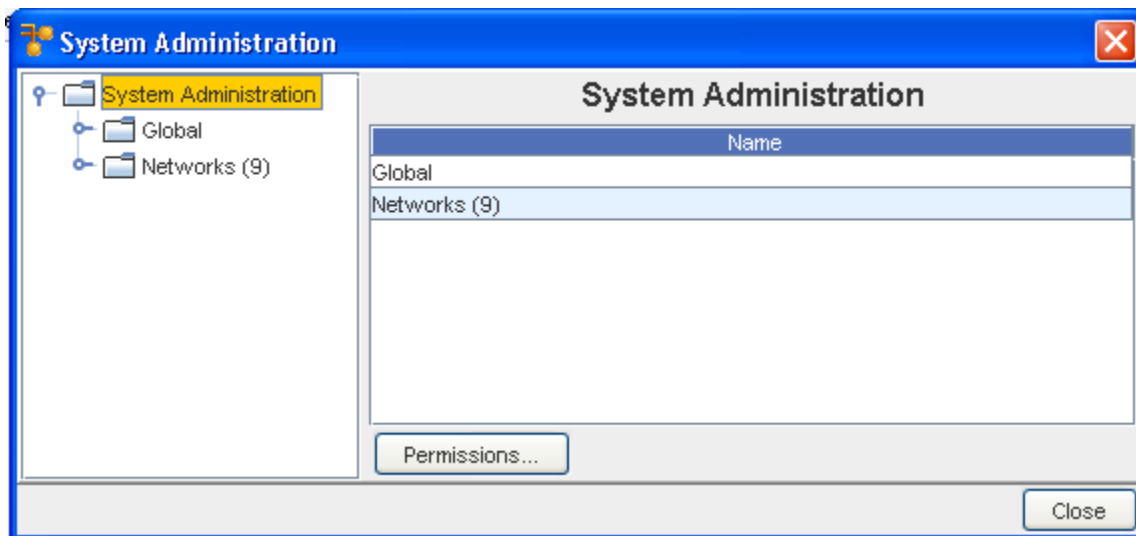
**User Administration** functions allow you to manage and create users and groups, and to associate users and groups to networks and devices by assigning authorization policies. User Administrators cannot manage networks, or edit system global information.

**To access the System Administration module:**

- 1 On the Menu Bar, click **Tools**.

Tools	Window	Help
Networks Navigation	F6	
Dashboard	F8	
Automation Library	F3	
Schedule Manager	F7	
QS Inventory	F9	
Event Manager	F11	
Data Field Manager		
Metadata	F12	
System Administration	F4	
EMC M&R		
Change Audit	Ctrl-U	
Global Device Search	Ctrl-S	
Single Device Auto Discovery		
Template Merge		
Change Password		
Change RSA Tokens PIN		

- From the list of Tools, select **System Administration**. The System Administration window opens.



From this opening view, you can expand on either **Global** or **Networks**.

For detailed information on both Global and Networks, go to:



## System Administration Best Practices

- Keep your list of managed device classes to the minimum of devices you want discovered in your network. Additional device classes in the managed device list causes unwanted devices to be discovered into your VoyencControl network, and extends the processing time of your auto discovery job. Use care when using the Generic Device class, as it can discover non-network devices, such as servers and client PCs.
- Always set up the appropriate credentials before executing any auto discovery jobs. This ensures all devices in your network are discovered appropriately, and their configurations are pulled successfully.
- Communication methods have different characteristics. For example, using SNMP/TFTP will not provide command failure notification in jobs, but this method is very fast. Raw SSH is secure, but much slower than using a less secure communication method like TFTP. A good compromise of speed and reporting, while not secure, is Telnet/TFTP.
- Minimize the number of credentials in your networks whenever possible to minimize the credential management process.
- For bulk updates, Command Line utilities exist to assist with modification of many credentials and communication methods.
- To avoid using auto discovery, Command Line utilities exist to assist with the loading of specific device IP's for management in VoyencControl.
- Keep in mind that the communication mechanisms you choose are only used between the device server and the end device. Communications between your client and the VoyencControl application, and the device server can be encrypted, and thus secured, regardless of the "last mile" protocol to the device.

## System Administration Tasks and Procedures

Within this section of the Network Configuration Manager Online User's Guide, you can access the following System Administration Tasks and Procedures.

- [Global Settings Overview](#)
- [Network Settings Overview](#)
- [Diagnostic Tool Overview](#)
- [Locking and Unlocking Users](#)
- [Device Servers Overview](#)
- [Proxy Functionality](#)
- [SNMP Support](#)
- [Out-of-Band Servers Overview](#)

- [Credential Settings Overview](#)
- [Device Class Management Overview](#)
- [Maintenance Window Overview](#)
- [User Management Overview](#)
- [Creating Groups](#)
- [Creating Users](#)
- [Setting Network Level Permissions](#)
- [Authentication Servers Overview](#)
- [NAT Configuration - Overriding Device Server IPs](#)
- [Using the Command Line Interface](#)
- [RSA Tokens Overview](#)

## System Administration User Rights

The following details the user rights within Network Configuration Manager, and the details of each permission.

---

**Note** The information noted here may not include all permissions.

---

### At the Network Level:

Permission	Permission Details
Manage User Access	Add/Remove users to the Network/Device Level permissions
Manage Templates	Add/Delete/Edit Templates (non-Global)
Manage Compliance Standards	Manage non-Global Automation Library entries
Network Edit	View Device Servers, Maintenance windows, IP Address Pools, Auto Discovery, Network Level Credentials, Device Classes, Device manage
Network Delete	Delete the selected Network
Network View	View Network from the Main window, receive Reports
Workspace Create	Create a Workspace view
Workspace Edit	Edit the Workspace view
Workspace View	View the Workspace from the Main window
Device Create	Create a Device in a Network

Permission	Permission Details
Device Edit	Disable mode Cut-through, saved commands, resync, and Quick Commands
Device View Details	Show tab information in the Properties tab, run Report
Device View Passwords	Enable mode Cut-through, Bulk Import Credentials
Device Update Operating System	Update the Device Operating System
Job Schedule	Network level Schedule jobs (overrides the System Level job Schedule)
Job Approve	Network level Approve/Cancel jobs (overrides the System level job Approval)
View Create	Create a custom View for a Network
View Edit	Required to View the Custom views
View Delete	Delete custom Views for the Network

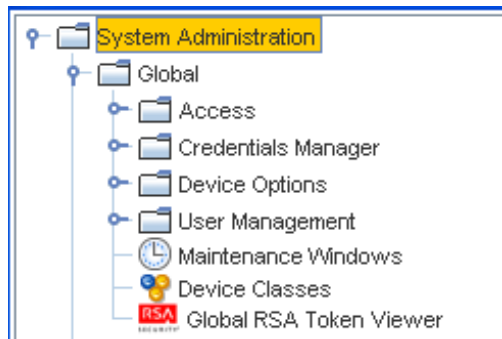
## System Permissions:

Permission	Permission Details
Manage User/Groups	Administrates Users and Groups
Manage User Access	Can change Permissions for Users/Groups
Manage Templates	Can manage Templates
Manage Compliance Standards	Can manage Compliance Standards
Manage OS Inventory	Can manage OS Inventory
Network Create	Create new Network (cannot assign Device Servers)
Job Schedule	Schedule jobs in all Networks with Network rights
Job Approve	Approve jobs in all Networks with Network rights
System Administration	Allows Global Credential access, Manage Global Automation Library, Bulk Import Credentials

## Working with Global Settings

### Global Settings Overview

The following example shows the **Global** branch of the tree menu expanded in the left frame. When selected from the tree menu, the contents for each branch display in the right frame.



The System Administration window has a traditional two frame view. On the left in the Navigation Pane are the entry points to the major sections of the System Administration module, including:

- Global
- Access - which can be expanded to include:
  - Device Servers
  - File Servers
  - Out-of-Band Servers
  - NCM RSA Token Service
- Credentials Manager
  - Credentials
  - Credentials Configuration
- Device Options - which can be expanded to include:
  - Device Naming Update
  - Device Naming Scheme
  - Device State Options
- User Management - which can be expanded to include:
  - System Users
  - System Groups
  - Authentication Servers - which can be expanded to include:
    - Native Registry
    - TACACS+
    - RADIUS
    - LDAP
- Maintenance Window
- Device Classes

- Global RSA Token Viewer

---

**Important** For information on **Lock Management**, see your system administrator.

---

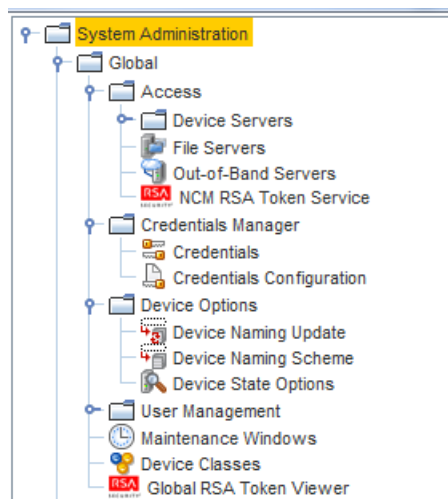
Within the above components, you are able to complete the following tasks:

- Determine which device servers are associated with your network
- Configure any out-of-band servers
- Set which devices are automatically managed by Network Configuration Manager when Auto Discovery runs
- Configure cross network shared and local credentials
- Add, edit, and delete Data Fields
- Designate Device Names that will be consistent throughout their system
- Manage server properties
- Manage users and groups, and their network permissions
- Manage the Authentication Servers, and determine user security
- Complete Maintenance on Windows
- Work with Global RSA Token service and viewers

## Global - Access

### Access Overview

From the **Global** view of the System Administration window, you can select **Access** to then view the Device Servers, Out-of-Band Servers, and RSA Token Servers.



### Global - Device Servers

## Device Servers Overview

Device Servers are created at the time of installation, and display in the **Device Server** folder in the tree menu.

Device Servers contain the devices that are used by your networks. For devices to be associated with networks, the device servers on which they reside, must be associated to the network.

The Device Server Administration screen is used to configure aspects of each device server in your system. Typically, the Network Configuration Manager application is deployed with a single applications server, and one or more Device Servers setup to monitor your network. Each Device Server has a set of devices associated with it, and all device communication occurs between the Device Server and the device.

The Application Server will never talk to a device directly, communication is done via the assigned Device Server.

There are properties of the Device Server that can be edited. A Device Server's properties are edited in two ways:

- [Edit Device Server](#)
- Editing device level defaults

### Device Server Properties - System Administration

To select the appropriate Device Server Properties at the Global Properties level, go to [Device State Options](#) information.

### Device Server Log

A Device Server log has been created that allows you to keep a log of the credentials that have been successfully changed. There is one log per Device Server. This log is encrypted.

To view the log,

- 1 At the Device Server, go to **\$VOYENCE\_HOME/tools**.
- 2 Next, enter **/view credchanges**.

### Device Server Details

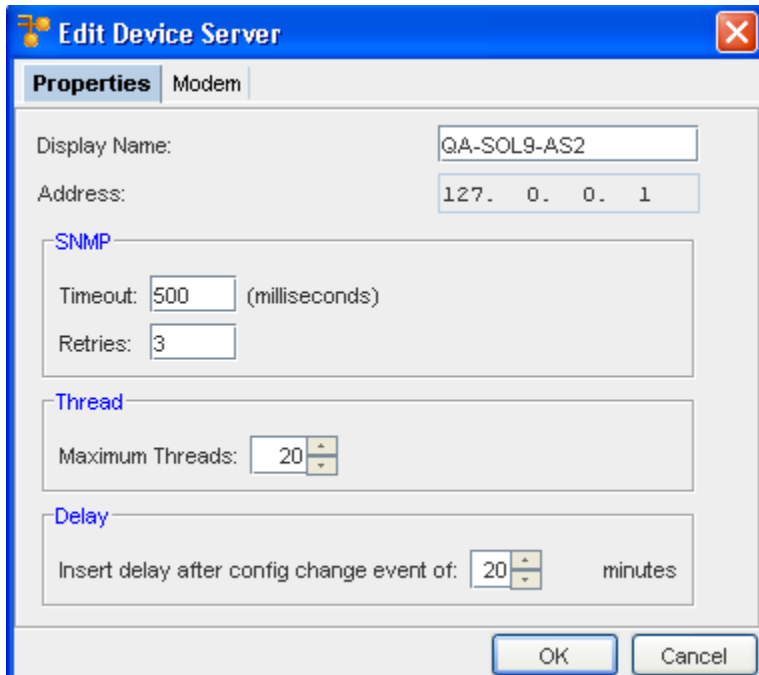
To access the device server details,

- 1 In the Network Configuration Manager menu bar, select **Tools**.
- 2 From the menu options, select **System Administration**. The System Administration window opens.
- 3 On the tree menu, expand the **Global** -> **Access** folders.
- 4 Open the **Device Sever folder** . At a minimum, at least one Device Server is available.



The basic properties of the Device Servers are listed on the right. Except for the number of the devices on the Device Server, these details can be edited on the Properties tab.

- To access the **edit feature**, - in the right pane, select a **Device Server**, then click **Edit**. Or... - in the navigation pane, expand the **Device Server folder**, then select the **Device Server**. The right pane refreshes. Click **Edit**. The **Edit Device Server** window opens.



Once accessed, you are able to edit the **Edit Device Server** tabs of the device server.

**Note** For more details on the Device Servers, contact [Customer Support](#).

### Device Servers Best Practices

Best Practices are methods of completing tasks, or tips that should be used based on a typical scenario.

When managing Device Sever configurations you should use the following best practices tips:

- If your devices have spotty SNMP communications (due to device busy failures or other network traffic issues) set the retry count **higher** to compensate. To avoid unnecessary delays, you may want to set your timeout value **lower**.
- If your devices reliably send SNMP responses, then set the retry count to 0 or 1, but make sure to set the timeout value **higher**. This ensures reliable delivery of SNMP traffic in this environment.
- Setting your timeout and retry values too high causes long hangs and delays when devices physically are not responding.
- Setting your timeout and retry values too low causes successful SNMP communication to appear as though it has failed.
- If you typically send jobs to large numbers of devices simultaneously, setting the Maximum Threads configuration variable to a **higher** value allows your job to complete quicker.
- If you are worried about network or device traffic and Device Server performance, but are not concerned as much about the total length of time a large job takes to execute, then set the maximum threads to a **smaller** value.
- It is recommended to never set the maximum threads value to a value less than 5. Doing so could cause serious application performance degradation.
- To set the maximum threads value to a number greater than 20, carefully monitor the CPU, memory and disk performance of the Device Server to make sure you are not overloading the system. At peak times with maximum threads set high, system delays could cause thrashing and an overall performance degradation, along with an increase in timeout and related errors.
- Decreasing the config change delay increases the responsiveness the system has to changes in the system, at the potential cost of a larger number of revisions being stored when multiple changes are happening simultaneously. This can easily happen when a user is interactively changing the configuration on the device itself.
- Increasing the config change delay decreases the number of revisions being stored when multiple changes are happening simultaneously, but causes an increase in the delay before a changed configuration is stored in the repository.

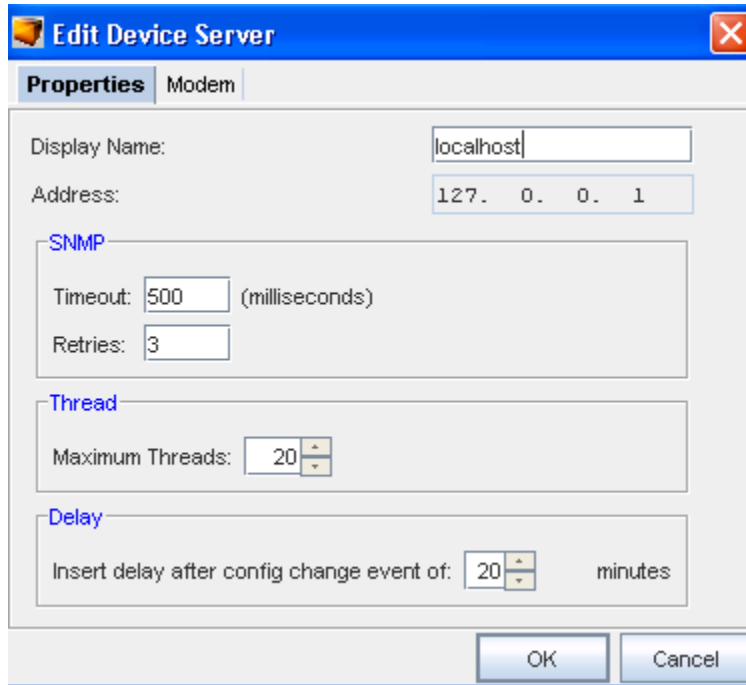
## Edit Device Server

Device Servers provide the control and communications for all network devices. Each device server has settable properties, including SNMP timeouts and retries, multi-task thread count, and external config update pull delay.

If a device server contains an internal modem for use in out-of-band communications, it can be configured here.

Once you have [Device Servers Overview](#), you can:





- Edit the Device Server Properties
- Edit the Modem properties for connecting to the device server
- Change the status of a device
- Edit the device credentials
- Edit device level defaults

There are two sections in the Device Server properties that can be edited:

- **Properties** - edits the name, address, SNMP, Thread and Delay details of the Device Server
- **Modem** - edits the modem communications details when connecting to the Device Server via modem

### The Properties Tab

The Properties tab contains the following SNMP configuration details.

Field	Description
<b>Display Name</b>	The name which identifies the Device Server. Appears in many spots within the application when the Device Server is being referenced.
<b>Address</b>	The IP Address of the Device Server. The IP Address cannot not be edited.

**SNMP  
Timeout/  
Retries**

This sets the default SNMP timeout and retry parameters for this Device Server. Timeout is the amount of time, in milliseconds, that SNMP probes before timing out. Retries is the number of attempts that are tried.

**Notes:**

- Guidelines for SNMP timeouts are relative to the speed and load of network resources. The following table has been provided for rules as to how to set SNMP timeout and retry parameters on the device server.
- In general, low **timeouts** make the network work harder, and applying low timeouts to an already stressed network increases failures. Low timeouts and high retry counts should only be used on fast networks with underutilized devices.
- Higher **retries** with a low timeout is not suggested, as devices can be overwhelmed by the queue of incoming requests, and can actually make a system worse.
- Higher rates of success can be achieved by increasing both retries and timeouts together.

Network Type	Network Speed/Response Time (ping)	Device Usage/User perception	Retries	Timeouts
Fast	< 10 ms	<ul style="list-style-type: none"> <li>■ Quick response</li> <li>■ low utilization</li> <li>■ 500+ kb/sec</li> </ul>	Low 1-3	Low 10 ms - 300 ms
Medium	10-15 ms	<ul style="list-style-type: none"> <li>■ Sometimes slow response</li> <li>■ low utilization</li> <li>■ &lt;500 Kb/sec</li> </ul>	Medium 3-5	Medium 300-1000 ms
Slow	> 50 ms	<ul style="list-style-type: none"> <li>■ Often slow data transfers and response times</li> <li>■ &lt;300 Kb/sec</li> </ul>	High 5-10	High 1000-3000 ms

**Threads**

This is the **maximum** number of simultaneous activities this Device Server can complete to separate devices allowed. Typically, multiple actions to a single device are executed sequentially, but actions to multiple devices can be executed concurrently.

This value specifies the maximum number of simultaneous activities that are allowed. Setting this value lower slows down large block transactions. Setting this value higher increases the load on the device server. The default value is 20.

**Delay**

This specifies the number of minutes to wait after a configuration change has been detected before pulling a new configuration. Typically, when a change to a device occurs, often several changes occur within a short period.

This delay allows all of these changes to result in a single new configuration stored in the repository. Setting this value lower results in multiple configs being stored in rapid succession. Setting this value higher results in a delay when a changed config is reflected within the system.

To edit the Properties tab (on the Edit Device Server window),

- 1 On the Properties tab, if needed, enter a new **Display Name**.
- 2 Under **SNMP**:
  - Enter the **Timeout** in milliseconds, before each SNMP probe times out.

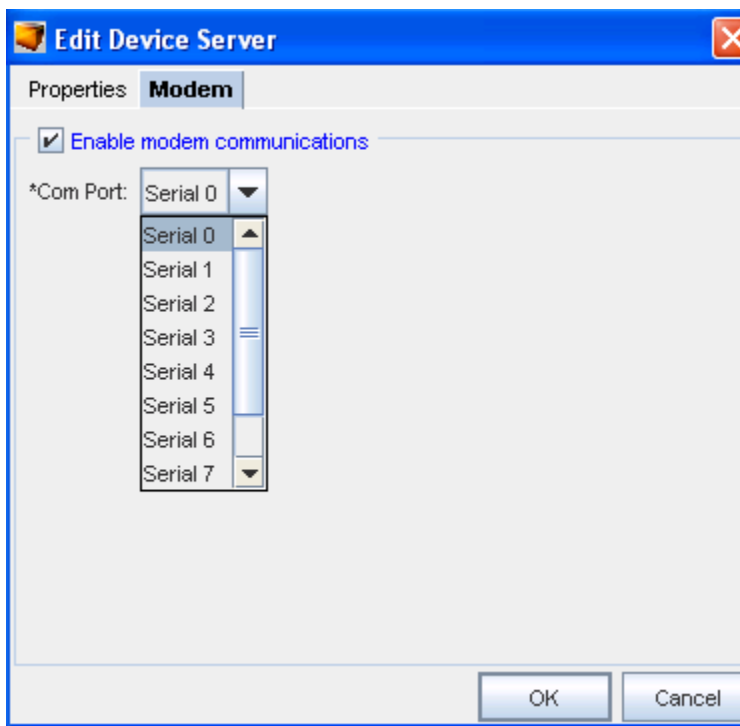
- Enter the number of **Retries** that the system will retry after each timeout.
- 3 Under **Thread** , enter the number of **Threads** if less than the maximum.
- 4 Under **Delay**, enter the time in minutes.
- 5 Click **OK** to save your changes.

### The Modem Tab

The Modem tab allows you to set the communications details for when a modem is used to communicate with the Device Server. For the modem to be used, the Enable modem communications check box must be checked.

To edit the Modem tab,

- 1 Select the **Modem tab** .



- 2 Select to **Enable Modem Communications** by clicking the check box.
- 3 Once selected, click the drop-down arrow, and select the **Communications Port** (Com Port) from the list.
- 4 Click **OK** to save your choices.

## Global - Devices

### The Devices

All the devices associated with each Device Server (managed by) can be viewed from the Devices option. From this view, you can unmanage devices that are in an unclassified state, permanently remove unmanaged devices, reassign device servers, and locate devices in their networks.

Devices live in one of three states; Managed (associated with networks), Unclassified (not in any networks, but kept as objects, or Unmanaged (discovered, but unimportant).

System Administration						
Devices (58)						
Discovered Name	Discovered FQDN	Type	State	IP Address	Device ID	
r2501-1	r2501.lab.voyence.c...	Cisco IOS Router	Managed	10.6.231.3	1001	
r3810-2	r3810-2.lab.voyence...	Cisco IOS Router	Managed	10.6.226.16	1002	
r2514-2	r2514-2.lab.voyence...	Cisco IOS Router	Managed	10.6.226.133	1003	
r2511	r2511-1.lab.voyence...	Cisco IOS Router	Managed	10.6.226.2	1004	
2502-2	r2502-2.lab.voyence...	Cisco IOS Router	Managed	10.6.226.134	1005	
Cisco2950	cat2950-1.lab.voyen...	Cisco IOS Switch	Managed	10.6.226.8	1006	
r2502-1	r2502-1.lab.voyence...	Cisco IOS Router	Managed	10.6.226.138	1007	
SmartInt	voyenceM71.lab.voy...	Juniper	Managed	10.6.226.11	1008	
ns5GT	ns5gt-wlan.lab.voye...	Netscreen	Managed	10.6.226.9	1009	
ns208	ns208.lab.voyence...	Netscreen	Managed	10.6.226.10	1010	
Cat3550	Cat3550.lab.voyenc...	Cisco IOS Switch	Managed	10.6.224.68	1011	
r3640-1	r3640-1.lab.voyence...	Cisco IOS Router	Managed	10.6.224.129	1012	
cat5500	cat5500.lab.voyenc...	Cisco CatOS Swi...	Managed	10.6.224.130	1013	
HP 4000	HP4000.lab.voyence...	HP Procurve Swi...	Managed	10.6.224.69	1014	
r3640-3	r3640-3.lab.voyence...	Cisco IOS Router	Managed	10.6.224.133	1015	

## Changing the Device Status

Once devices are located, devices are classified in the following states:

<b>Managed</b>	Indicates devices that are associated with networks. Managed devices reside in the central repository, and are under the control of authorized network users. Users can be assigned permissions at the device level related to what actions (tasks) the user is able to complete on the managed device.
<b>Unmanaged</b>	Indicates devices that are discovered, but are flagged, so that they are not repeatedly rediscovered in subsequent auto discovery runs
<b>Unclassified</b>	Similar to Unmanaged devices, except these devices have not been designated as Managed or Unmanaged. By default, all devices are Unclassified until located and associated to a network.

Prior to assigning devices to networks, you can select devices that are Unclassified, and classify them to Unmanaged.

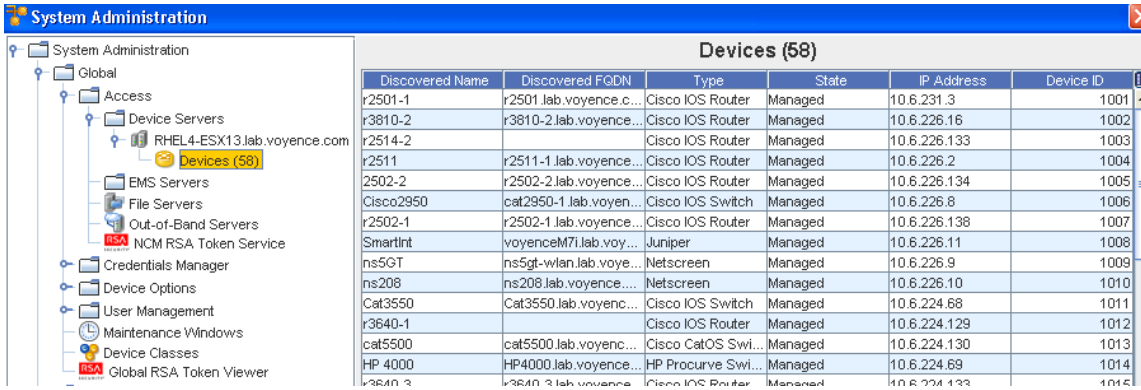
- When a device is classified as an **Unmanaged** device, the state of the device cannot be reversed to Unclassified, unless your network is the only network controlling the device.
- When a device is being managed by other networks, although your network is no longer controlling it, it will not be released to the **Unclassified** state unless released by all networks.
- If a device is managed by your network only, when you remove the device from your network, it's state is then re-classified to **Unclassified**. See [Managing Network Devices](#) for more information on assigning devices to networks.

**Important** When Unmanaged devices are discovered, they can be flagged because:

- They will not be used by networks
- The system does not need to continually acknowledge them during auto discovery

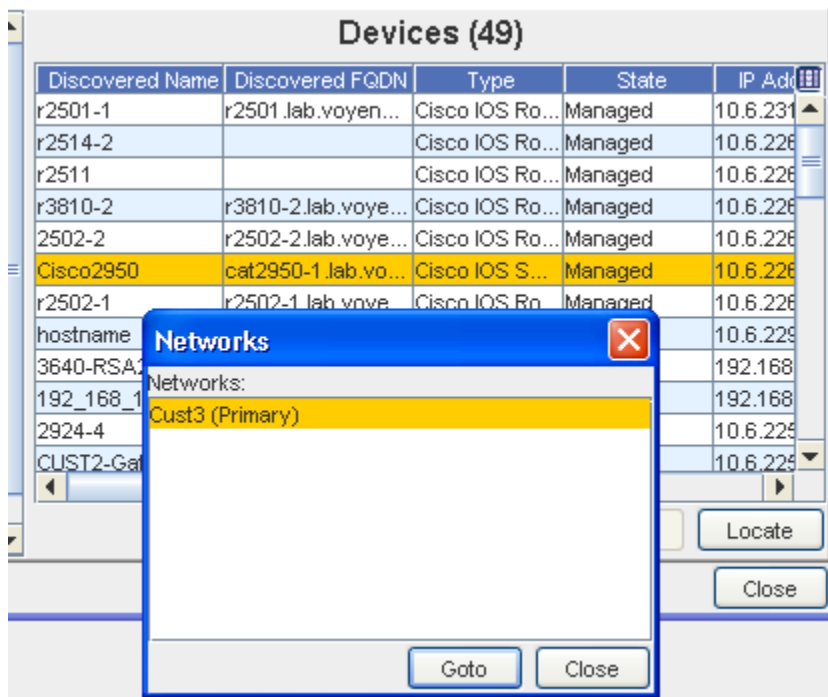
To set devices as unmanaged in a network,

- 1 In the **System Administration** window, expand the **Global** tree menu and navigate to **Device Servers**.
- 2 Select the **name of the Device Server** where the device you are looking for resides.
- 3 Click **Devices**.



The devices within the Device Server display in the right frame. Listed devices can be sorted in ascending or descending order, by Name, Type, State, or IP Address.

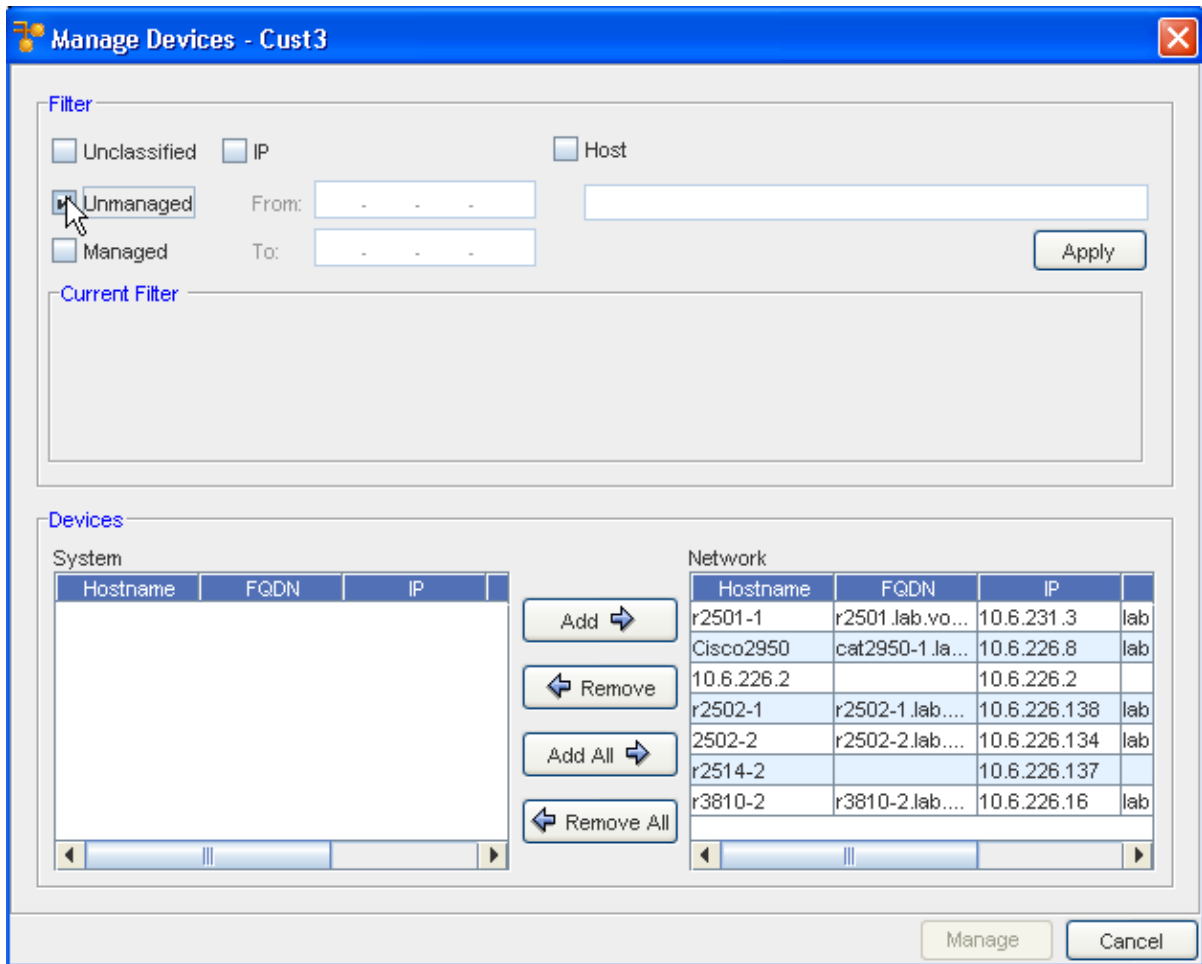
- 4 Select a device, then click **Locate**. The Networks window opens.



- 5 Select the **Network**, then click **GoTo** to get to the next Devices window.

Devices				
Device Name	Type	IP Address	Primary Network	Device ID
ciscoasa	Firewall	10.6.224.71	Cust1	1019
Pix-501	Firewall	10.6.224.3	Cust1	1020
rsm	Router	10.6.224.131	Cust1	1022
r3640-1	Router	10.6.224.129	Cust1	1012
r3640-3	Router	10.6.224.133	Cust1	1015
Cust1-GW	Router	10.6.227.193	Cust1	1017
Bay-city	Router	10.6.229.18	RSA	1023
cat-3524	Switch	10.6.224.66	Cust1	1018
Cat3550	Switch	10.6.224.68	Cust1	1011
cat5500	Switch	10.6.224.130	Cust1	1013
HP4000	Switch	10.6.224.69	Cust1	1014
Nortel-450	Switch	10.6.224.76	Cust1	1016
cat2924-2	Switch	10.6.224.132	Cust1	1021

- 6 From this window, click **Manage (under the Filter section)**. Note that you can also access and change Permissions, and change the Primary Network from this window.
- 7 From the Manage Devices window, select the new status check box (by clicking inside the appropriate check box; Unclassified, **Unmanaged**, or Managed). You can select if the Device is IP or Host as well.
- 8 Click **Apply**. The State of the device, now displayed in the original Devices view, is reclassified as Unmanaged.



**Important** You can remove devices from the Network by selecting the Device in the Network section, then using the Remove button to move them into the System pane. You can also Add any existing System Devices into the Network pane.

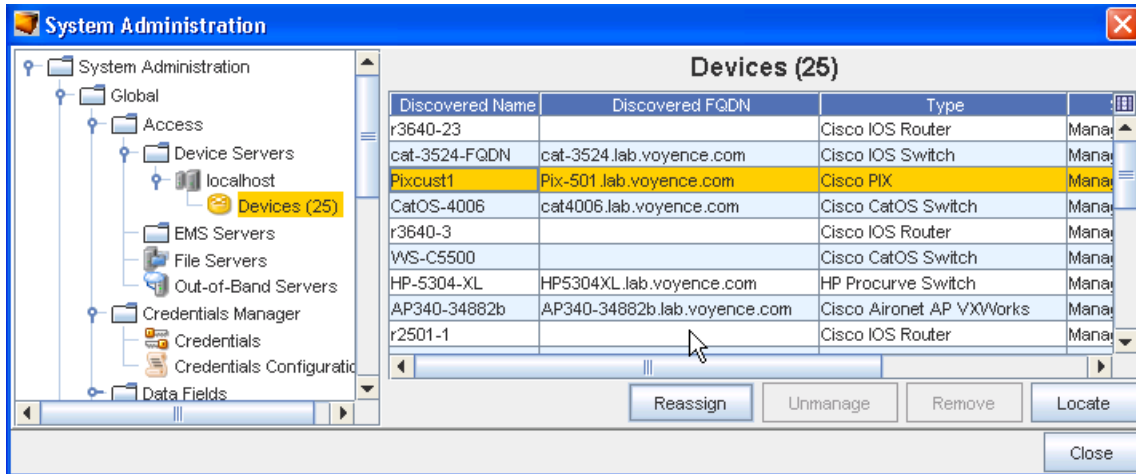
- 9 You must **Refresh** the view to access the Devices view and see your Unmanaged Devices listed.

### Reassigning Devices to Another Device Server

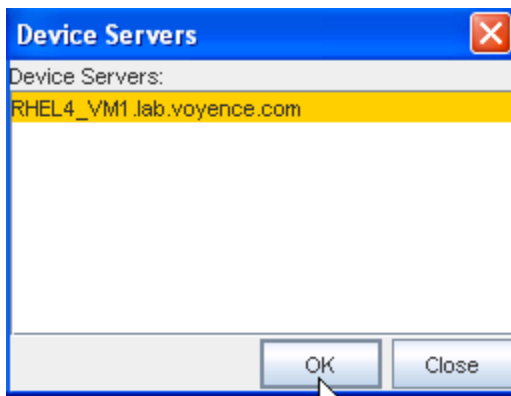
**Note** You must have at least two different **Device Servers** to reassign a device, or a number of devices, from one server to another.

To reassign a device to another device server,

- 1 In the **System Administration** window, expand the **Global** tree menu and navigate to **Device Servers**.
- 2 Select the **name of the Device Server** where the device you are looking for resides.
- 3 Click **Devices**.



- From the listing of devices, select the **device** (or any number of devices) you want to reassign to another Device Server, then click **Reassign**.
- From the list of Device Servers displayed in the Device Servers window, highlight the appropriate **Device Server** you want your selected devices to be reassigned to, then click **OK**.



- You can now verify the reassignment to make sure your devices are now listed under the Device Server you selected as the Reassigned Device Server.

## Global - File Servers

### File Servers Overview

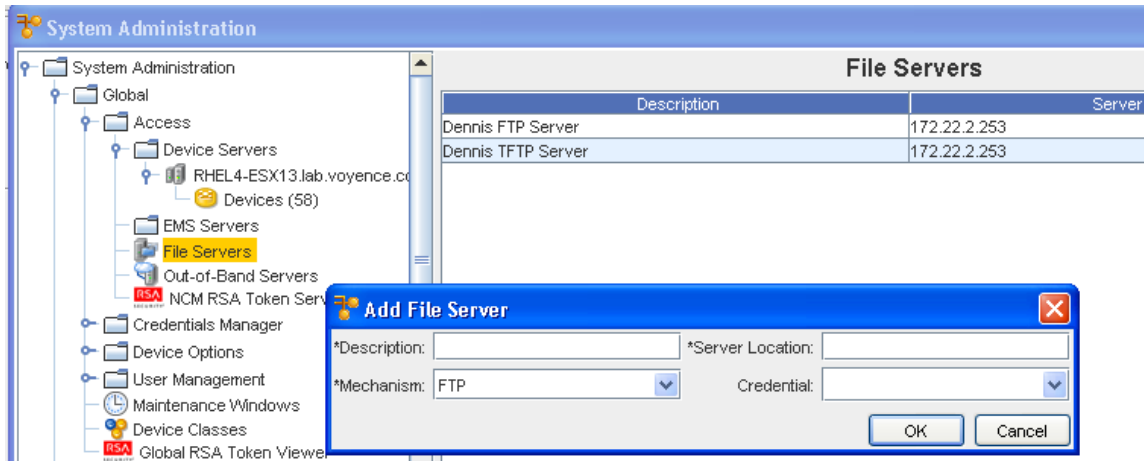
File Servers define the properties of any OS Management servers in your network. File Servers can be TFTP or FTP Servers. A File Server acts as the storage location for all Network OS images for your network devices.

Credentials can be used to define User ID and Password information for FTP Servers. A Network Configuration Manager Device Server can be configured to act as a TFTP image server.

The Device Server Properties window is available from:



Tools -> System Administration -> Global -> Access -> File Servers



From this window, you can Add, Edit, or Remove File Servers.

To Add a File Server,

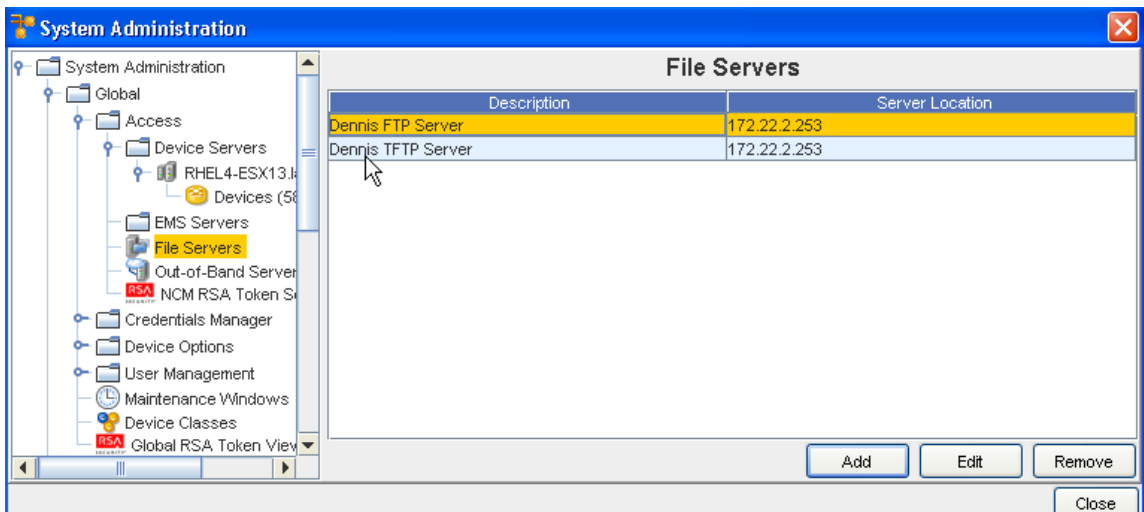
- 1 From the File Servers window, click the **Add** button.
- 2 Enter the **Server Name** and **Server Location** , then using the drop-down windows, complete the remaining needed information.

**Note** Selecting FTP or SCP from the \*Mechanism field activates the Credentials field, where you can then select a Credential from the drop-down window.

- 3 Click **Ok**.

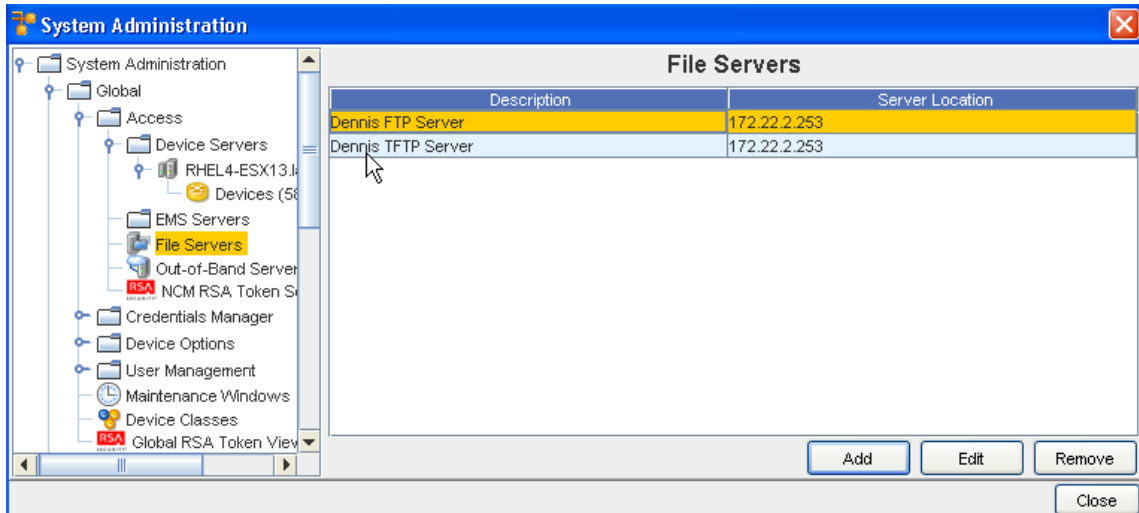
**Edit a File Server**

- 1 From the File Servers window, select an existing File Server, then click **Edit**.
- 2 Make any changes to the existing information within the Edit File Server window, then click **Ok**.



## Remove File Server

- 1 From the File Servers window, select an existing File Server, then click **Remove**.



- 2 At the confirmation message, click **Ok**.

## Global - Out-of-Band Servers

### Out-of-Band Servers Overview

Out-of-Band management of devices is a method to access a device when the primary management path is not available. Out-of-Band (OOB) Servers provide for direct console or AUX connectivity to your devices.

The servers that can be configured include, Modem Banks and Term Services. Both OOB server types support sever authentication.

Phone numbers and port information for each device is set within the device properties Communications tab.

Network Configuration Manager provides an option for setting up *alternative communication methods* using out-of-band servers.

For example, if there is a problem with a device and traffic cannot flow through the network, an *alternate path* can be set using a terminal server to reach the network nodes--even when the network is down.

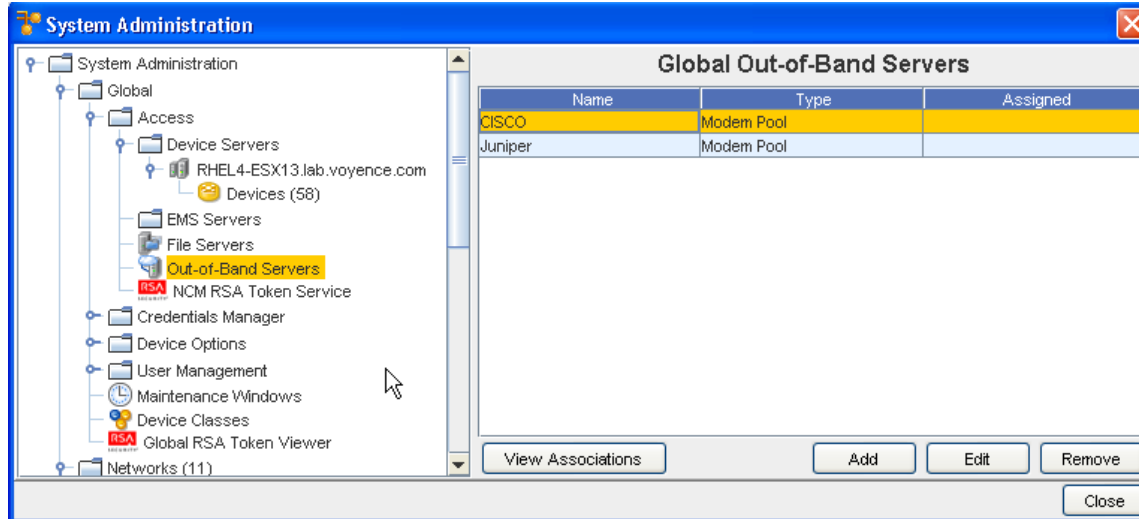
Out-of-Band servers are used when you need a secure, remote, emergency network access path to manage and troubleshoot device issues when:

- The device is not on the network
- The device is not network manageable
- The network is down

Network Configuration Manager allows you to set up out-of-band servers at two levels:

- Global level
- Network Level

**Global level out-of-band servers** allow you to set up access to out-of-band servers that can be used by any network being managed using Network Configuration Manager.



When you have configured an out-of-band server for a network, the network defaults to use the network level out-of-band server, unless otherwise indicated.

### Adding an Out-of-Band Server

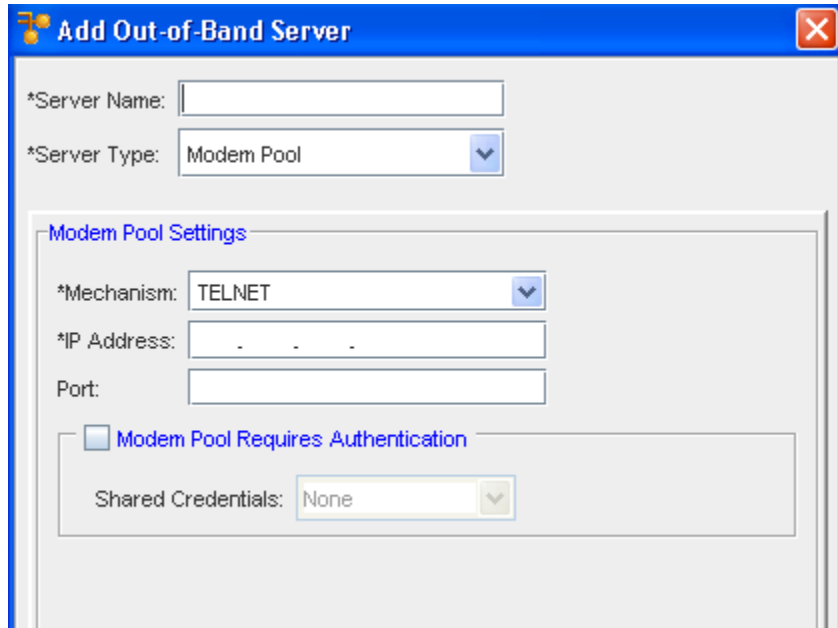
---

**Note** An out-of-band server can be configured at the Global or Network Level.

---

To access the Global level set up,

- 1 In the menu bar, select **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Global**, then the **Access** folders.
- 3 Click **Out-of-Band Servers**. The Global Out-of-Band Servers window opens in the right pane.



To add an Out-of-Band Server,

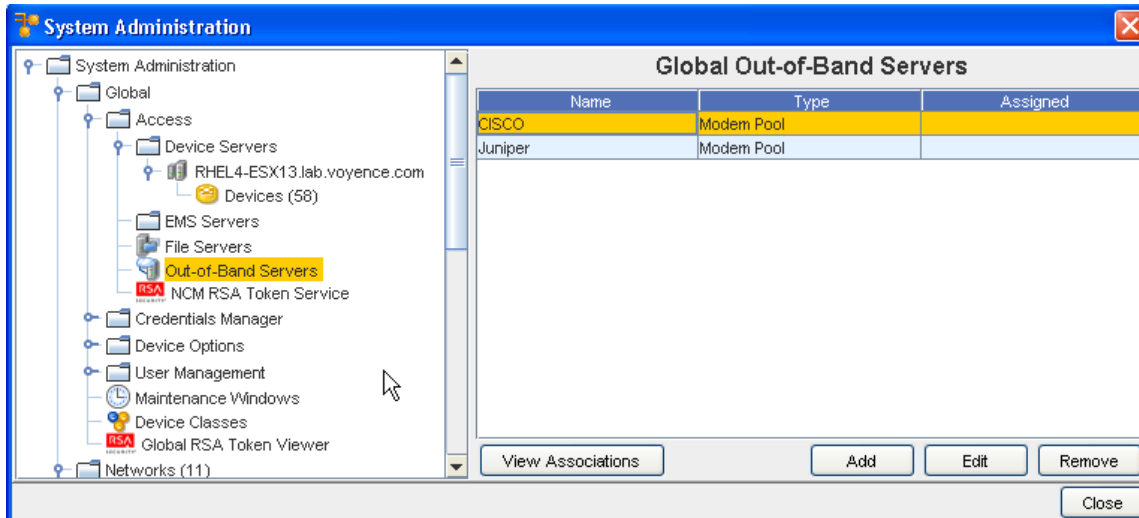
- 1 Click **Add**. The Add Out-of-Band Server window opens.  
The following fields are available. Note that the required fields are identified by an asterisk (\*).
- 2 Complete the setup of the out-of-band server options, as needed.
- 3 When finished, click **OK**. The Add Out-of-Band Server window closes.

Field	Description
Server Name	The name of the server being used for out-of-band access
Server Type	The type of server being used. Current options: - Modem Pool Settings - Terminal Settings
Modem Pool Settings	Based on the selected server type, the available fields are:
Mechanism:	Telnet or SSH
IP Address:	IP address used for connection
Port:	The <b>Modem Pool Requires Authentication</b> check box should only be used if you have configured a User name and Password access security in Shared Credentials. You can also select from the listing of <b>Shared Credentials</b> using the drop-down arrow to see the list.

The configured out-of-band server is listed in the Out-of-Band Server window.

### Editing an Out-of-Band Server

- 1 Select a Server from the listing in the **Network Out-of-Band Servers** window, then click **Edit**.



The Edit Out-of-Band Server window opens.

- 2 Make any changes needed to the existing information, then click **Ok**.

### Deleting (Removing) an Out-of-Band Server

If you have configured an Out-of-Band Server to be used by a device, you will not be able to communicate with the device using this configuration once the Out-of-Band Server is deleted.

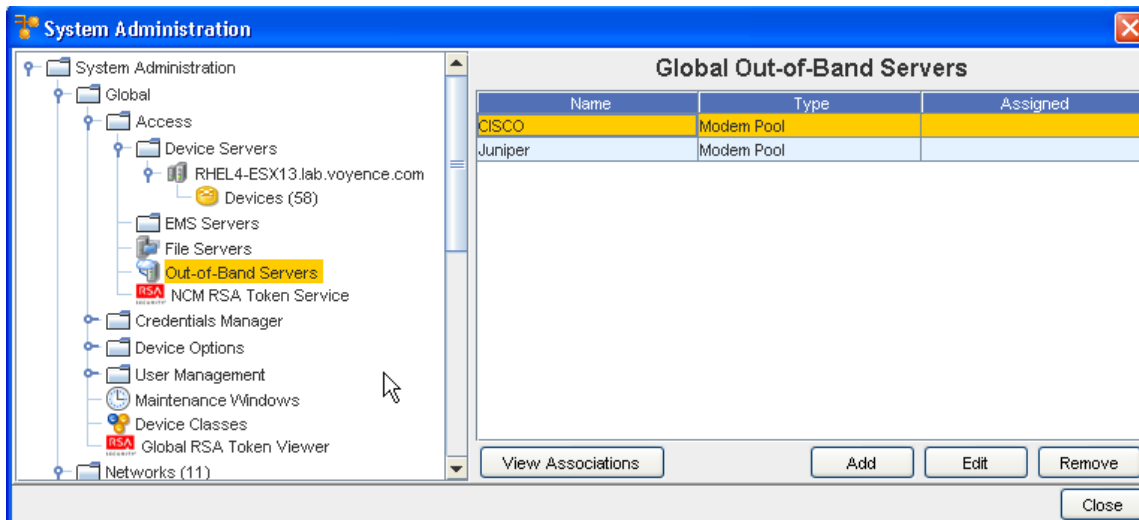
---

**Note** Once a server is removed from the list, it cannot be retrieved. You must add the server again.

---

To delete an out-of-band set up at the global level,

- 1 In the menu bar, select **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Global**, then the **Access** folders.
- 3 Click the **Out-of-Band Servers**. The Global Out-of-Band Servers window opens in the right pane.
- 4 Select the Server you want to remove, then click **Remove**.



5 Click **Ok** at the confirmation message.

**Or...**

To delete an out-of-band set up at the network Level,

- 1 In the menu bar toolbar, select **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Networks folder**.
- 3 Double-click the **network name**.
- 4 Expand the **Access** folder.
- 5 Click the **Out-of-Band Servers** . The Network Out-of-Band Servers window opens in the right pane.
- 6 Select the server you want to remove, then click **Remove**.
- 7 Click **Ok** at the confirmation message.

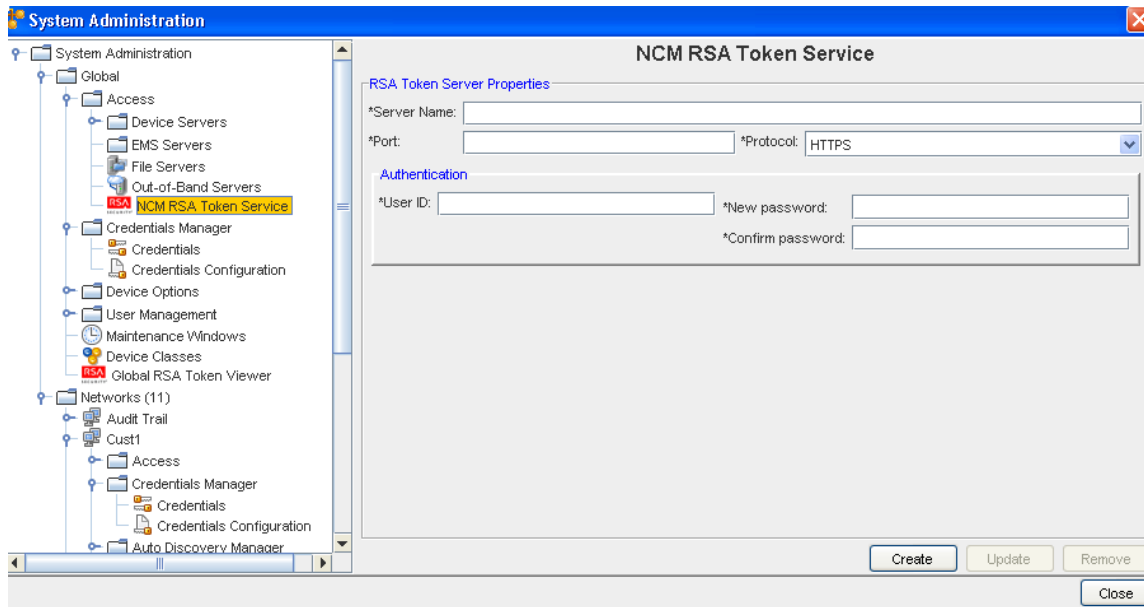
## Global - NCM RSA Token Service

### RSA Token Service Overview

RSA Token Service define the properties of the RSA Token Service servers in your network. An RSA Token Service acts as the storage location for all RSA Tokens for your network.

The RSA Token Service Properties window is available from:

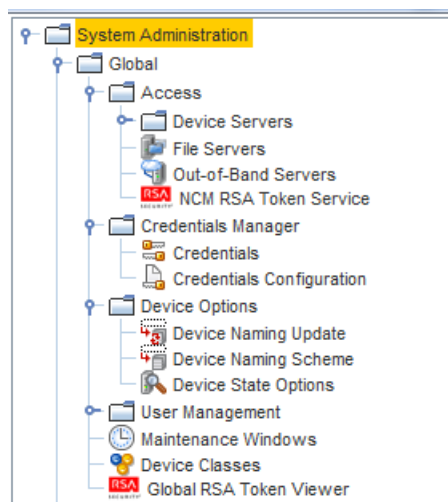
**Tools -> System Administration -> Global -> Access -> NCM RSA Token Service**



From this window, you can change the Server Name, Port, and Protocol for the RSA Token Server.

### Accessing a Network Configuration Management (NCM) RSA Token Service

From the Global view of the System Administration window, you can select Access to view the Device Servers, EMS Servers, Out-of-Band Servers, NCM RSA Token Service, and Server Properties.



### Creating an RSA Token Service

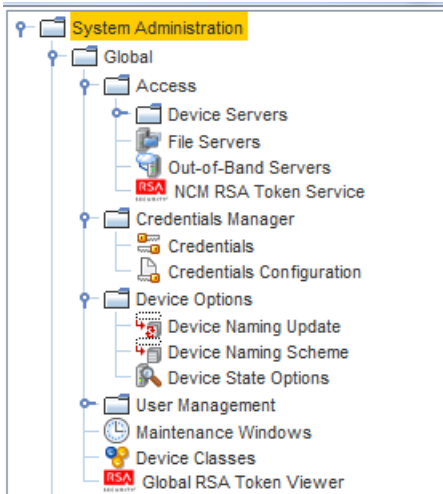
---

**Note** An RSA Token Server can be configured at the Global Level only.

---

To access the Global level set up,

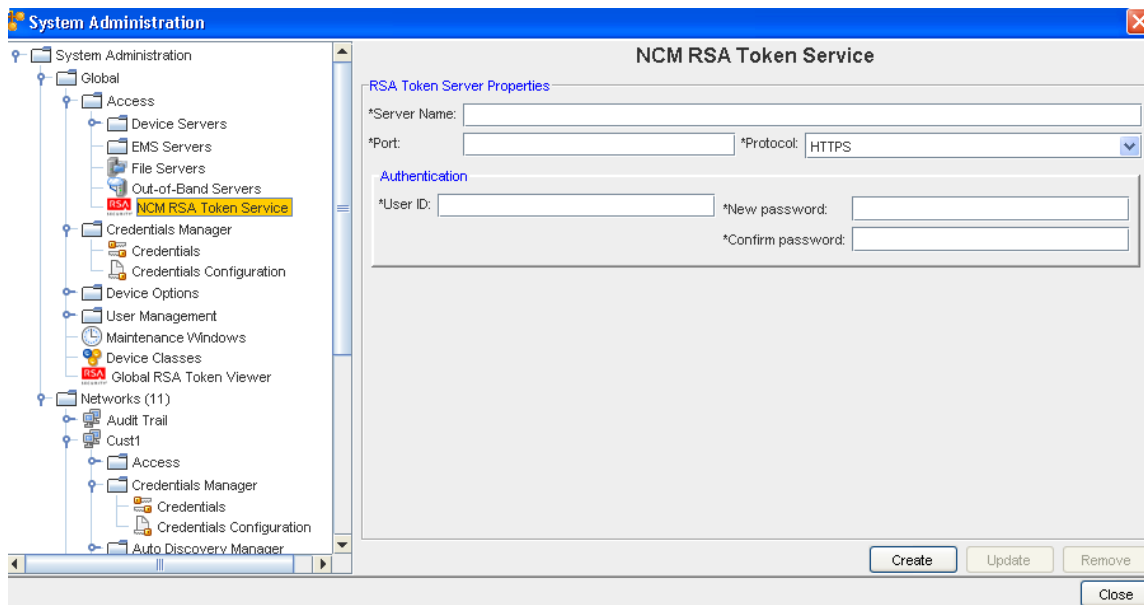
- 1 In the menu bar, select **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Global**, then the **Access** folders.



- 3 Click **NCM R SA Token Service**. The Global RSA Token Service window opens in the right pane.

To create an RSA Token Service,

**Note** Network Configuration Manager supports the use of only **one** RSA Token Service



- 1 Click the **Create** button.
- 2 Complete the setup of the RSA Token Server options, as needed.
- 3 When finished, click **Update**.



The following fields are available. Note that the required fields are identified by an asterisk (\*).

Field	Description
Server Name	The name of the server being used for the RSA Token Server.
Port	The port number used to access the RSA Token Server.
Protocol	HTTP or HTTPS
User ID	The username used to access the RSA Token Server
New password	The password used to access the RSA Token Server

The configured RSA Token Server information is listed in the RSA Token Server window.

### Updating an NCM RSA Token Service

---

**Note** An RSA Token Service can be configured at the **Global Level only** .

---

To access the Global level set up,

- 1 In the menu bar, select **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Global**, then the **Access** folders.
- 3 Click **NCM RSA Token Server**. The Global RSA Token Server window opens in the right pane.

To update an NCM RSA Token Service,

- 1 Complete the setup of the RSA Token Service options, as needed.

The following fields are available. Note that the required fields are identified by an asterisk (\*).

- 2 When finished, click **Update**.

Field	Description
Server Name	The name of the server being used for the RSA Token Server.
Port	The port number used to access the RSA Token Server.
Protocol	HTTP or HTTPS
User ID	The username used to access the RSA Token Server
New password	The password used to access the RSA Token Server

The configured NCM RSA Token Service information is listed in the NCM RSA Token Service window.

## Removing an NCM RSA Token Service

---

**Note** An NCM RSA Token Service can be configured at the **Global Level only**.

---

To access the Global level set up,

- 1 In the menu bar, select **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Global**, then the **Access** folders.
- 3 Click **NCM RSA Token Service**. The Global NCM RSA Token Service window opens in the right pane.

To remove an RSA Token Server,

- 1 Click the **Remove** button.
- 2 A warning is displayed. Click **Yes** to complete the removal of the RSA Token Server.

## Global - Credentials Manager

### Global - Credentials Manager Overview

Credentials are created by the System Administrator in the Credentials section of System Administration. Credentials are initially associated with devices during Auto Discovery. Credential associations can be reset for one or more devices using the right-click menu, or for a single device within Device Properties.

Unique credentials can be assigned for both the device management and cut-through mechanism. Built in prompt and Account credentials are available for cut-through.

Additional internal auditing enhancements are now available allowing a System Administrator more insight into who is accessing devices, and what tasks are being completed within the system.

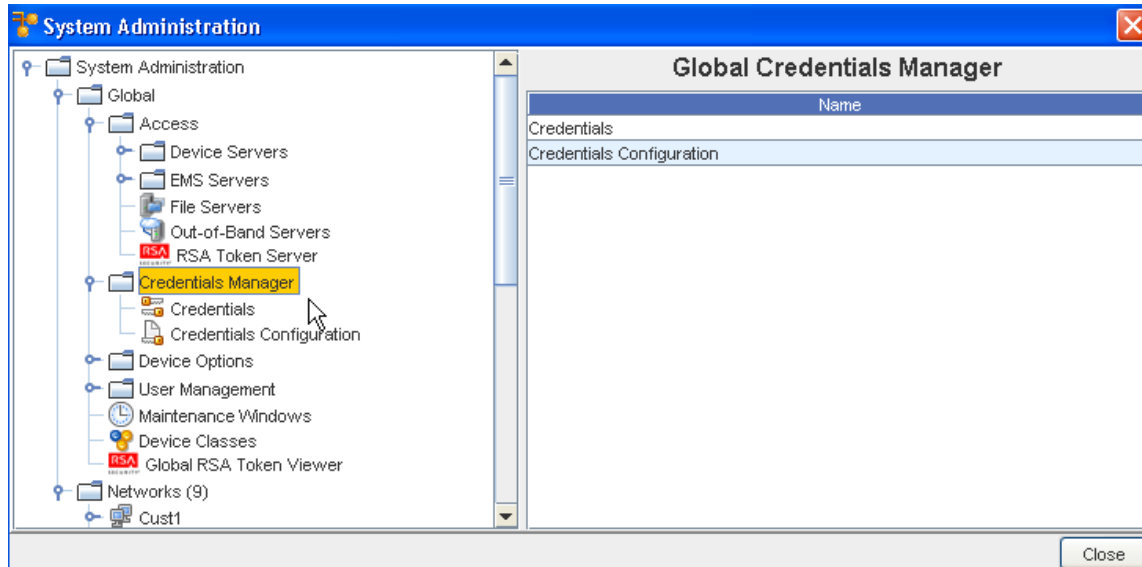
As the System Administrator, you now have a method of dynamically controlling the credentials used for any device operation, as well as being offered the flexibility to deal with special and exception scenarios to manage certain devices.

As a System Administrator, you can now determine if credentials are to be governed by Global Credential Configuration settings, or allow Credential Configurations at the Network level to override the Global Configuration settings.

Now, shared credentials to all network devices can be overridden at the time of actual execution, whether the operation is scheduled or non-scheduled.

The Credentials Manager has two options that you can view and work with:

- Credentials
- Credentials Configuration



From **Credentials** you can:

- View Associations
- Roll
- Add
- Copy
- Edit
- Remove

From **Credentials Configurations** you can select configuration options, for either **Scheduled** or **Non-Scheduled** jobs and operations:

- Use Static Device Assignment
- Use Login Credentials
- Prompts User

## Credentials Best Practices

- Use credential management to specify how to secure your device communications.
- Use Credentials Configurations to determine the credentials that need to be used for communication with the devices.
- Manage credentials on a network or global basis, **not per device** . This allows you to make changes to a single credential, rather than make changes to each of many individual devices.
- If your Device Server and its devices are within a secured private network, then using unsecured protocols such as Telnet, FTP, and SNMP provides better overall performance and management ease, as well as better device coverage.

- If your Device Server and its devices are not within a single secured private network, then use credential management to disable non-secure protocols, and allow only secure protocols, such as SSH and SCP.

### When using SNMP Communications

- Enabling SNMP communications provides the best overall quality of device information, with the greatest span of device coverage. The cost is a lower network security on traffic between the Device Servers and the monitored devices.
- Disabling SNMP communications gives you improved network security (by disabling non-secure SNMP traffic). The cost is having less device-specific information available, from a fewer number of device types. Information that is lost could include connection information, memory availability, and system information.

## Credential Settings Overview

Network Configuration Manager has a sophisticated, flexible mechanism for assigning credentials used for communicating with devices. Credentials include:

- The device local username
- The device local password
- The device local privilege-access password
- The device username and password(s) from TACACS
- SNMP community strings (Read-Only and Read-Write)
- Telnet and SSH terminal access
- Out-of-band terminal access (for example, modem pools and terminal servers)
- FTP and SCP file transfer access

Credentials can be created and managed independently from the devices they apply to. Multiple credentials can then be applied to an individual device, or groups of devices. This way, if a credential changes, the change can be propagated quickly and efficiently to all devices within a specific credential class.

Credentials can be created at the following levels:

- Global, product level . These credentials are created and managed **globally**, and are available for assignment to any device that is managed by Network Configuration Manager on any Device Server, in any network.
- Network level . These credentials are created and managed at the **network** level, and are available for assignment to any device within a specific network.

here are four types of credentials:

- Account. This credential specifies how to log into a device, for either a terminal session or a file transfer session. It contains a username, and a password.

- **Privilege Password** . This credential specifies the password used to provide privileged access to a device.
- **SNMP v1/v2c** . This credential is used to provide Read-Only and Read-Write access to SNMP.
- **SNMP v3** . This credential specifies the version of SNMP.

Each device can have four account credentials and a community string credential assigned to it. All access to the device (such as telnet, ftp, and SNMP) use these credentials. Additionally, the Account credential can have a privilege credential associated with it, which specifies additional validation necessary for privilege access.

Credentials are assigned to devices by selecting a group of devices (either a single device, an entire network, site, or view of devices, or some subset of devices), and applying a credential to those devices. Once the credential is assigned, changing any of the values in the credential (such as the username or password) applies that change to all assigned devices.

### Out-of-Band Communications

In addition to the normal credentials, a separate set of credentials can be applied to Out-of-Band communications. If a device has an Out-of-Band communications mechanism that requires authentication (such as using a terminal server), then a separate account credential can be assigned to the device for use in this authentication. This is a separate credential used to connect to the terminal server , and is different than the device credential.

### Cut-Through Communications

Finally, you can configure credentials to use for devices when cut-through communications is used. Cut-through communication is the ability to establish a telnet or SSH session directly with the device; running a telnet client on your client machine. This allows you to communicate directly with the device with standard auditing and traceability.

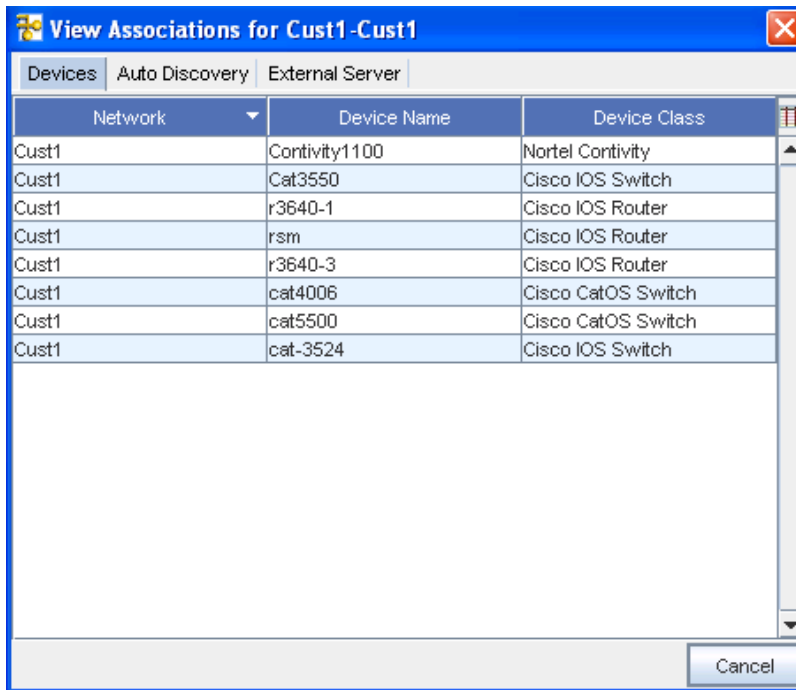
When you establish the Cut-through connection, the system automatically logs you onto the selected device, either in privileged or non-privileged mode. To do this, an account credential (with optionally, an associated privilege credential) must be available.

You can choose different credentials to authenticate the Cut-through session - depending on the Jobs Credentials Configuration selected.

- **Primary device credential.** This causes Cut-through to connect to the device using the primary account credential (with optionally, an associated privileged credential). Permission to complete this action is provided within the security subsystem of Network Configuration Manager. This mode allows a device to have a single user configured that is used for *all communications*, and allows Network Configuration Manager to provide the per-user authentication needed.

- **User Account.** This causes Cut-Through to use the credentials assigned to the user themselves (the credentials they use to log into the Network Configuration Manager system) to authenticate to the device. This mode is very convenient if both the device and Network Configuration Manager are configured to use an authentication server, such as TACACS. This allows the device to better provide controlled access during the Cut-through session to internal capabilities, based on the user's TACACS credentials.
- **User Prompted .**This prompts you for credentials (Username, Password and Privilege Password) when accessing the device.

## Auto Discovery



Network	Device Name	Device Class
Cust1	Contivity1100	Nortel Contivity
Cust1	Cat3550	Cisco IOS Switch
Cust1	r3640-1	Cisco IOS Router
Cust1	rsm	Cisco IOS Router
Cust1	r3640-3	Cisco IOS Router
Cust1	cat4006	Cisco CatOS Switch
Cust1	cat5500	Cisco CatOS Switch
Cust1	cat-3524	Cisco IOS Switch

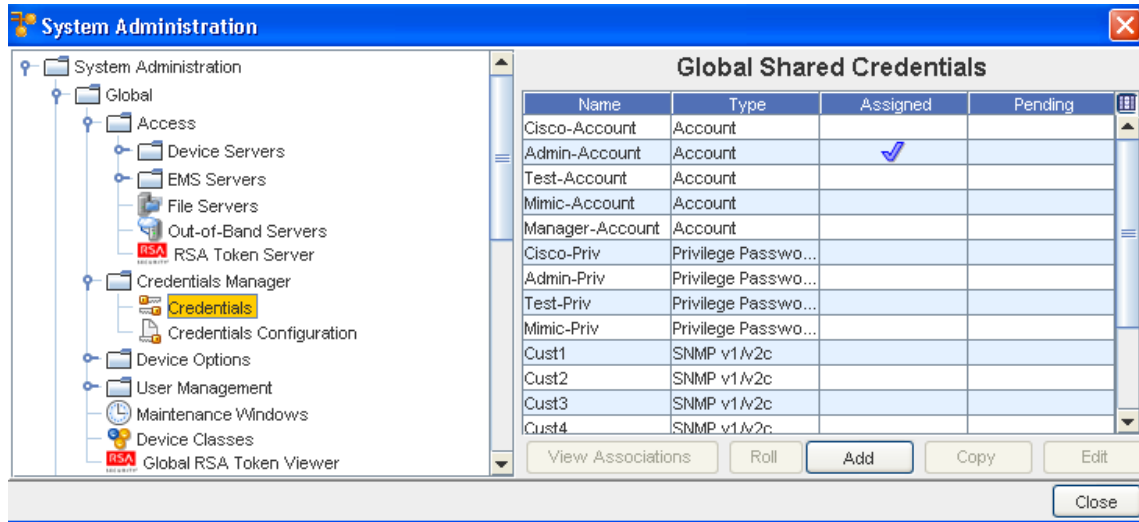
When auto discovery is configured, a series of credentials can be assigned to the auto discovery job.

When auto discovery finds a new device , it attempts to authenticate the credentials, one-by-one, in order, until a credential is found that communicates to the device. This credential is then automatically assigned to that device. A device may associate either an account credential, an SNMP credential, or both to each device during an auto discovery job.

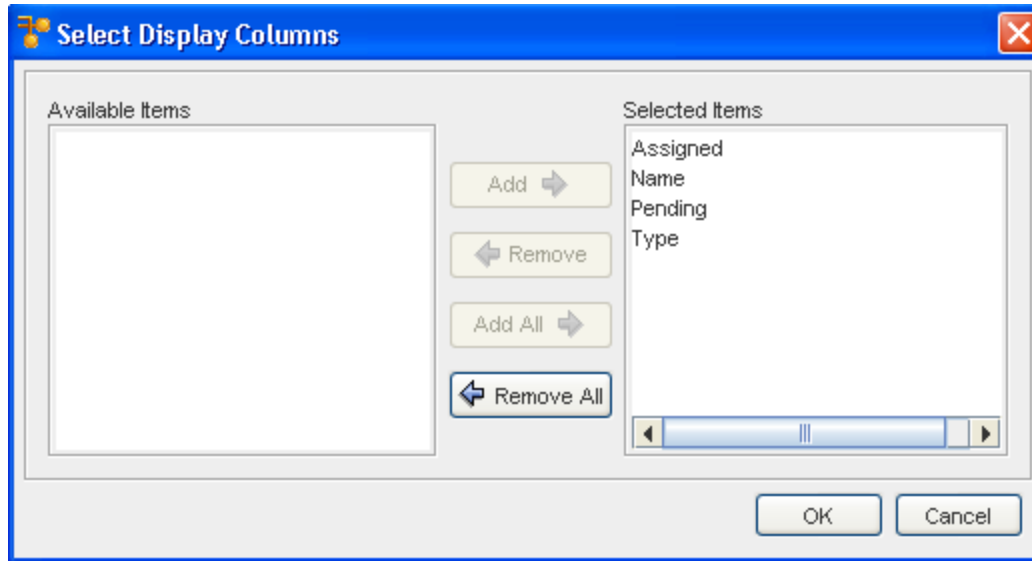
## Working with Credentials

To access and work with Credentials, you must first select the credentials areas you want to work with. To see a listing of existing credentials and to work with the listing, or add to it, select Credentials from the **Credentials Manager**.

Once selected, you can then complete various tasks on the **Global Shared Credentials** .



From this window, you can determine which columns you would like to display by clicking inside any column heading. You can select from Name, Type, Assigned, and Pending using the display column icon, or you can right-click in any column heading name to view the Select Display Columns window, and then select from the listing.



- Viewing Associations
- Rolling Credentials
- Adding Global Shared Credentials
- **Copy** - to copy an existing credentials
- Editing global Shared Credentials
- **Remove** - to remove an existing credential from the listing

## Global Credential Settings

Credentials is a layer of security that has been incorporated into Network Configuration Manager. Similar to the permissions that can be set at the network, device, or workspace levels, credentials are application security settings.

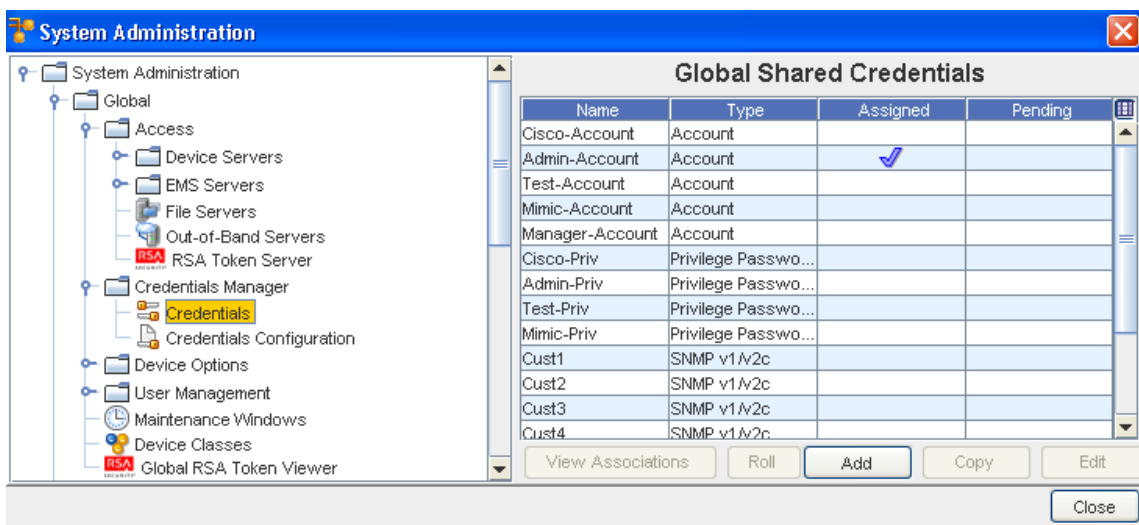
Setting credentials allows you to designate **how you connect with Network Configuration Manager**. There are three available options:

- 
- Managed** Indicates devices that are associated with networks. Managed devices reside in the central repository, and are under the control of authorized network users. Users can be assigned permissions at the device level related to what actions (tasks) the user is able to complete on the managed device.
- 
- Unmanaged** Indicates devices that are discovered, but are flagged, so that they are not repeatedly rediscovered in subsequent auto discovery runs.
- 
- Unclassified** Similar to Unmanaged devices, except these devices have not been designated as Managed or Unmanaged. By default, all devices are Unclassified until located and associated to a network.
- 

One or more of these settings can be filled, providing you with multi-access methods.

To set credential access,

- 1 Open **Tools -> System Administration** .
- 2 In the navigation pane, select **Global -> Credentials Manager**, then **Credentials** .



- 3 To add a credential, click the **Add** button on the bottom of the Global Shared Credentials window. The Add Credential window opens.



The screenshot shows a dialog box titled "Add Credential". It features a blue header bar with the title and a close button. The main area contains the following elements:

- \*Credential Name: [Text Input Field]
- Credential Type: [Dropdown Menu, currently set to "Account"]
- Voyence Unique Credentials Length: [Text Input Field]
- User Name: [Text Input Field]
- Password: [Text Input Field]
- Confirm Password: [Text Input Field]
- This account is managed by an external authentication server.
- Generate... [Button]
- OK [Button]
- Cancel [Button]

- 4 Enter the **Credential Name** .
- 5 From the **Credential Type** drop-down arrow, make your selection from the list of types. You can select from Account, Community String, Privilege Password, or SNMP v3.
- 6 To select a unique credential, click in the **Voyence Unique Credentials** checkbox. This allows the application to create a unique placeholder (with the length designated by you). Notice that when this check box is selected, the remaining fields change. See [Unique Credentials](#) for more information.
- 7 Enter a **User Name** and a **Password**. Confirm the password you just entered by entering the Password again.
- 8 Click inside the check box if this account is managed by an External Authentication Server .
- 9 Click **Ok** to save your information, and complete setting the global credentials.

---

**Note** Network Configuration Manager supports two privileged password modes: **Single-Level and Multi-Level**.

---

- The Multi-Level mode allows **multiple levels of privileged passwords** to be created and associated within the Network Configuration Manager application.

- If **Multi-Level** was selected during installation, go to [Privilege Password for Multi-Level Mode](#)

## Privilege Password for Multi-Level Mode

Network Configuration Manager supports two different privileged password credential modes: **Single-Level** and **Multi-Level**.

The Multi-Level mode allows **multiple levels of privileged passwords** to be associated with a device in the Network Configuration Manager application. If **Multi-Level** was selected during post installation, use this section to work with Privilege Password tasks.

To Setup discovery of different levels of Privilege Passwords,

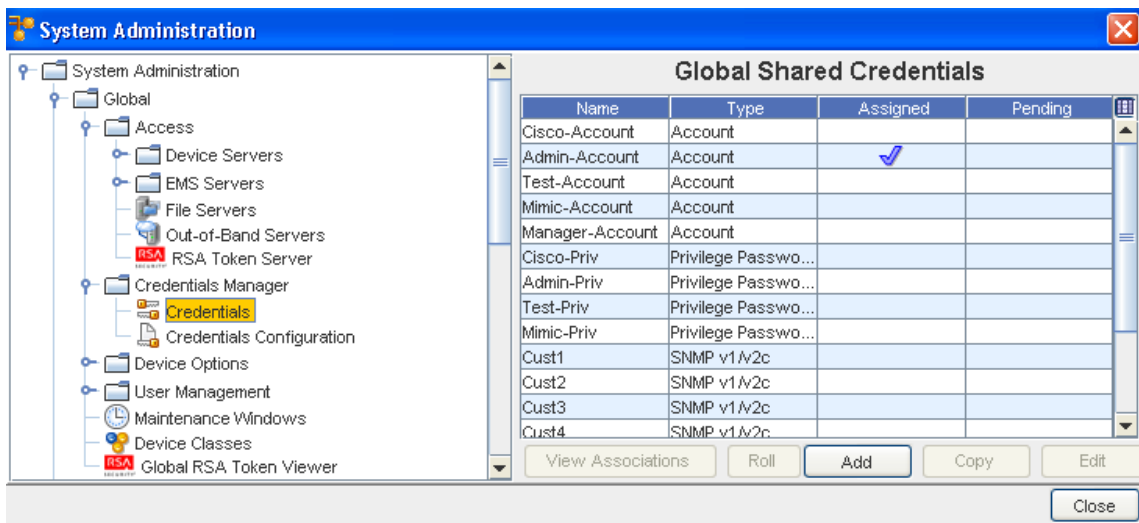
**Note** Network Configuration Manager Privilege Password level support is preset to manage only level 15.

- 1 To view, Add, or Remove managed levels manually by the device server, login as the **root user** on the **Device Server box**, or on the **Combo box**.
- 2 Change directory ( **cd**) to **\$VOYENCE\_HOME/package/privilegelevels/pkgxml**.
- 3 Edit the **privlevels.xml** file to add, remove, or modify the managed levels.
- 4 Add, Remove, or Modify user configuration levels.

For more information, see [Managing and Viewing Privilege Password Levels](#)

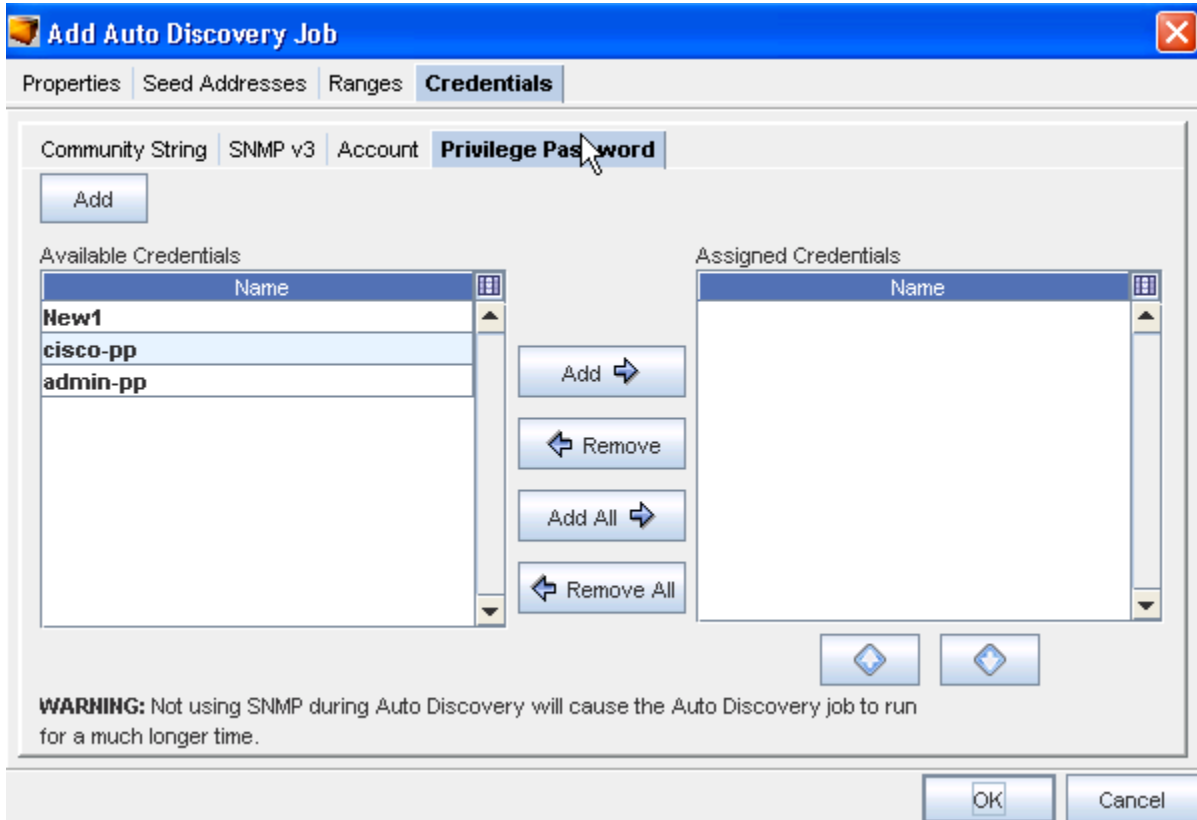
To discover multiple Privilege Passwords for a device,

- 1 At **System Administration** (in Tools on the Network Configuration Manager launch window), select **Global -> Credentials Manager** , then select **Credentials**.



- 2 Create **Credentials** (Add) for all Privilege Passwords to be discovered and associated to levels.

- 3 Setup the Auto Discovery profile (through **Networks -> Auto Discovery** ), and select **New** to either create a New profile, or to edit an **Existing profile** , then click **Edit** to discover multiple Privilege Passwords.
- 4 At the Credentials tab, add all the **Privilege Passwords** to be discovered.



- 5 Next, click the **Privilege Password** tab within the Communications tab. From here you can add or remove any Available Credentials using the arrows. Select, then move the Available Credentials into the **Assigned Credentials** pane. You can use the up and down arrows in the Assigned Credentials pane to determine the order of the Credentials.
- 6 To add a new Credential, click **Add**. Enter the information needed to add this credential, then click **OK**.

Network Configuration Manager then discovers all the valid Privilege Passwords for the device. For example,

**Device 1** - for password levels **2, 8, 9, 10, 15**

2 - Level 2

8 - Level 8

15 - Cisco Privilege Password

**Device 2** - for password levels **2, 8, 15**

During Auto Discovery, all the devices are discovered, and the different level-based Privilege Passwords that are configured with the Privilege Password are also discovered. During this discovery, the application attempts to login using the password levels.

- 7 Select the **Auto Discovery Profile**, then Update or Schedule.
- 8 Click **Ok** when you have added the Credential information.

## Credential Types

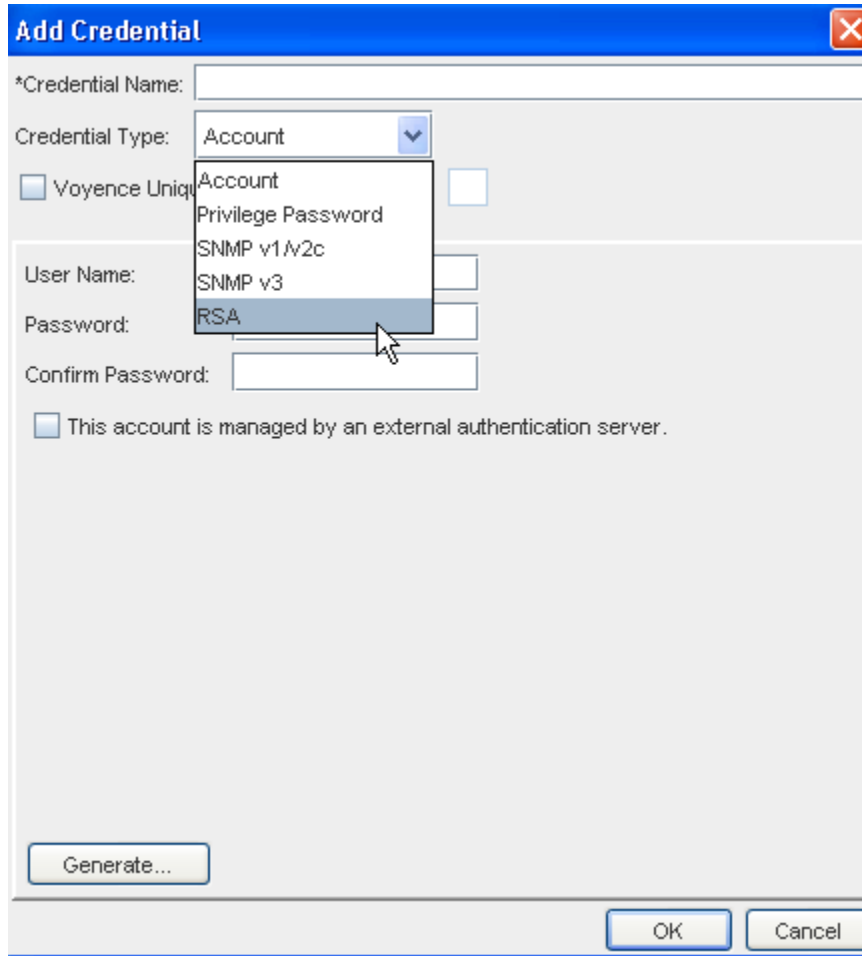
When you are working in the **Add Credential** window, you have the choice of selecting the type of Credential.

You can select from the following types:

- Account
- Privilege Password
- SNMP v1/v2c
- SNMP v3
- RSA

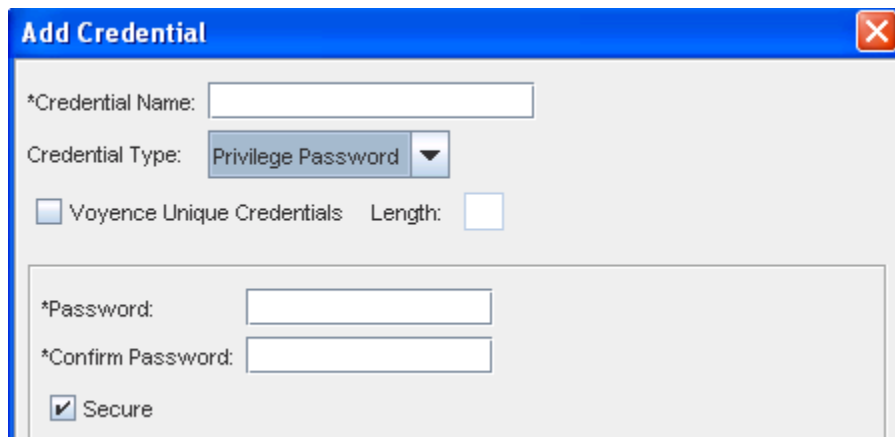
### Account

When working to create a new Credential, the following illustration shows the fields you need to add information into for this credential type.



### Privilege Password

When working to create a new Credential, the following illustration shows the fields you need to add information into for this credential type .



### SNMP v1/v2c

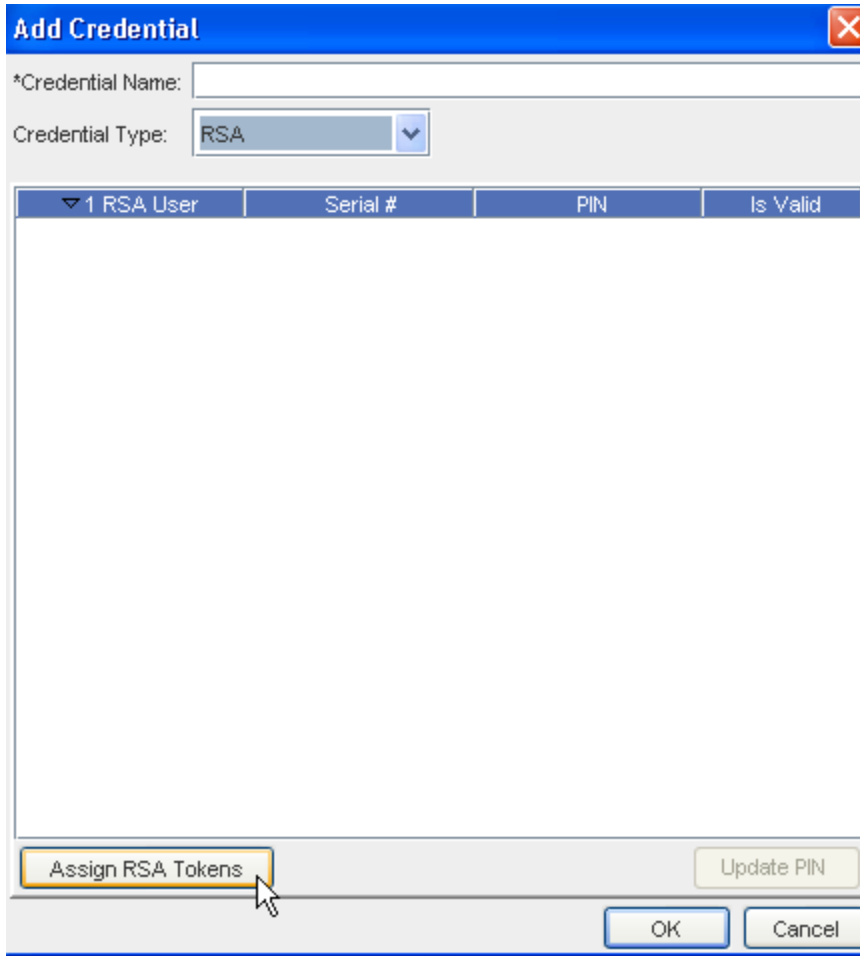
When working to create a new Credential, the following illustration shows the fields you need to add information into for this credential type .

### SNMP v3

When working to create a new Credential, the following illustration shows the fields you need to add information into for this credential type .

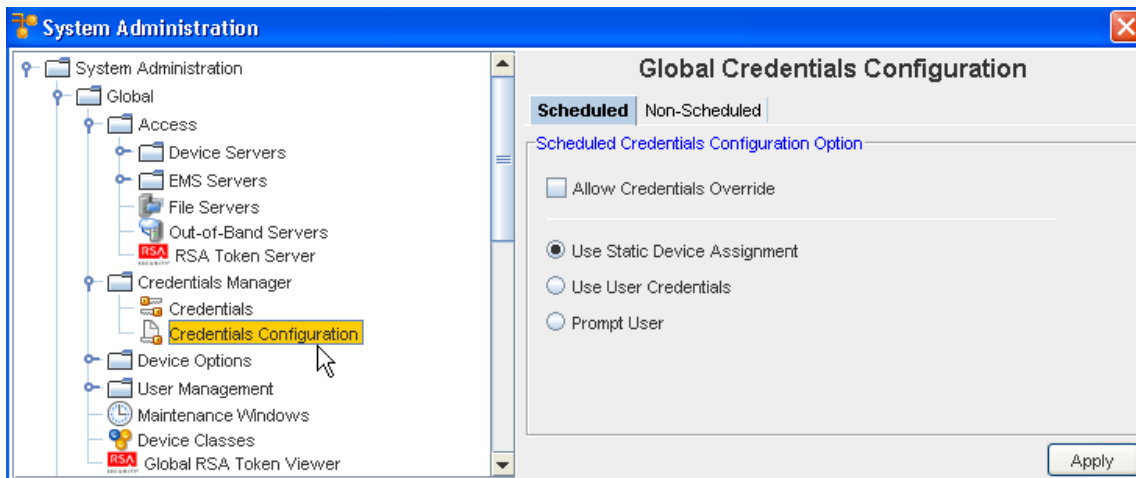
### RSA

When working to create a new Credential, the following illustration shows the fields you need to add information into for this credential type .



## Using Credentials Configuration

Access to the Credentials Configuration is through the **Credentials Manager** .



## At the Global Credentials Configuration Level

At this level, you are provided the options to determine the credentials that need to be used for communication with the device. This includes scheduled jobs, as well as synchronous operations targeted on a device, such as cut-through, quick commands, and more.

- The **Scheduled** tab refers to the jobs that can be scheduled to run (with the exception of Auto Discovery and Pulls).
- The **Non-Scheduled** tab refers to those operations (Cut-Through, Quick Commands, and Save Commands, for example) that are not scheduled.

You can select from the following options:

### The Scheduled Tab

#### Users Static Device Assignment

- **Uses Static Device Assignment** - If Uses Static Device Assignment is selected- this indicates to the system to use the Shared Credentials assigned at the device level within a network. This is the default option.

The screenshot shows a window titled "Global Credentials Configuration". At the top, there are two tabs: "Scheduled" (which is selected) and "Non-Scheduled". Below the tabs, the "Scheduled Credentials Configuration Option" section is visible. It contains four radio button options:
 

- Allow Credentials Override
- Use Static Device Assignment
- Use Login Credentials
- Prompt User

 An "Apply" button is located at the bottom right of the dialog box.

#### Use Login Credentials

- **Use Login Credentials** - When **Use Login Credentials** is selected - this indicates to the system to use the user's application login account as the device credentials (the account name/account password). You have the choice to select any of the options of when the user's are now prompted to enter account and password information before completing tasks.
- You can also select to **Allow Credentials Override**



### Global Credentials Configuration

**Scheduled** | Non-Scheduled

**Scheduled Credentials Configuration Option**

Allow Credentials Override

---

Use Static Device Assignment

**Use Login Credentials**

Prompt for Privilege Password

**Run Upon Approval / Run Scheduled Time / Run Next MW / Run as Recurring Se**

Use Submitter Credentials

Use Approver Credentials

**Run Operator Initiated**

Use Submitter Credentials

Use Approver Credentials

Use Operator Credentials

Prompt User

**Note** In some cases where a job may be scheduled in the future, the user's login credentials may need to be preserved until the job executes (to construct the device server request). These credentials must be deleted immediately after the task request is sent to the device server. You must pay attention to jobs with "Preserve Order" selected, as each task execution depends on the success of the previous task in the list (the credentials must be preserved until the last task executes).

- You can select to **Prompt for Privilege Password**

To determine whose credentials are to be used for jobs, the following options are available for each run option as applicable, **one** of which must be selected:

- **Use Submitter Credentials** – In case of scheduled operations, the system uses the submitter's credentials. This includes any job submission through "Submit" button on the scheduler.
- **Use Approver Credentials** – In case of jobs, the system uses the approver's credentials. This includes any job submission through –Approve&Submit– button on the scheduler or the "Approve" icon on the Schedule Manager.
- **Use Operator Credentials** (in case of jobs whose run option is –Run Operator Initiated–) – In case of jobs, the system uses the credentials of the user attempting to manually execute the job.

In case of non-scheduled operations, the login credentials of the user executing the operation are used, and the above options are redundant.

### Global Credentials Configuration

**Scheduled** | Non-Scheduled

Scheduled Credentials Configuration Option

Allow Credentials Override

---

Use Static Device Assignment

Use Login Credentials

Prompt for Privilege Password

Run Upon Approval / Run Scheduled Time / Run Next MW / Run as Recurring Se

Use Submitter Credentials

Use Approver Credentials

Run Operator Initiated

Use Submitter Credentials

Use Approver Credentials

Use Operator Credentials

Prompt User

If Prompt User is selected from this window, see the following information.

#### Prompt User

### Global Credentials Configuration

**Scheduled** | Non-Scheduled

[Scheduled Credentials Configuration Option](#)

Allow Credentials Override

---

Use Static Device Assignment

Use Login Credentials

**Prompt User**

Invalidates Credentials on Job Modification

[Run Upon Approval](#)

Prompt on Submit

Prompt on Approve

[Run Operator Initiated](#)

Prompt on Submit

Prompt on Approve

Prompt on Manual Execute

[Run Scheduled Time / Run Next MW / Run as Recurring Series](#)

Prompt on Submit

Prompt on Approve

- **Prompts User** - When Prompts User is selected - this indicates to the system that the user is to be prompted for the credentials before the device operation , based on the following options: Account Password, and Privilege Password.

To determine whose prompts are used for jobs, the following options are available for each run option as applicable, **one** of which must be selected:

- Run on Approval
- Prompts on Submit - Prompts at the time the job is submitted for "Pending Approval".
- Prompts on Approval - Prompts at the time the job is Approved.
- Run Operator Initiated
- Prompts on Submit - Prompts at the time the job is submitted for "Pending Approval".
- Prompts on Approve - Prompts at the time the job is Approved.
- Prompts on Manual Execute - Prompts at the time the job is manually executed.
- Run Scheduled Time / Run Next MW / Run as Recurring Series
- Prompts on Submit - Prompts at the time the job is submitted for "Pending Approval".

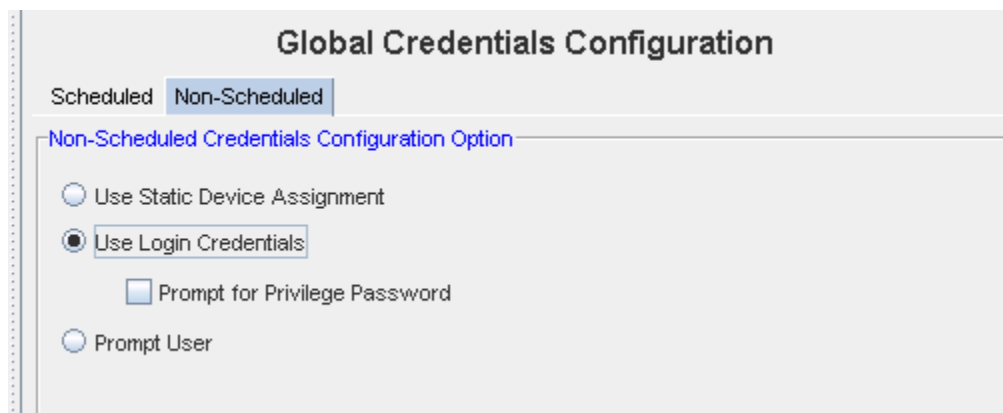
- Prompts on Approval - Prompts at the time the job is Approved.

**Note** You also have the option of selecting **Invalidate Credentials on Job Modification** . If this is selected, after a job is **edited**, any credential associated with that job is now invalid.

- 1 After making your selections from the various options, click **Apply** to apply your credential choices.
- 2 Read the system message carefully to fully understand your selection to apply the changes you have made, then select **Yes to Continue**.
- 3 If applicable, click **Yes** at the Confirmation message.

### The Non-Scheduled Tab

The **Non-Scheduled** tab refers to those operations (Cut-Through, Quick Commands, and Save Commands, for example) that are not scheduled to run.



#### Use Static Device Assignment

- **Use Static Device Assignment** - If Uses Static Device Assignment is selected- this indicates to the system to use the Network Shared Credentials assigned at the device level within a network. This is the default option.

#### Use Login Credentials

- **Use Login Credential s** - When **Use Login Credentials** is selected - this indicates to the system to use the user's application login account as the device credentials (the account name/account password).

You can select to have the user prompted for their **Privilege Password** information before completing tasks.

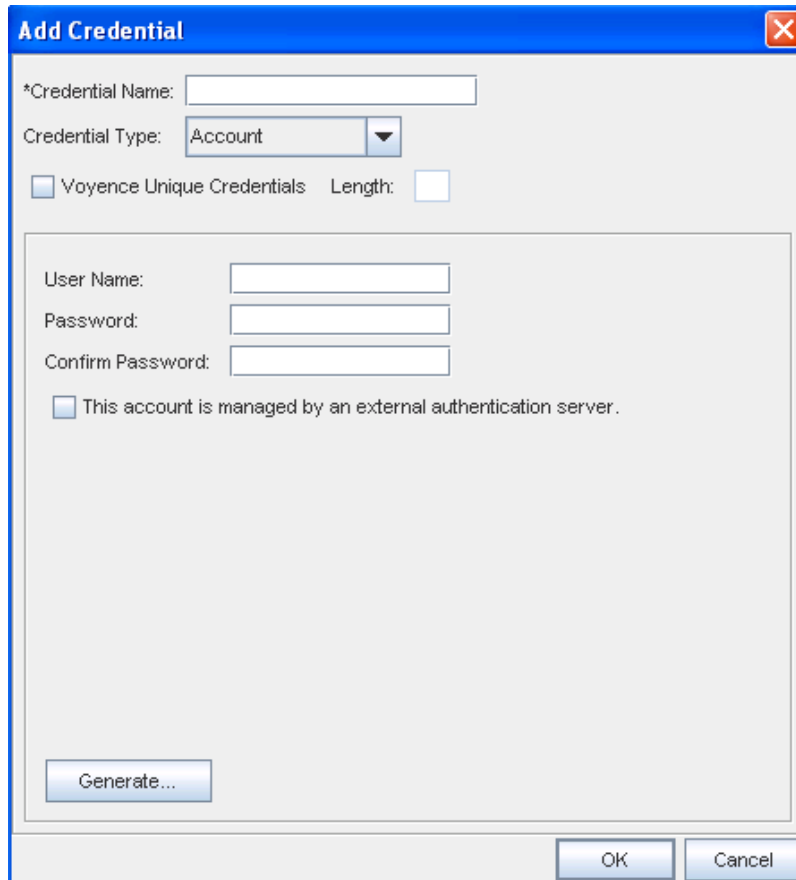
You can also select **Prompt User** from this window.

**Prompt User** - When **Prompt User** is selected - this indicates to the system that the user is to be prompted for the credentials before the device operation, based on the following options: Account Password, and Privilege Password.

### Unique Credentials

To use Unique passwords per device, creating a Unique Credential eases the deployment of device passwords. A Unique credential is a placeholder that tells the system there are unique individual passwords on each device associated with the credential. Unique credentials have no passwords stored with them, but create a different password for each device associated with them. Unique credentials must be coupled with an update to devices.

The unique feature (when checked), allows the application to create a **unique placeholder** with the length designated by you. When **Voyence Unique Credentials** check box is checked, you must enter a length of **at least 3** (as the unique string contains one uppercase, one lowercase, and one numeric entry).



The screenshot shows a dialog box titled "Add Credential". It features a blue title bar with a close button. The main area contains the following elements:

- \*Credential Name: [Text Input Field]
- Credential Type: [Dropdown Menu, currently set to "Account"]
- Voyence Unique Credentials    Length: [Text Input Field]
- User Name: [Text Input Field]
- Password: [Text Input Field]
- Confirm Password: [Text Input Field]
- This account is managed by an external authentication server.

At the bottom left, there is a "Generate..." button. At the bottom right, there are "OK" and "Cancel" buttons.

When you actually update a credential on a device and choose the unique credential that you just created, and also choose to schedule this change, at the run time, the unique values are generated.

- For Account - UserName and Password
- For Priv Pass - password
- For SNMP v1/v2c - RO and RW
- SNMPv3 - password

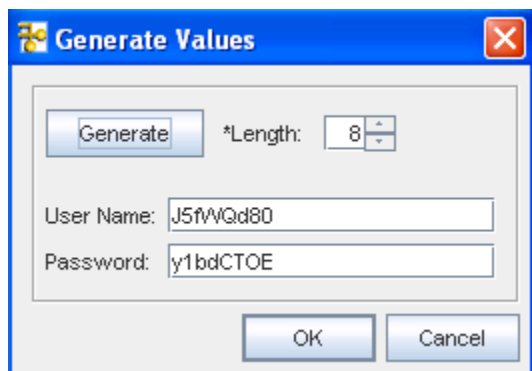
These are updated on the device physically. Network Configuration Manager is updated with the unique values, and these are stored on the device table of the database. The Unique credential that you defined is associated with the device, but does not have any of the attribute values (usernames, passwords, RO, or RW). It is a marker or placeholder to convey that this particular device has a unique set of credentials, and the Network Configuration Manager application knows how to communicate to the device.

When you edit the unique credential, you are only allowed to change the name and the length of the credential.

### The Generate button

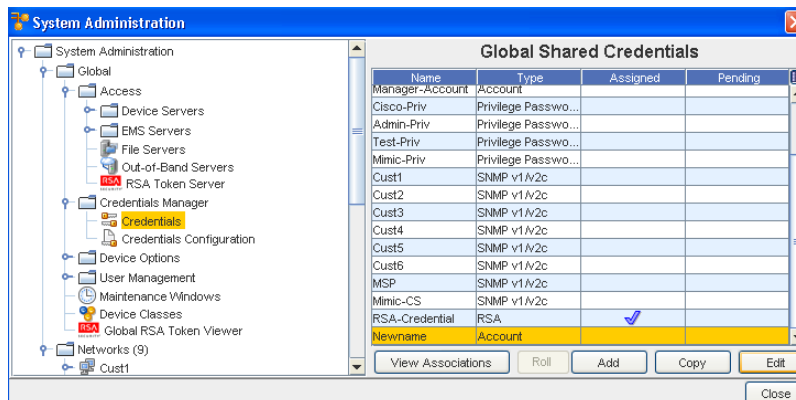
You can click **Generate** to have the application generate the password or you.

- 1 Click **Generate**.
- 2 At the Generate Values window, review the User Name and Password that has been generated for you.
- 3 Click **Ok**.



### Global Shared Credentials Options

When using the **Global Shared Credentials** Options displayed at the bottom of the Global Shared Credentials window, you can complete the following tasks.



- **Viewing Associations** - to view the associations and review the Devices and the Auto Discovery information

- **Roll** - to go to the Roll Candidate Selection screen and select a candidate. Then go to the Credential Roll Job window to schedule the roll.
- **Adding Global Shared Credentials**- to add a credential
- **Copy** - to copy a shared credential
- **Editing global Shared Credentials** - to make changes to existing information
- **Remove** - to remove (delete) the credentials
- **Close** - to leave this window

## Adding Global Shared Credentials

There are five of Shared Credentials:

- Account
- Privilege password
- SNMP V1/V2c
- SNMP v3
- RSA

---

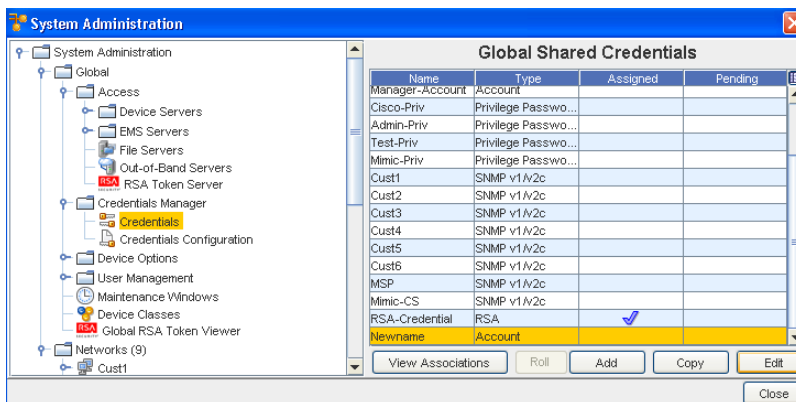
**Note** To import credentials in bulk, see [Using the Command Line Interface](#) for more information.

---

### Creating Shared Credential - Account Class

To Create a shared credential with the class type of Account, follow these steps:

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Global -> Credentials**.



The **Global** Shared Credentials window displays with a listing of pre-assigned, shared credentials. At the bottom of the window are the View Associations, Roll, Add, Edit, and Remove buttons, along with the Close option.

- 3 Click **Add** to display the Add Credential window.

---

**Note** You can also Copy the Shared Credential using the Copy button.

---

- 4 Enter the **Credential Name** .
- 5 From the **Credential Type** section, select **Account** type from the options shown (using the drop-down arrow to display your selection).

---

**Note** Depending on the credential type you select, additional information is displayed in the lower portion of the window. For example, when you select Account as the credential type, additional fields display where you enter information. See [Unique Credentials](#) for more information.

---

Credentials provide you the option to generate unique, random passwords of user definable length when using the Generate button.

- 6 Complete the following steps:
  - Enter the **User Name** .
  - Enter a **Password**. Confirm the Password.
  - Select the check box if this account is managed by an external authentication server.
- 7 Click **OK** when you have completed these steps.

**Add Credential**

\*Credential Name:

Credential Type:

Voyence Unique Credentials Length:

User Name:

Password:

Confirm Password:

This account is managed by an external authentication server.

Generate...

OK Cancel



## Creating Shared Credential - Privilege Password Class

With the **Network Shared Credentials** window displayed showing a listing of pre-assigned, shared credentials:

- 1 Click **Add** to display the Add Credential window.
- 2 Enter the **Credential Name**.
- 3 From the **Credential Type** section, select **Privilege Password** from the options shown (using the drop-down arrow). See [Unique Credentials](#) for more information.

To use Unique passwords per device, creating a Unique Credential eases the deployment of device passwords. A Unique credential is a placeholder that tells the system there are unique individual passwords on each device associated with the credential. Unique credentials have no passwords stored with them, but create a different password for each device associated with them. Unique credentials must be coupled with an update to devices.

- 4 **Note** Enter a **Password**. Confirm the Password you just entered. You can also click the **Secure** check box, then click **Generate** to have the application generate a system-only-known password. Secure passwords will generate the appropriate enable-secure command when used to update a Cisco IOS device.
- 5 Click **OK** when you have completed these steps.

## Creating Shared Credential - SNMP v1/v2c

With the **Network Shared Credentials** window displayed showing a listing of pre-assigned, shared credentials:

- 1 Click **Add** to display the Add Credential window.
- 2 Enter the **Credential Name**.
- 3 From the **Credential Type** section, select **Community String** from the options shown (using the drop-down arrow). See [Unique Credentials](#) for more information.

The screenshot shows the 'Add Credential' dialog box. It features a blue title bar with the text 'Add Credential' and a close button. Below the title bar, there is a text field for '\*Credential Name:'. Below that is a dropdown menu for 'Credential Type:' with 'SNMP v1/v2c' selected. There is a checkbox for 'Voyence Unique Credentials' and a 'Length:' field. The main area is divided into two sections: 'Read-Only' and 'Read-Write'. The 'Read-Only' section has two text fields: '\*Community String:' and '\*Confirm Community String:'. The 'Read-Write' section has two text fields: 'Community String:' and 'Confirm Community String:'. At the bottom left is a 'Generate...' button. At the bottom right are 'OK' and 'Cancel' buttons.

- 4 Complete the following steps for the **Read-Only** section:
  - Enter the Community String.
  - Confirm the Community String entered.
- 5 Complete the following steps for the **Read-Write** section:
  - Enter the Community String.
  - Confirm the Community String entered.
- 6 Click **OK** when you have completed these steps.

### Creating Shared Credential - SNMP v3

With the **Network Shared Credentials** window displayed showing a listing of pre-assigned, shared credentials:

- 1 Click **Add** to display the Add Credential window.
- 2 Enter the **Credential Name**.
- 3 From the **Credential Type** section, select **SNMP v3** from the options shown (using the drop-down arrow). See [Unique Credentials](#) for more information.

**Add Credential**

\*Credential Name:

Credential Type: **SNMP v3** ▼

Voyence Unique Credentials    Length:

**Security**    Context

\*User Name:

Security Level: **AUTH\_PRIV** ▼

Authentication Protocol: **HMACMD5** ▼

Privacy Protocol: **DES** ▼

\*Authentication Password:

\*Reenter Auth. Password:

\*Privacy Password:

\*Reenter Privacy Password:

When **SNMP v3** is selected as the Credential Type, the information you need to select and enter is divided between two tabs; **Security** and **Context**.

- From the **Security** tab, complete the following steps:
- Enter a User Name
- From the drop-down arrow, select Security Level. Depending on the Security Level you select, Authentication Protocol and Privacy Protocol may not be selectable.
- From the drop-down arrow, select a Authentication Protocol (if appropriate).
- From the drop-down arrow, select a Privacy Protocol (if appropriate).

---

**Note** You can select **AES192W3DESKEYExt** and **AES256W3DESKEYExt** protocols, only for the Cisco specific device(s).

---

- Enter an Authentication Password, then re-enter the password.
- Enter a Privacy Password, then re-enter the password. Note that you can click Generate to have Network Configuration Manager create passwords for you.
- Once your passwords are verified, click **Ok**.

---

**Note** Mibs refer to Management Information Bases, and Oids refer to Object Identifiers.

---

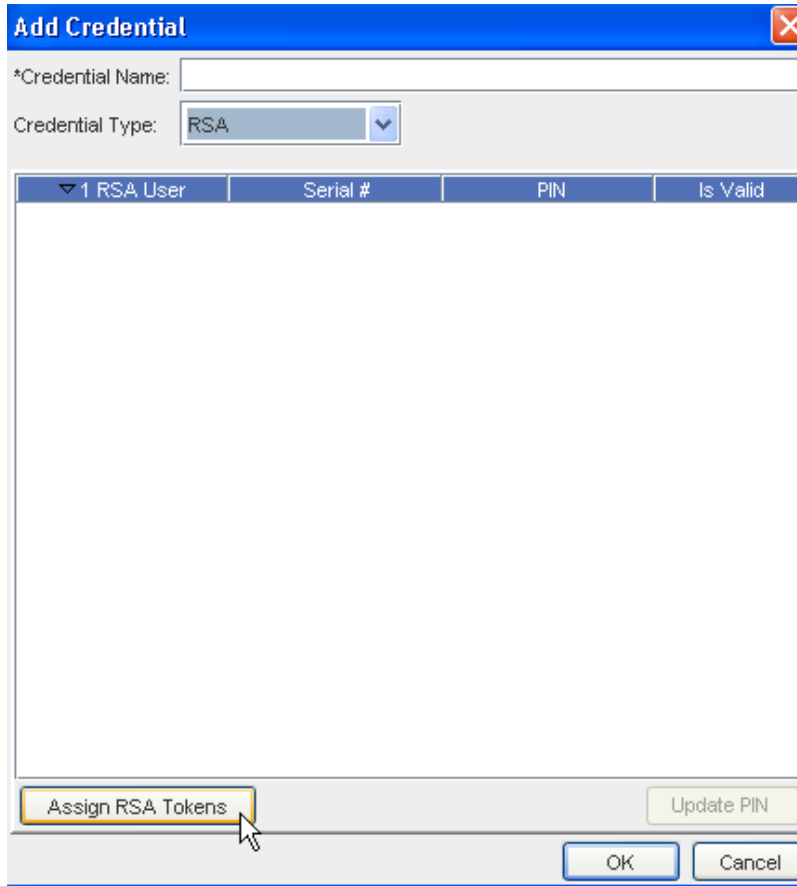
- From the **Context** tab, complete the following steps:
- Enter the Context Name
- Enter the Context Engine ID
- Enter a User Group Name
- Enter a View Name
- Select a View Access from the drop-down arrow
- Enter the Mibs/Oids you want included
- Enter the Mibs/Oids you want to be excluded from these credentials
- Click **Ok** to keep your selections

### Creating Shared Credential - RSA

With the Network Shared Credentials window displayed showing a listing of pre-assigned, shared credentials:

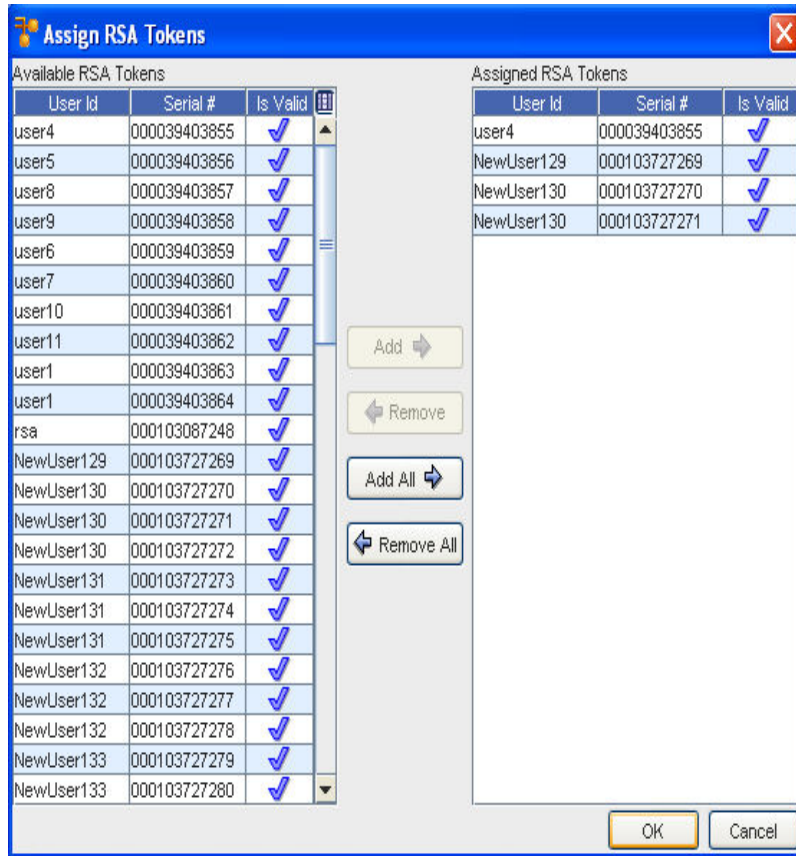
- 1 Click Add to display the Add Credential window.
- 2 Enter the Credential Name.

- 3 From the Credential Type section, select RSA from the options shown (using the drop-down arrow). See Unique Credentials for more information.
- 4 Assign RSA tokens using the steps in the Assigning RSA Tokens section below.
- 5 Set the PINs for the RSA tokens using the steps in the Setting RSA Token PINs section below.
- 6 Click OK when you have completed these steps.



### Assigning RSA Token

- 1 Select **Assign RSA Tokens**. The Assign RSA Tokens window pens.



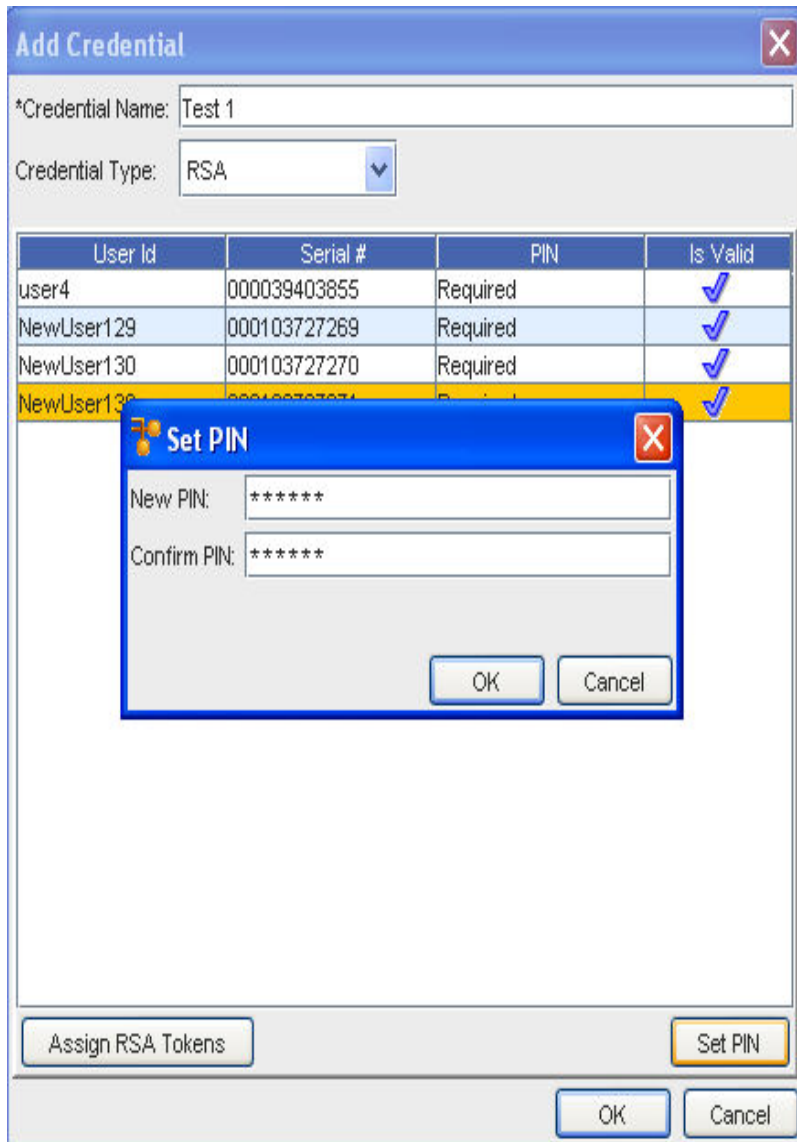
- 1 The Available RSA Tokens column is a list of all unassigned RSA tokens. Select the **RSA** tokens to which the user or group will have permissions.

**Note** A sequence of RSA tokens can be selected by holding down the Shift-key while clicking RSA tokens. Or, multiple, non-sequential RSA tokens can be selected by holding the Ctrl key while clicking the RSA token.

- 2 When you have finished selecting RSA tokens, click **Add** or **Add all**.
- 3 If you are unassigning RSA tokens, in the Assigned RSA Tokens column, select the **RSA tokens** to which the user will no longer be associated, then click **Remove All**.
- 4 Once you have completed selecting the RSA tokens for the user, click **OK**. The Assign RSA Tokens window closes.
- 5 You can now proceed with setting RSA token PINs for the user or group.

### Setting RSA Token PINs

- 1 From the list of RSA tokens, select an **RSA token**. RSA tokens that have not had the PIN set, show as Required under the PIN column.
- 2 At the bottom of the Manage RSA Tokens pane, select **Set PIN**. The Set PIN window (for the user you selected) now opens.



- 1 At the Set PIN screen, enter a **valid PIN** in the New PIN field.
- 2 Enter the PIN again in the **Confirm PIN** field.
- 3 Click **Ok**.

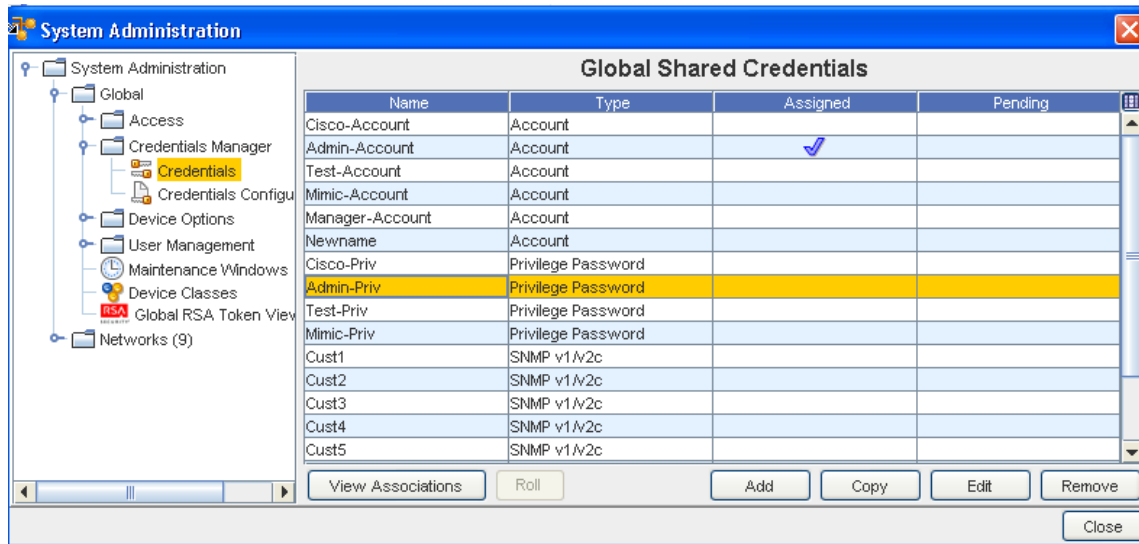
## Viewing Associations

When using the **Global Shared Credentials** window, you can select to complete tasks using the option buttons located at the bottom of the window.

These options include **View Associations** , Roll, Add, Edit, Remove and Close.

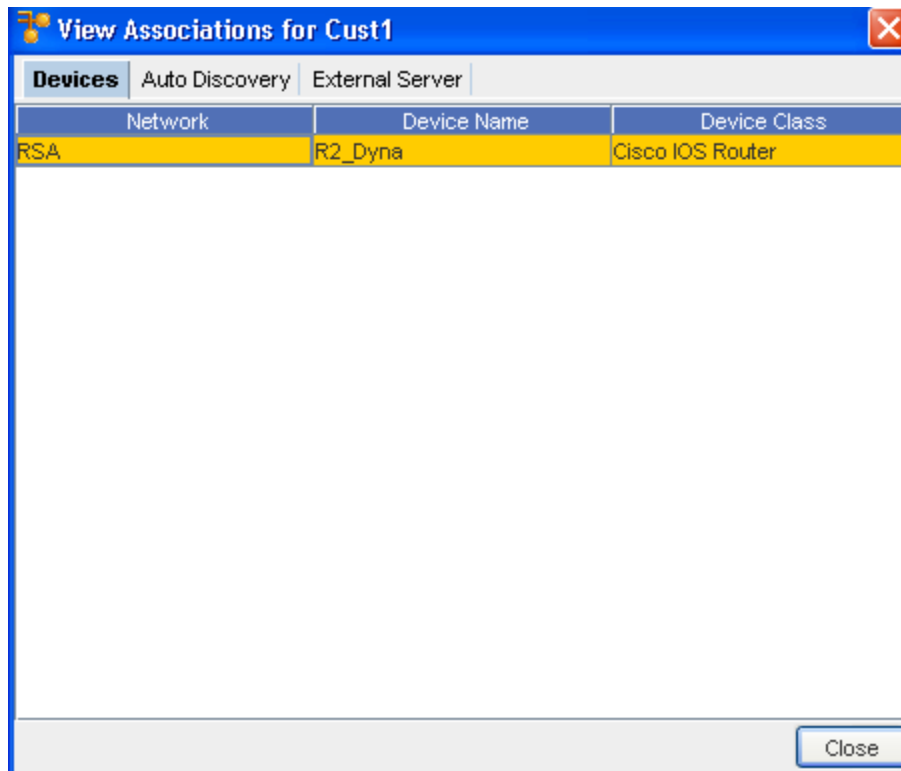
When you select to **View Associations** , you go to the View Associations window for the Name and Account you selected.





From this window you can see the:

- Network name, Device Name, and Device Class information for that account from the **Devices** tab
- Network, Name, and Type from the **Auto Discovery** tab
- Server Name and Server Type from the **External Server** tab



## Roll Credentials

When using the **Global Shared Credentials** window, you can select to complete tasks using the option buttons located at the bottom of the window.

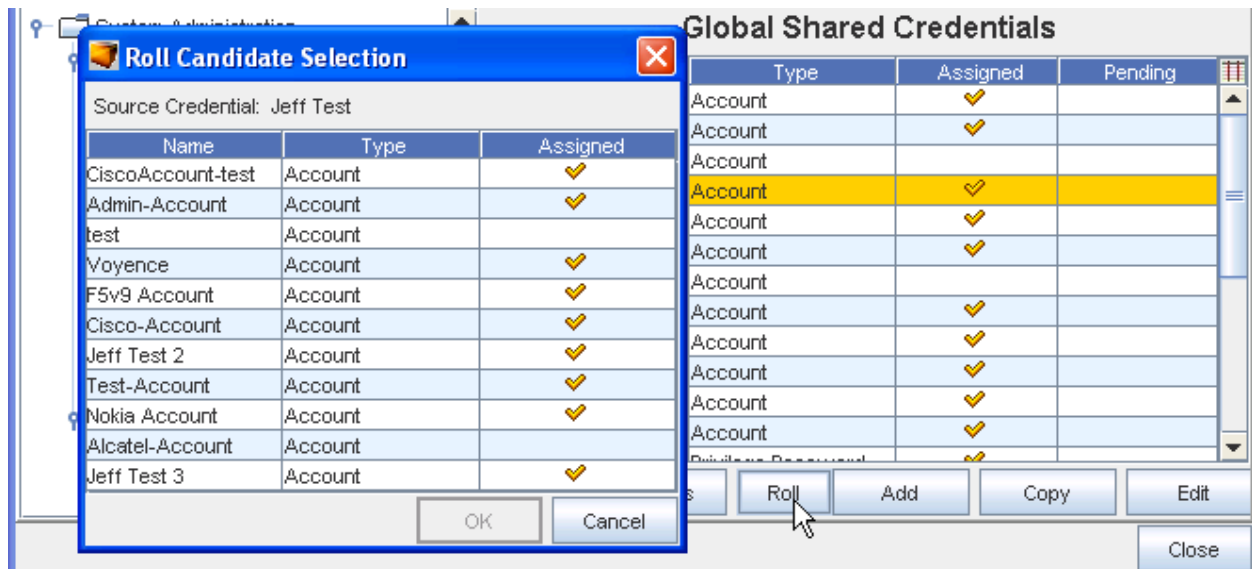
Using **Roll**, you can now:

- Select to roll from one credential to another credential
- Manage credentials on devices
- View a history of the credentials and their devices

These options include View Associations, **Roll**, Add, Edit, Remove and Close.

When you select **Roll**, you go to the Roll Candidate Selection, where you can select the Account you want to assign. Using Roll allows you to assign the Account before it is actually scheduled. Once scheduled, the status changes from Assigned to Pending until the scheduled job is run.

You can select to Roll from one credential to another credential .



- 1 Click the **Account** name (one or more) in the Roll Candidate Selection window to assign, then click **Ok**.
- 2 At the Credential Roll Job window, make your selections, and complete the information contained within the [Using the Schedule Tab](#) and [Using the Notification Tab to Send an Email](#) tabs. You must also complete and make selections in the **Schedule Job** section.

**Credential Roll Job**

**Schedule Job** Notification

**Job details**

\*Job Name: Credential Roll: Jeff Test to Admin-Account

Job owner: sysadmin

Job description:

\*Priority: Low

**Schedule job**

Run in next maintenance window  
 Run upon approval  
 Run upon operator initiation  
 Run at scheduled date/time: 12:00 PM

Run as recurring series:

Hourly  
 Weekly  
 Monthly

Start time: 12:00 PM (GMT-06:00) America/Chicago

End Time:

Never Ends  
 Ends after occurrences  
 Ends on this date/time 12:00 PM

Interval:

Approve & Submit Submit Cancel

- 3 Click the appropriate action to **Approve and Submit** or **Submit**.

### Viewing the Credentials Roll Out Log

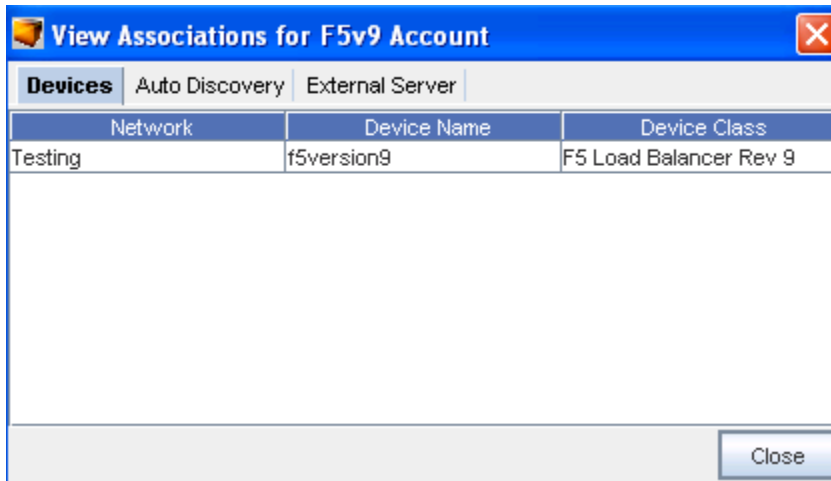
- 1 In a telnet window, verify your command results by entering change directory ( **cd** ) to **\$VOYENCE\_HOME / logs**, then pressing **Enter**. The log file to review is **credential-rollout.log**.
- 2 You can also go to the System Administrator **Credential** screen in Network Configuration Manager to verify that the credentials on the devices have been changed (rolled).

### Rolling Credentials - Privilege Passwords

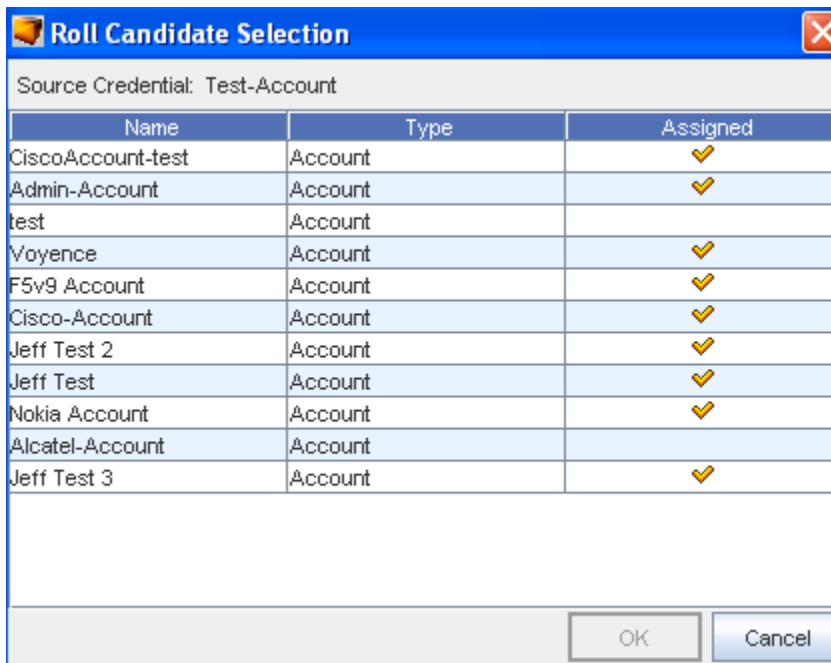
The final step is to **Roll** the Credentials.

- 1 From the **System Administration** tool (in the Network Configuration Manager window), select **Credentials Manager**, then select **Credentials**.

- 2 Select **View Associations** to see the devices associated with the Credential to verify what devices are to be involved or changed.



- 3 Back at the **Global Shared Credentials** window, select **Add**, then create a new **Privilege Password Credential** to roll your devices to. Select the Privilege Passwords on those associated devices.
- 4 At the Roll Candidate Selection window, select the New Credential from the **Roll to Privilege Password name** column, then click **Ok**.



- 5 The Credential Roll Job window opens. Complete the fields in the **Job Details** section.

**Credential Roll Job**

**Schedule Job** Notification

**Job details**

\*Job Name: Credential Roll: Jeff Test to Admin-Account

Job owner: sysadmin

Job description:

\*Priority: Low

**Schedule job**

Run in next maintenance window  
 Run upon approval  
 Run upon operator initiation  
 Run at scheduled date/time: 12:00 PM

Run as recurring series:

Hourly  
 Weekly  
 Monthly

Start time: 12:00 PM (GMT-06:00) America/Chicago  
 End Time: Never Ends

Ends after occurrences  
 Ends on this date/time: 12:00 PM

Interval:

Approve & Submit Submit Cancel

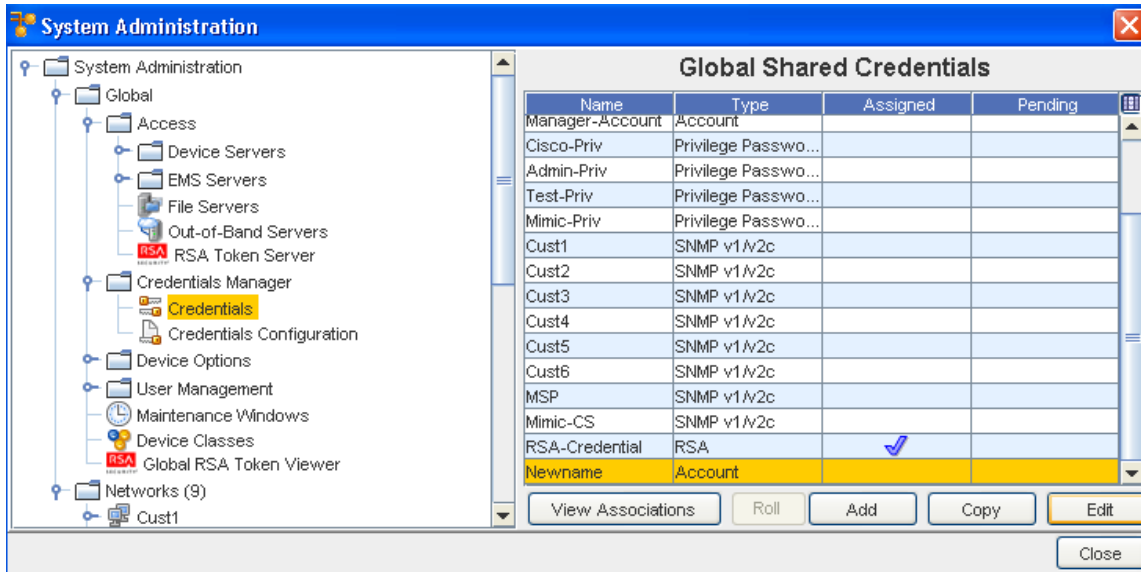
- 6 Next, complete the fields to schedule this Credential Roll job.
- 7 Click the [Using the Notification Tab to Send an Email](#) tab in the Credential Roll Job window, and select the **Users and Groups** you want to receive this job information.
- 8 Select **Approve & Submit** or **Submit** after making your selections in this window.

After the Roll job is completed, each device should now be associated with the **new Credential**. Any devices that failed the roll, remain associated with the original Credentials.

## Editing global Shared Credentials

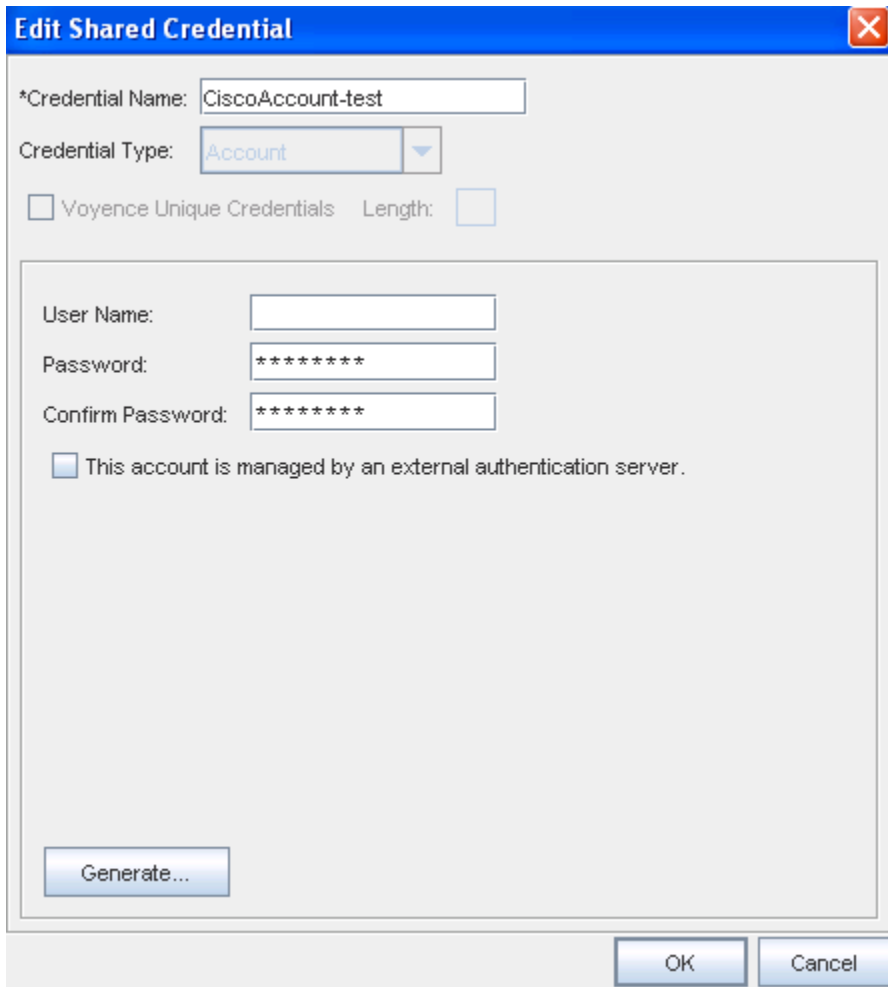
To edit a shared or local credential,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Global -> Credentials Manage, then Credentials**. The **Global Shared Credentials** window displays, with a listing of pre-assigned, shared credentials.



At the bottom of the window are the View Associations, Roll, Add, Edit, and Remove buttons, along with the Close option.

- 3 Select a credential from the list, then click **Edit** to display the Edit Shared Credential window.



- 4 Make any changes to the existing information in each section, based on the Credential Type you selected when you created the credential.
- 5 Click **OK** to save your edits.

**Notes:**

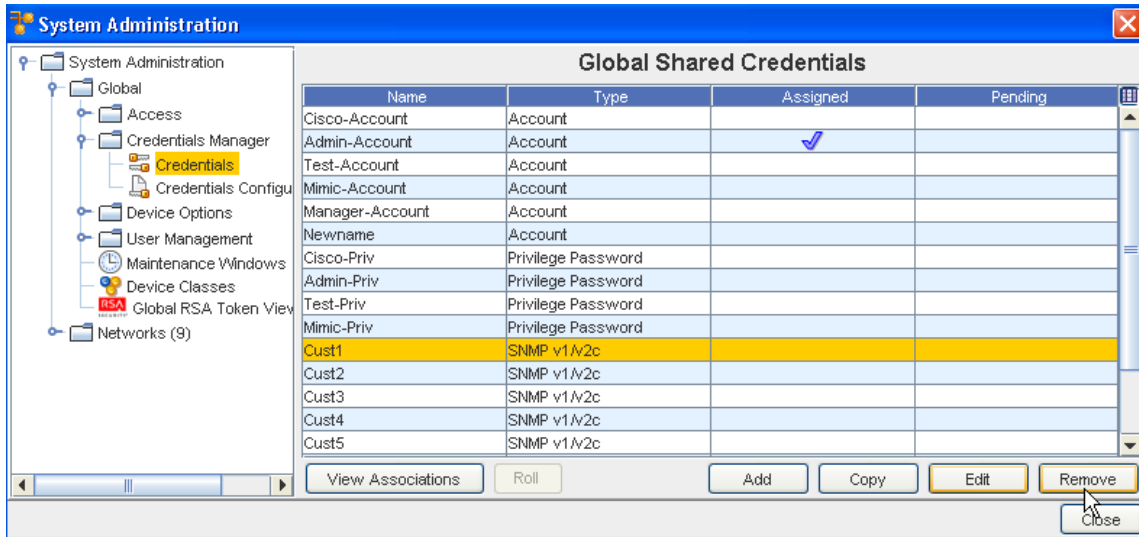
- The updating credentials process requires that an account be associated with a device. This account is used to establish the initial session into the device to make the credential updates.
- This manual process creates an association with the credential, and the local device to represent the username/password that is present on the device.
- If an Autodiscovery is made with an established account credential, the manual process of association is not required. The Communication tab on a device contains the account association for the Primary In-Band mechanism.

See [Global Shared Credentials Options](#) for more information.

## Removing Shared Credentials

To Remove a shared or local credential,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Global -> Credentials**. The **Global Shared Credentials** window displays, with a listing of pre-assigned, shared credentials.



At the bottom of the window are the View Associations, Roll, Add, Edit, and Remove buttons, along with the Close option.

- 3 Select a credential from the list, then click **Remove**.
- 4 At the Confirmation message, click **OK**.

See [Global Shared Credentials Options](#) for more information.

## Prompt User

While **User Login** helps for authorization for the operations performed on the device, there are scenarios where users need to provide the **passwords** at the time of the operation. Here are a few scenarios:

- **Rolling Passwords** – lots of accounts incorporate the rolling passwords where the password is only valid for a certain configured time. In such cases, the prompting is required for those accounts.
- Another scenario would be when the Network Administrator is assigned a temporary account to make the changes during a well-defined maintenance window. This account expires after this maintenance window. Prompting the user comes handy in these cases.
- **Authorization Granularity** - There are times when certain users may not be allowed to execute certain commands – in other words, the authorization is done at the granularity of a command and it may so happen that certain users may need to use a different account to make certain changes, and cannot be tied down with the high level configuration.
- **NOC Users** – There are times when a Network Operations Center (NOC) user has to execute a job (for example, Run as Operator Initiated), although the job may have been scheduled and approved by another user.

All of the above scenarios warrant the need to **prompt the user** .

The Network Administrator always has the need to override the configuration at a per operation basis – in other words, the flexibility to deal with special and exception scenarios to manage certain devices .

This may depend on the role and the privileges of the user. There are also times when certain operations have to be performed to repair the state of the network, and this needs to be done without disturbing the current configuration.

### Additional Prompt User Information

Network Configuration Manager has provided a way to control **dynamically** the credentials used for any device operation. This is encapsulated as part of configuration that is exposed to the administrator.

The credentials include the following (note all of them can be optional, depending upon the target device):

- Account Name
- Account Password
- Privilege Password

---

**Note** The privilege level is not necessary, as most of the time the TACACS server determines the privilege level based on the login credentials. Also, at least one of the credentials is required by the device.

---



Depending upon the configuration, the system uses the appropriate credentials for the device to perform the task. If there is a need to prompt the user, the system will do so.

- The configuration does not apply for devices whose access is controlled through SNMP.
- The credential configuration does not apply for "pull" jobs – statically assigned device credentials will be used. Similarly, all automated pulls shall use the shared credentials assigned to the target device.
- When a copy of the job or task is made, the device credentials are copied to the new job or task.
- All credential related information stored in the database is encrypted. The same applies for credentials in transit between the application tiers.
- All credentials that are persisted or cached as part of the job will be discarded after the task request is sent to the target device servers.
- If multiple devices are selected for a "Non-Scheduled" operation, and if it requires that the user be prompted for the credentials, the same user input credentials are used for all devices targeted.
- If multiple tasks (devices) are involved in a job, and the job requires that the user be prompted for the credentials, the same user input credentials are used for all devices.
- If the job is modified, the system invalidates the credentials if it existed, and causes the job to go through the same semantics as if no credentials were yet provided for the job.
- The system provides the user the ability to override the credentials for a job or other non-scheduled operations. This enables the Network Admin to deal with exception scenarios where one user has to perform an operation on another's behalf.
- Only users with "Override Credential" permission are allowed to update the credentials. The override ability is available as part of the scheduler. Any new credentials entered simply replace the existing ones if any.
- All password information transmitted over the wire between the client and the server is encrypted to prevent snooping.
- For cut-through operations, device level assignment (specifically –Network Configuration Manager! Account– and "User Prompt") take precedence over the global or network configuration.
- API clients have the ability to specify device level credentials as part of every device operation – scheduled and non-scheduled. However, these credentials are only taken into account if the configuration is set up for "User Prompt" or the API user has the appropriate privileges to override at an operation level.

## Global - Device Options

### Device Naming Overview

A consistent naming convention for the Devices is now provided. This ensures that the name of the device remains constant throughout naming-related operations, such as Search, Resync, and Filtering.

The **Device Name** of a device is the name you view and use to work with the Device throughout Network Configuration Manager.

Previously, a device name could be one of the following:

- hostname
- FQDN
- Alias

However, using these as the actual device names did not ensure that there was a consistent name used for the device when completing naming-related operations. For example, when using Search, the device name could also be classified as the hostname, or the device Alias, or FQDN.

Now, there is only one **device name** to use when searching for the device. This device name is still derived from a hostname, a device Alias or a FQDN, but now you have the ability to control which of these three options you want to use as the device name. You can now designate the device name as a device Alias, a hostname, or FQDN by using the Device Naming Scheme.

- [Device Naming Update](#)
- [Device Naming Scheme](#)
- [Device State Options](#)

## Device Naming Update

---

**Note** You must have System Administration privileges to change any update options in the Device Naming Update window.

---

To ensure that the hostname or FQDN does not get changed, use this window. When this window is accessed, the **default** (Always) is already selected. This allows you to have control over **when** any device gets updated throughout the application.

- For example, when a **hostname or FQDN** is changed (by a Network Admin), and if the default is marked as **Always**, the hostname or FQDN gets updated. If the default is **Discovery** or **Never**, the hostname or FQDN will never (**NOT**) get changed .
- If **Discovery** is selected, the hostname will only be updated during an Auto Discovery procedure.
- If **Never** is selected, the hostname will never be changed - after the initial Auto Discovery procedure.



Using this naming update procedure allows you to control when the hostname or FQDN of a device within the Network Configuration Manager application is changed.

To Define Name Update Options,

- 1 In the Update Options section, select from the following by clicking within the appropriate radio button. Select:

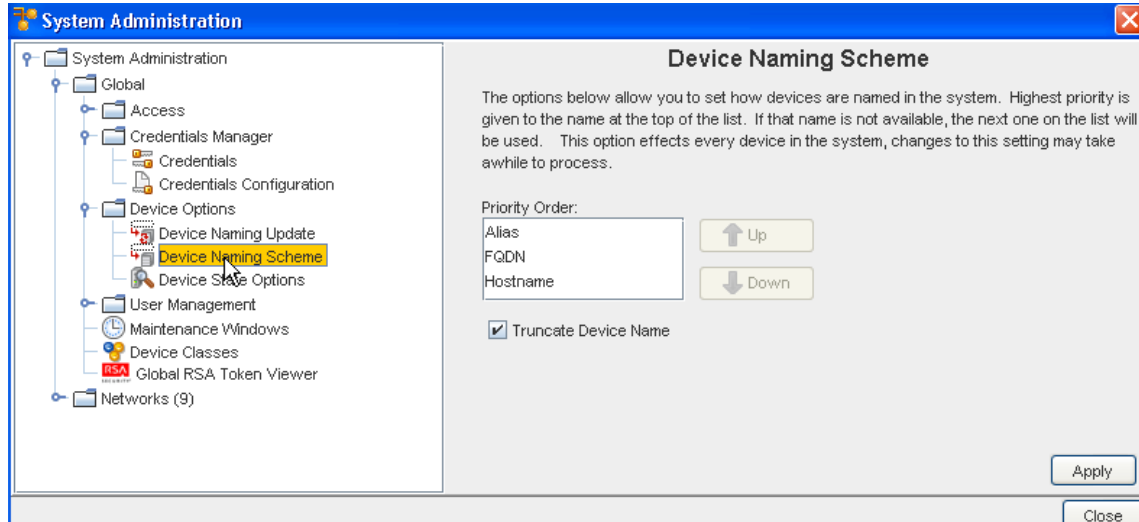


- **Always** - indicating that the hostname or FQDN name will be changed automatically when there are changes detected in the device.
- **Discovery** - indicating the device hostname or FQDN will change only after auto discovery has successfully completed.
- **Never** - indicating that the device hostname or FQDN will remain the same, no matter what device changes occur.

- 2 After making your selection on this window, click **Apply**.

## Device Naming Scheme

**Note** You must have System Administration privileges to change any update options (the Naming Scheme) in the Device Naming Update (Scheme) window.



Use this Device Naming Scheme to determine **how** the device name is generated from one of these three names of the device. For example, if you prefer to use **Alias** for the device name, you select Alias as the highest priority by making sure Alias is shown in the top position of the Priority Order list (as shown in the following graphic).

When you select a device name (Alias, FQDN, or Hostname) you must determine the priority order you want Network Configuration Manager to use when naming the device. As displayed in the graphic, Alias is the first priority (default), then FQDN is the second priority, with Hostname being the last priority you want Network Configuration Manager to use when naming the device.

You have several combinations of these three priority orders to select. Each combination could make the name of the device different.

For one example:

- If a device has the following names; **Alias** (XX), Hostname (YY) and FQDN (ZZ), using the default priority order, using Alias as the top priority, the device name of this device would be XX.
- If you change the top priority order to use **FQDN**, the device would be ZZ.
- If you change the top priority order to use **Hostname**, the device would be YY.

Another example would be:

- If a device has the following names; Hostname (YY) and FQDN (ZZ), using the default priority order, you would still use the default priority. Network Configuration Manager uses the designated priority (Alias, FQDN and then Hostname) to name the device. Not finding Alias

as a name for the device, Network Configuration Manager would then go to the next priority order (FQDN) and use that as the device name. Subsequently, if neither Alias or FQDN is available as a device name, Network Configuration Manager uses Hostname as the device name.

- The hostname is always available for every device in Network Configuration Manager. The device name will always be resolved, resulting in a device name for every device.

Once the order is determined, Network Configuration Manager attempts to assign the device name following the order you specified.

### Device Naming Scheme

The options below allow you to set how devices are named in the system. Highest priority is given to the name at the top of the list. If that name is not available, the next one on the list will be used. This option effects every device in the system, changes to this setting may take awhile to process.

Priority Order:

Alias	▲ Up
FQDN	
Hostname	▼ Down

Truncate Device Name

Apply

To Select a Device Name,

- 1 Select the **naming scheme** from the Priority Order list. Use the Up and Down arrows to move your naming scheme to the top of the list.
- 2 After making your selection, click **Apply**.

## Device State Options

The Device Server Properties window is available from:

- **Menu bar -> System Administration**
- **Global -> Access -> Device Options -> Device State Options**



You indicate, by entering a number into the field, how many attempts (the maximum) you want to limit on device task communications, using the Device communication properties field.

To Define communication properties,

- In the Device Communication Properties section of the window, note that the default is **5**.
- To change the number of attempts a device can go through a task and fail (and have no additional attempts), enter the **appropriate number**. When this number is met, the device will have a No Communications icon in the State column of the Devices view. This indicates that all attempts (allowed) have failed to complete the task (such as Pull, Push, Cut-through, etc.) successfully.
- Click **Apply**.




---

**Important** Go to the **Event Manager** and view the details on this communications problem, and address the issue as needed.

---

## Global - User Management

## User Management Overview

The User Management module is designed for managing users and their access to the Network Configuration Manager application, and to the networks. Under User Management you can:

- Define external authentication services, such as TACACS+, RADIUS and LDAP
- Create users and set their authentication preferences
- Manage users and groups
- Create group assignments
- Establish default network permissions for users and groups
- Create permission policies to associate protected resources (such as networks and devices) with users and groups
- Lock and unlock user accounts
- Change passwords for users in the Network Configuration Manager native registry
- Work with NCM RSA Services and RSA Tokens

Network Configuration Manager user security is segmented into two components:

- **Authentication services** , providing login access to the application itself
- **Authorization services** , which allows access to networks and devices managed by Network Configuration Manager

Authentication is provided via an external TACACS+ or Radius server, or through the Network Configuration Manager Native Registry. When creating user access to the application, you must first designate how they are authenticated during login; either via one of the external mechanisms, or via the application's native registry. No account passwords are required for external user authentication, as Network Configuration Manager passes the user credentials to an external authentication server.

Access to different networks, devices, and modules in Network Configuration Manager is handled by a robust, secure authorization system. Users and groups can be given default permissions that apply to all networks , or each network can be provided with a set of permission overrides. Global device overrides can also be granted to users and groups for the purpose of managing individual devices.

For more information on setting up authentication mechanisms in Network Configuration Manager, see [Setting up the TACACS+ Server](#) and [Setting up the Native Registry](#).

The User Management module allows the following functions to be completed:

### Manage System Users

- [Creating Users](#)
- [Editing Users](#)
- [Removing Users](#)

- [Managing User and Group Device Permissions](#)
- [Locking and Unlocking Users](#)
- [Managing User Groups](#)
- [Managing User Permissions](#)

### Manage System Groups

- [Creating Groups](#)
- [Edit Groups](#)
- [Set Group Permissions](#)
- [Delete Groups](#)

### Manage Permissions

- [Setting System Level Permissions](#)
- [Setting Network Level Permissions](#)
- [Setting Workspace Permissions](#)
- [Setting Device Level Permissions](#)

## Working with System Users or Groups

### Creating Users

System users are users that are authorized to have access to the application for the purpose of network configuration and maintenance. Before any user can be included in a System Group, they must first be added to Network Configuration Manager. Once entered into the system and assigned privileges, the user is given access to specific networks and their devices.

When a user is created, the user is either assigned permissions as a *single user* or *included in a group*, where the group is assigned privileges as a whole.

There are four methods of authentication that are used by Network Configuration Manager:

- **Validation by an external TACACS+ server**, the default - user's that are validated against the TACACS+ server must be entered onto the TACACS+ server **before** attempting to log into the application.
- **Validation by the Native Registry** - when a user's access is to be validated by the native registry, you must enter a password along with the User ID. The combination of the User ID and the password provides access to the application.
- **Validation using RADIUS** - a protocol for carrying authentication, authorization, and configuration information between a Network Access Server, which desires to authenticate its links, and a shared Authentication Server



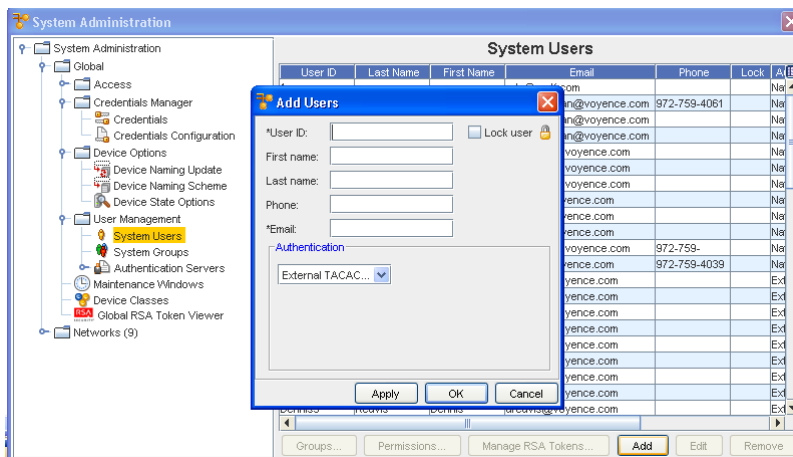
- **Validation using LDAP Server** - a protocol for carrying authentication, authorization, and configuration information between a Network Access Server, which desires to authenticate its links, and a shared Authentication Server

**Note** The **Changing Your Password** is available in Native Registry only. For all other instances for changing a password, you must contact the server administrator.

Each user in Network Configuration Manager must have a user record that is to be associated with its network authorizations. Users can authenticate using one of the three available external authentication servers, or via the Network Configuration Manager native registry. Users can be given individual permissions, or can inherit permission as members of groups.

To create a new user,

- 1 From the menu options, select **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand **Global -> User Management**.
- 3 Click **System Users** to see all authorized system users displayed.



- 4 At the bottom right of the window, click **Add**. The Add Users window opens.

**Note** Required fields are indicated by an asterisk.

- 5 At a minimum, enter information in the required fields (User ID and Email).
- 6 At the Authentication section, the RADIUS, LDAP and TACACS+ server options require only input of the User ID and Email. By default, the External TACACS+ server is the primary option, if this is okay, click **Apply**. The window refreshes ready for input of another user profile. **Or**, if you would like to set up the user to be validated by the Native Registry in the Authentication section, select **Native Registry** from the drop-down menu. The Password fields display.
- 7 Enter a **password**.
- 8 To validate the password, re-enter it in the \*Confirm Password field, then click **Apply**. If there are no additional users to be entered, click **OK**. The last user entered is saved, and the Add User window closes.

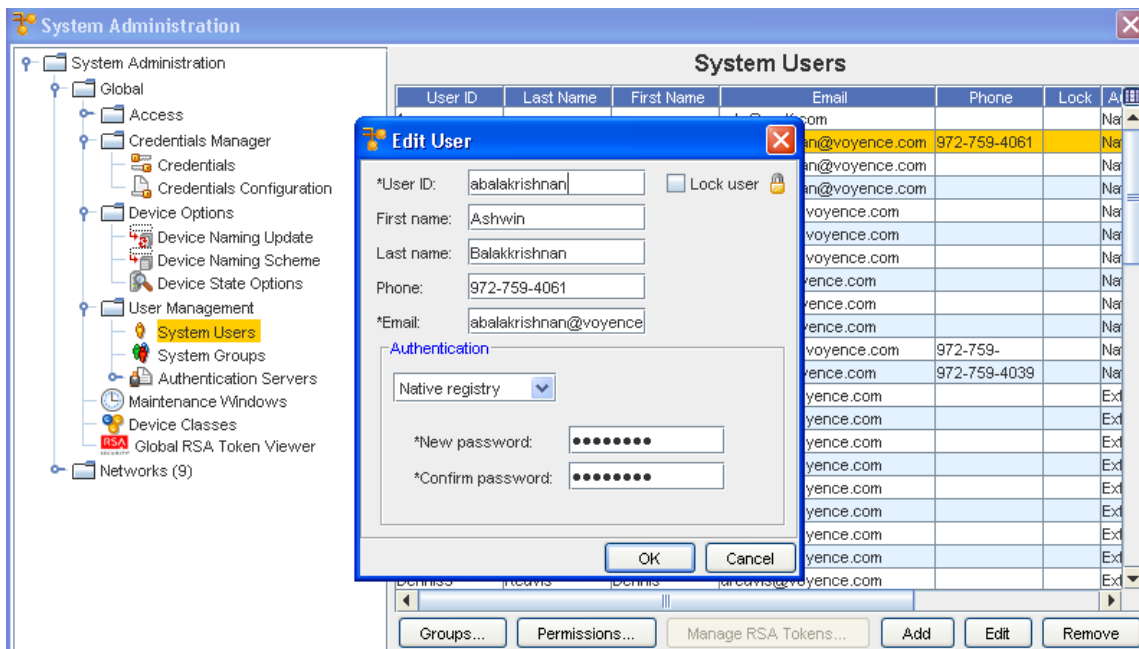
You are now able to [Setting User and Group Permissions](#) or manage groups for the users.

## Editing Users

Part of managing users is the ability to edit the profile for users as needed. After a user has been added to Network Configuration Manager, they have a profile that can be edited.

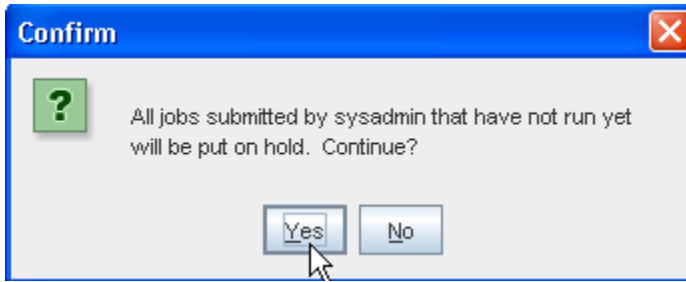
**Important** If the user is being validated by an external server, TACACS+, LDAP, or Radius, the user's ID must match the ID on the server. If not, the user is not able to access Network Configuration Manager.

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand **Global -> User Management**.



- 3 Click **System Users** . All authorized system users display in the right pane of the System Users window.
- 4 From the list of authorized users, select the **user**.
- 5 At the bottom right of the window, click **Edit**. The Edit User window opens.
- 6 At a minimum, any required fields must contain information (User ID and Email).
- 7 If you are locking the user out of the application, click **Lock User**. Or, if the user has previously been locked out of the system, de-select the **Lock User** box to allow the user access to the application.
- 8 Make changes to the available fields as needed.





The user's profile is removed from the list of authorized users.

### Locking and Unlocking Users

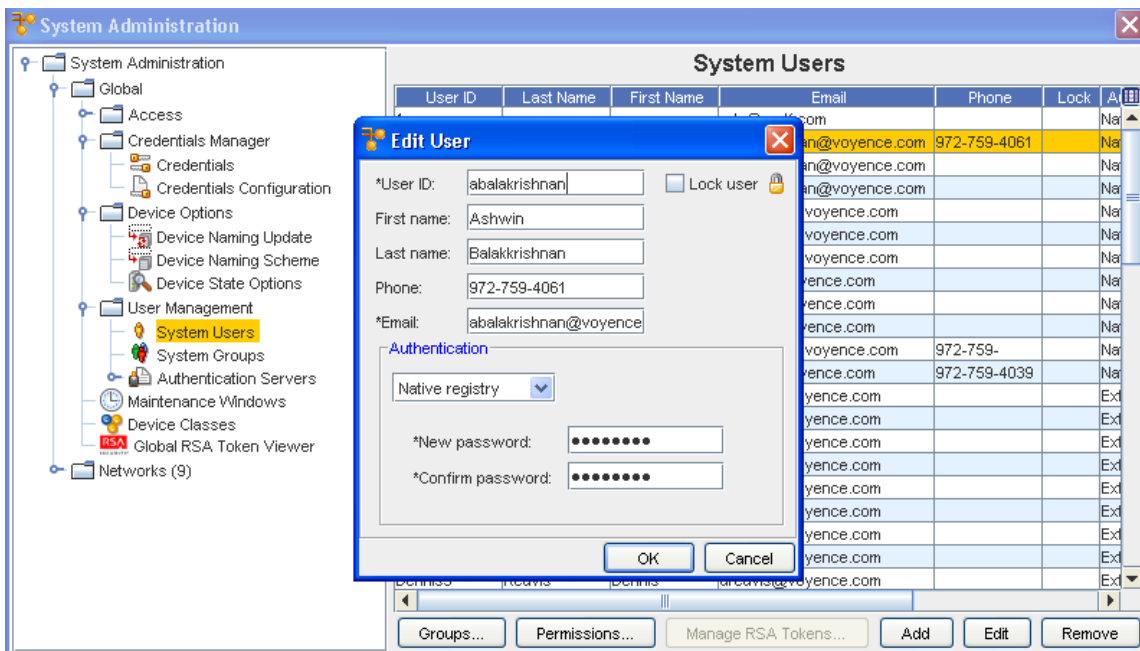
As an added **safety feature**, a user can be locked out of Network Configuration Manager. There are two ways a user can be locked out of the application:

- A user can be locked out the system by the system administrator.
- A user can be locked out when they have attempted to login multiple times, and the login attempts have failed.


If either of these scenarios occur, you must open the user's profile and unlock the user.

To lock a user profile,

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand **Global -> User Management**.
- 3 Select **System Users** . All authorized system users display in the right pane.
- 4 Select the **user**.



- 5 Click **Edit**.
- 6 In the upper right corner, click in the **Lock User** box.
- 7 Click **OK**. The Edit Users window closes.

In the System Administration window, the last column of the user's row now contains a Lock  icon, indicating that a lock has been placed on the user's profile.

To unlock a user profile,

If the user has been locked out of the system, a lock displays in the Lock column of the System Administration window, and on the user's profile, the Lock User box is checked.

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand **Global -> User Management**.
- 3 Select **System Users**. A listing of all authorized system users is displayed in the right pane.
- 4 Select the **user**. Click **Edit**. The Edit User window displays.
- 5 De-select the **Lock User** box (by clicking within the box to remove the check mark).
- 6 Click **OK**. The Edit Users window closes.

In the System Administration window, the user's profile should no longer have a lock in the Lock column.

## Creating Groups

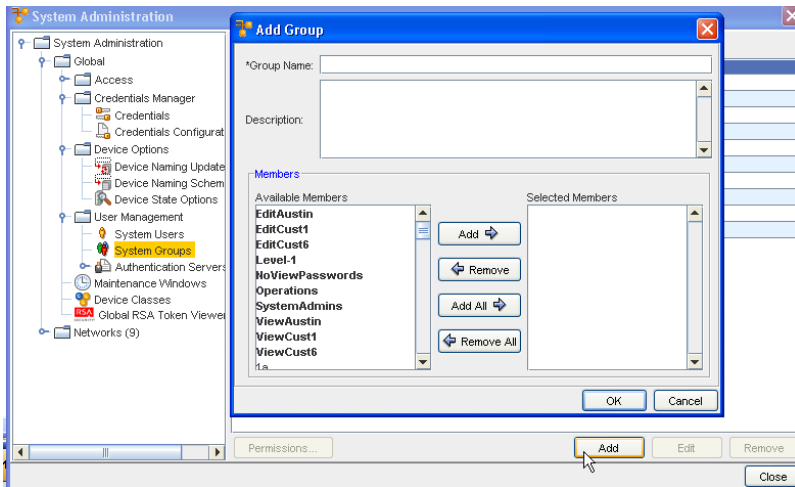
Unlike users, groups are just containers for creating relationships between users and other groups, and do not offer authentication or have passwords. Groups, like users, can have permission relationships with networks and devices.

For ease of security management, Network Configuration Manager recommends that you create permission groups for your users, assigning your users to the appropriate permission group.

A System Group is a defined group of users that have the same permission levels in the networks. System groups can be nested within other system groups. Nesting allows one group to "inherit" the permissions of the group in which it is nested. The nesting helps ensure that access permissions remain consistent, and decreases the time required to manually assign each user individual permissions.

To create a new group,

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand **Global -> User Management**.
- 3 Select **System Groups**. The right pane contains all available groups.



- At the bottom of the window, click **Add**. The Add Group window opens.

---

**Note** You can now add a **Description** to the Group information. Once entered, this description information is displayed in the System Groups window.

---

- If needed, enter a **Description**.
- In the Available Members column, select the **groups and users** to be included in the new group.

---

**Note** A sequence of groups or users can be selected by holding down the Shift key while clicking groups. Or, multiple, non-sequential groups or users can be selected by holding the Ctrl key while clicking groups.

---

**Important** If the users have not yet been created, continue to the next step. You can manage users to groups later.

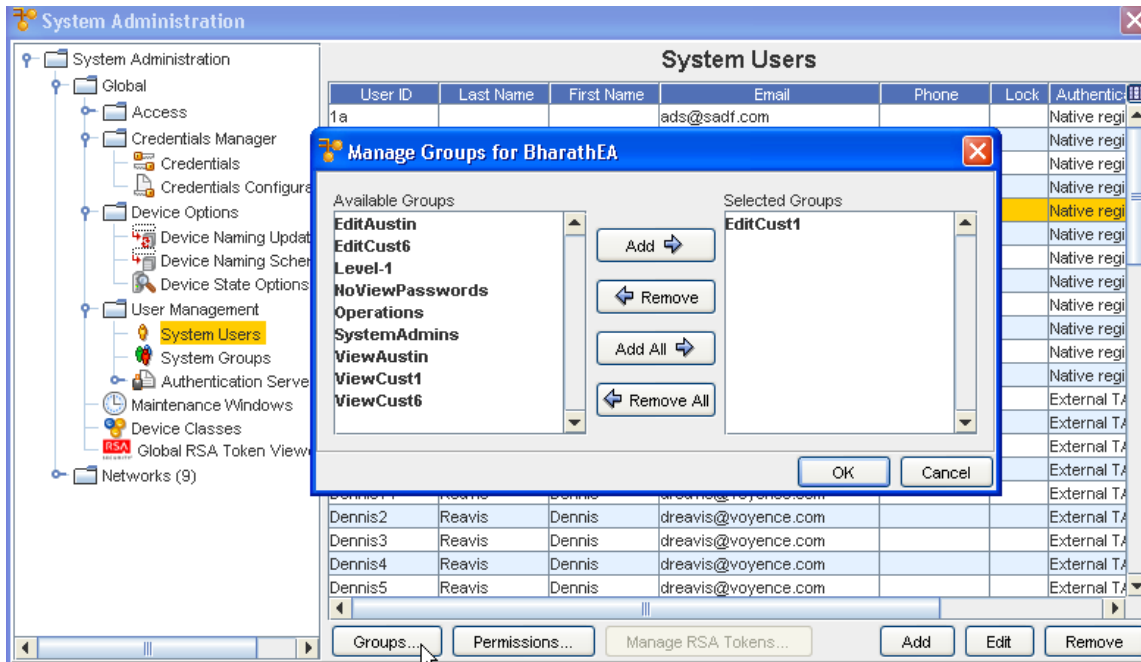
---

- When finished, click **OK**. The Add Group window closes.

Once a group is created, permissions for the group must be set. See [Set Group Permissions](#).

### Managing User Groups

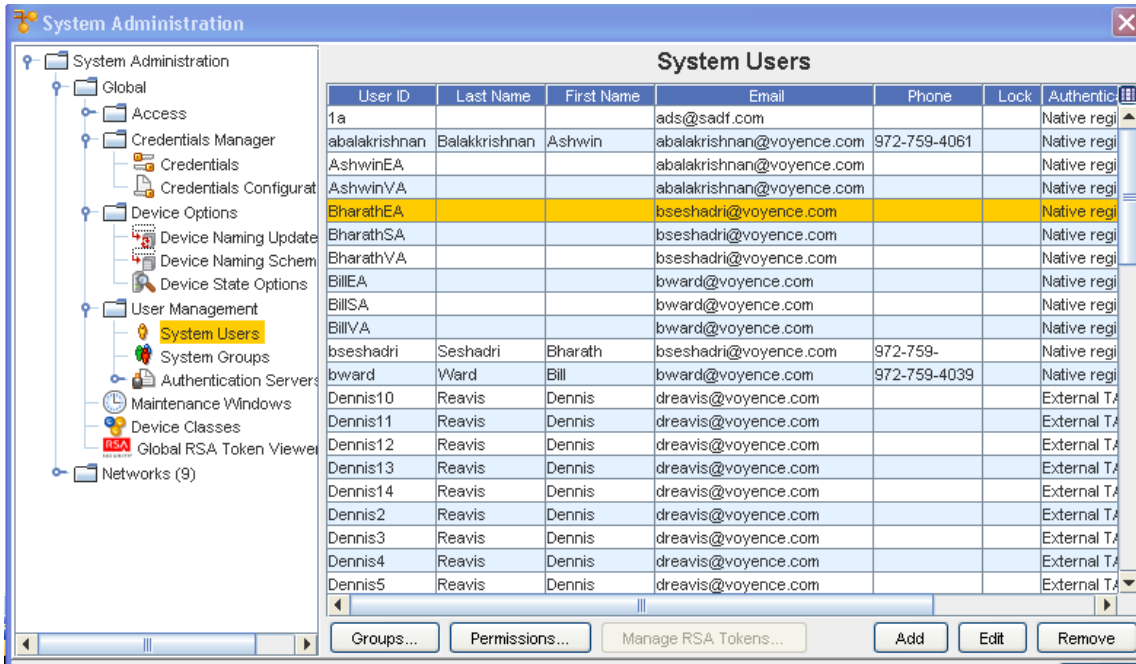
- From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- In the navigation pane, expand **Global -> User Management**.
- Click **System Users** . All authorized system users display in the right pane of the System Users window.



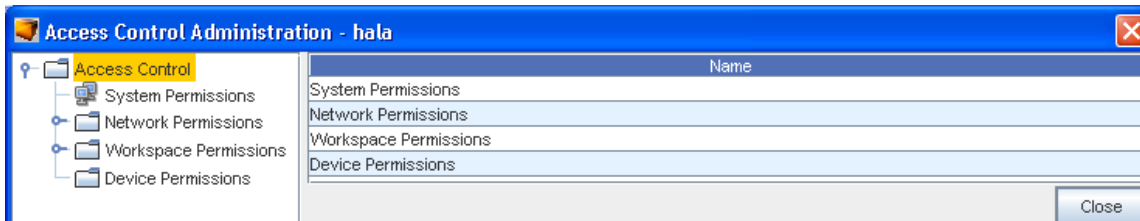
- 4 From the list of authorized users, select the **user**.
- 5 At the bottom of the System Users pane, select **Groups**. The Manage Groups (for the user you selected) now opens. From this window, you can select to **Add** Available Groups, or **Remove** previously Selected groups for this user by making selections from either pane, then using the arrows.
- 6 Click **Ok** when you have made your selections.

### Managing User Permissions

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand **Global -> User Management**.
- 3 Click **System Users**. All authorized system users display in the right pane of the System Users window.



- From the list of authorized users, select the **user**.
- At the bottom of the System Users pane, select **Permissions**. The Access Control Administration window (for the user you selected) now opens.



- From this window, you can work with permissions for this user. See [Setting User and Group Permissions](#) for more information.

## Working with Permissions

### Setting Network Configuration Manager Permissions

Network Configuration Manager security is segmented into two components:

- **Authentication services** , providing login access to the application itself
- **A uthorization services** , which allow access to networks and devices managed by the application



**Authentication** is provided via an external TACACS+ server, or through the Network Configuration Manager Native Registry. When creating users that require authorized access to the application, you must *first designate how they will be authenticated during login*, via one of two mechanisms, an external TACACS+ server, or the internal Native Registry. Then, access to the different modules of the application is controlled by a flexible, secure authorization system.

---

**Note** For more information on setting up authentication mechanisms in Network Configuration Manager, see the sections on [Setting up the TACACS+ Server](#) and [Setting up the Native Registry](#). This section describes how the Network Configuration Manager authorization system is implemented and managed.

---

**Authorizations** provides each user with access security, based on their network roles. Authorizations allow secure access to all protected resources within Network Configuration Manager including networks, devices, jobs, and workspaces. Authorizations can be granted to users or groups on a default, or on a per-resource basis.

For security management purposes, it is recommended that "like users" be placed within groups. Groups could then be provided with a set of default authorizations for all the resources they control. Network Configuration Manager recommends (for ease of management) that you deploy authorizations for your network at the group level. In this way, security management for all users in the group can be handled at one time, with a single change. However, individual users can also be granted permissions, and if desired, a customized environment can be created in which each user is provided separate access authorizations to each resource.

It is important to note that due to the great flexibility of the authorization scheme within Network Configuration Manager that permissions can be defaulted, implicit, explicit, inherited, summed, and overridden, thus encouraging great care be taken in planning the correct approach for deployment in your environment.

The following are examples offered for clarification.

<b>Default Permissions</b>	Each user and group has a set of default network and workspace permissions (called the Default Network and Default Workspace, respectively), that when set, apply those access lists to any network or workspace associated with the user or group.
<b>Implicit Permissions</b>	Permissions granted at the system level are granted implicit to all networks, regardless of the networks assigned to the user or group.
<b>Explicit Permissions</b>	Any permissions granted at the device level explicitly override any grants to that device given at the network or system level.
<b>Inherited Permissions</b>	Any user or group placed into another group having access permissions to a protected resource, will inherit those permissions as well.

<b>Permission Summation</b>	Users or Groups can be placed in group relationships in such a way they obtain the sum of permissions to a protected resource. For example, if a user is placed in a group that has View, Edit, and Schedule access to Network A, and into a group that has Approve access for Network A, the user effectively then has View, Edit, Schedule and Approve permissions in Network A.
<b>Override Permissions</b>	Continuing with the example above, if the user was also associated directly to Network A and given an override permission of View Only, the user would lose all other access to Network A, except for the override permissions. This rule applies to any user or group where the override check box has been selected. This, then overrides any other access provided to the protected resource.

All permissions are granted at the following levels:

<b>Setting System Level Permissions</b>	Highest level of permissions in Network Configuration Manager. System Level Permissions allow you to manage networks, users and groups, access for users, System Administration, and more.
<b>Setting Network Level Permissions</b>	Each user or group must be associated to a network, prior to having permissions for the network defined. A default network provides the ability to associate the same rights to any network assigned to the user or group. Any changes to the default network affect all associated networks that do not have overridden authorizations.
<b>Setting Workspace Permissions for Each User and Group</b>	Permissions can be set to allow specific users or groups to have access to design workspaces that have been created for the network. A default workspace provides the ability to associate the same rights to any workspace assigned to the user or group. Any changes to the default workspace affect all associated workspaces that do not have overridden authorizations.
<b>Setting Device Level Permissions</b>	Each device within Network Configuration Manager can have its own set of authorizations. Any authorizations provided at the device level override all other permissions. For example, giving a user device level permissions will deny access to any other user that has access to that device at the network level.

The **User Management** module is where all permissions originate. The user or group is created and defined in this module.

<b>Managing User Permissions</b>	User permissions define the authorizations to protected resources granted to an <b>individual user</b> of the application.
<b>Managing User Groups</b>	Identical to user permissions, but assigned at the <b>group level</b> , group permissions define a group to protected resource authorizations.

## Best Practices when using Permissions

Contained within this information are the Best Practices for setting up user permissions in Network Configuration Manager.

**Important** It is recommended the creation of **six distinct user groups** to accommodate the division of responsibilities as it pertains to managing compliance and configuration management for your network.

The recommended groups are specific to the following responsibilities:

- Super User for the application (Administrator group)
- Viewing of configuration information (Viewers group)

- Submission of proposed change (Submitters group)
- Approval of change (Approvers group)
- Creation of standards (Standards group)
- Auditing change (Auditors group)

Each group, when established, must be managed. In addition, any network associated with the group must also be managed.

### **Administrator Group**

Users assigned to this group have the ability to make changes throughout the system. The number of users assigned to this group should be dictated by internal security policies. When setting up the group, enable Systems Administration under Systems Permissions.

### **Viewers Group**

Users assigned to this group have read only views of network devices for all assigned networks.

When setting up this group, ensure they have no rights under System Permissions.

Under Network Permissions, for the default Network, ensure only the following are enabled:

- Network – View
- Workspace – View
- Device – View Details

Under Workspace Permissions, for the default Workspace, ensure only the following are enabled:

- Workspace – View
- Device – View Details

### **Submitters Group**

Users assigned to this group have the ability to schedule jobs, run cut-throughs, and perform OS upgrades.

When setting up this group, under System Permissions, enable Schedule permissions.

Under Network Permissions, for the default Network, ensure the following are enabled:

- Network – View Details
- Workspaces – Create, Edit, Delete
- Device – Create, View Passwords, Manage OS, Assign Credentials, View Details, & Run Cut-Throughs
- Job – Schedule
- View – Create, Edit, Delete

Under Workspace Permissions, under default Workspace, ensure the following are enabled:

- Workspace – Edit, Delete

- Device – Create, Manage OS, Assign Credentials, Run Cut-Throughs, View details
- Job - Schedule

### **Approvers Group**

Users assigned to this group have the ability to schedule and approve jobs.

Under Systems Permissions, ensure that Job Approval is enabled.

Under Network Permissions, for the default Network, ensure only the following are enabled:

- Network – View
- Device – View Details
- Job – Approve

Ensure the Users assigned to this group do not have Workspace permissions.

### **Standards Group**

The Standards group should have the following Systems permissions enabled:

- Manage Templates
- Manage Queries
- Manage Compliance Standards

Under Network Permissions, for the default Network, ensure the following are enabled:

- Manage Templates
- Manage Queries
- Manage Compliance Standards
- Network – View
- Workspaces – View
- Device – View Details

Under Workspace Permissions, under default Workspace, ensure the following are enabled:

- Workspace – View
- Device – View details

### **Auditors Group**

The Auditor group should be given system permissions to view the event manager.

Under Network Permissions, for the default Network, ensure the following are enabled:

- Network – View
- Workspaces – View
- Device – View Sensitive Data, View Details

Under Workspace Permissions, under default Workspace, ensure the following are enabled:

- Workspace – View
- Device – View details

## Setting User and Group Permissions

Authorizations are access control relationships between non-protected resources, such as users and groups, and protected resources, which includes networks, workspaces, jobs, and devices.

Creating associations between non-protected resources and protected resources can be initiated either by accessing the user or group and assigning it a protected resource, or by accessing a protected resource such as a network or device, and assigning a user or group to it.

The authorizations, or access controls between users or groups, and the protected resources within Network Configuration Manager are always created within User and Group Management.

Each user or group can be assigned a set of system, network, workspace and device permissions. By design, system permissions are global to the application and are implicit to all protected resources in the application, regardless of those resources assigned to the user or group.

*Device permissions* however, are explicit authorizations granted between a user or group, and a device. Any device permissions override all other permissions, superceded any network or system level permissions.

For networks and workspaces, default authorizations can be provided that will apply to any network or workspace assigned to the user or group. These permissions are assigned in either the default network, or default workspace created for each user or group. Then, when a network or workspace is associated with a user or group, these access controls will be automatically created.

However, any network or workspace can be granted customized access different from the defaults, by choosing to *override the defaults*. No defaults need to be set if you choose to define the customer access authorizations for all access to protected resources. Within users and groups, the four permission levels are:

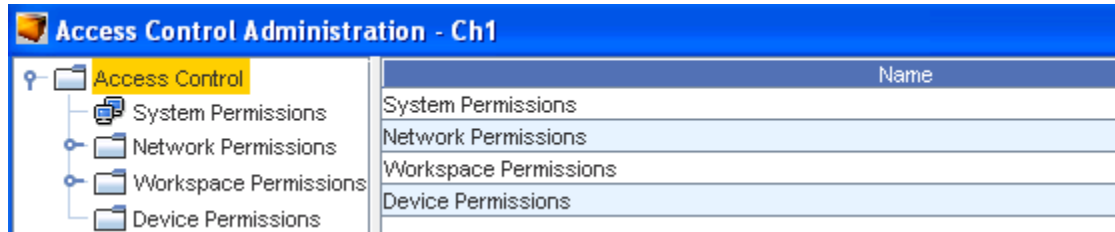
- [Setting System Level Permissions](#)
- [Setting Network Level Permissions](#)
- [Setting Workspace Permissions](#)
- [Setting Device Level Permissions](#)

Each level provides the user with permissions that dictate what actions the user is able to complete when using Network Configuration Manager. User settings are indicated by checking options. When an option does not have a check mark, the permission is not available to the user within the application.

To manage the permissions for users and groups,

- 1 In the menu bar, open **Tools > System Administration**.

- 2 Select **Global -> User Management** .
- 3 Expand **User Management** , then select **System Users** or **System Groups**. All authorized system users or groups display in the right pane.
- 4 Scroll the user or group list, locate, then click the **user or group name**.
- 5 At the bottom of the window, click **Permissions**. The Access Control Administration - [CH1] window opens.



The left pane of the Access Control Administration - [ID] window is an expandable tree menu. Within the tree menu are separate branches for each permission level.

All device, networks, systems, and workspaces associated with the user or group display under their respective branches. When selected, the permission settings for each device, network, system or workspace display in the right pane.

### Setting System Level Permissions

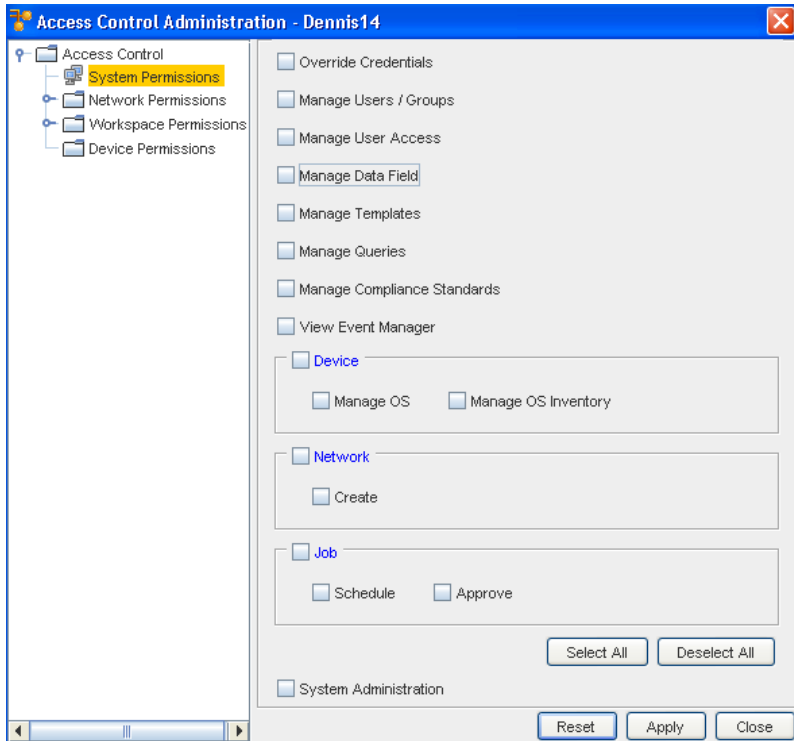
System level permissions provide users the ability to access some or all of the features within System Administration, Automation Library, Event Manager, and OS Image Management.

From within System Permissions, you can create user roles such as, System Administrators, Network Administrators, Policy Managers, and Auditors.

System permissions defines the actions that a user or group is able to complete at the *system level*. System level permissions are independent of the networks or workspaces associated with a user or group. For example, by granting a user or group Job Approve at the system level, the user or group could then approve jobs submitted for any network within Network Configuration Manager.

To set system permissions for a user or group,

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand **Global -> User Management**.
- 3 Select **System Users** or **System Groups** . The right pane contains all available user/groups.
- 4 Select a **user/group**, then click **Permissions**. The Access Control Administration - [User ID name] window opens.
- 5 In the tree menu, select **System Permissions**. The right pane populates and appears like the following:



**Note** System Administrator permissions include not only the listed permissions, but permissions to complete **all tasks** in Network Configuration Manager.

**Note** By default, when a user/group is given permissions to View Networks and Workspaces, they are able to View their devices.

- 6 Assign the system level privileges for the user/group, selecting the areas for which the user/group should have access.
- 7 If the user/group does not require one or more of the included task permissions, click that **related check box** to de-select the option.
- 8 Repeat **steps 6-7** for each area to which the user requires access.
- 9 If a user requires access to all options in the Access Control Administration window, click **Select All**. You can also click **Deselect All** to begin without any selections checked.
- 10 When finished, click **Apply**. The window remains open allowing you to set other permissions. Or... If you are not making changes to the other permission level settings, click **Close**.

<b>Override Credentials</b>	Allows you to set the permission for the user to update the existing credentials
<b>Manage users/groups</b>	Allows the user/group system level privileges to manage users and groups
<b>Manage user access</b>	Allows the user/group system level privileges to manage access for other users
<b>Manage Data Field</b>	Allows the user/group system level permission to manage Data Fields
<b>Manage Templates</b>	Allows the user/group system level privileges to create or modify templates that reside in the Automation Library. By default, you can view existing templates.

<b>Manage Queries</b>	Allows the user/group system level privileges to create or modify queries that reside in the Automation Library. By default, you can view existing queries.
<b>Manage Compliance Standards</b>	Allows the user/group system level privileges to create or modify Compliance Standards
<b>View Event Manager</b>	Allows user/group to view all Events that have occurred
<b>Device - Manage OS or Manage OS Inventory</b>	Allows the user/group system level privileges to create or modify OS or OS Inventory
<b>Network - Create</b>	Allows the user/group system level privileges to Create a network
<b>Job - Schedule/Approve</b>	Allows the user/group to Schedule or Approve a job
<b>System Administration</b>	Allows the user/group level the access and the privileges of a System Administrator

To change system permissions for a user,

Once permissions have been set, they can be edited as the role of the user/group changes. Permissions are changed by editing the set of permissions currently selected for the user/group.

- 1 After selecting a user/group, open the Access Control Administration - [UserID] window.
- 2 Select **System Permissions** . The right pane populates with the current permission settings for the user.
- 3 Make the changes by selecting and de-selecting from the available options .
- 4 When finished, click **Apply**. The window remains open allowing you to edit other permissions. Or, if you are not making changes to the other permission level settings, click **Close**. The System Administration window is active.

### Setting Network Level Permissions

Network Level Permissions provide the access required to change device configurations, run Auto Discovery, access the Scheduler, Approve jobs, and other permissions.

Networks must be assigned to a user or group in this area for access to the devices in the network. Permissions can be assigned per Network.

To ease management, default Network Permissions apply to every Network assigned to the user or group. Default Network Permission can be overridden on a network with the proper permissions.

For each network, the user or group must be assigned permissions based on the tasks to be completed in the network. For example, a user has access to three networks:

- In Network A, the user has the ability to Create, Edit, and View workspaces for the network.
- In Network B, the user cannot complete any of those tasks, but is able to Schedule and Approve jobs.



- In Network C, the user can complete all tasks .

**Note** Permissions set in one network do not overlap to other networks.

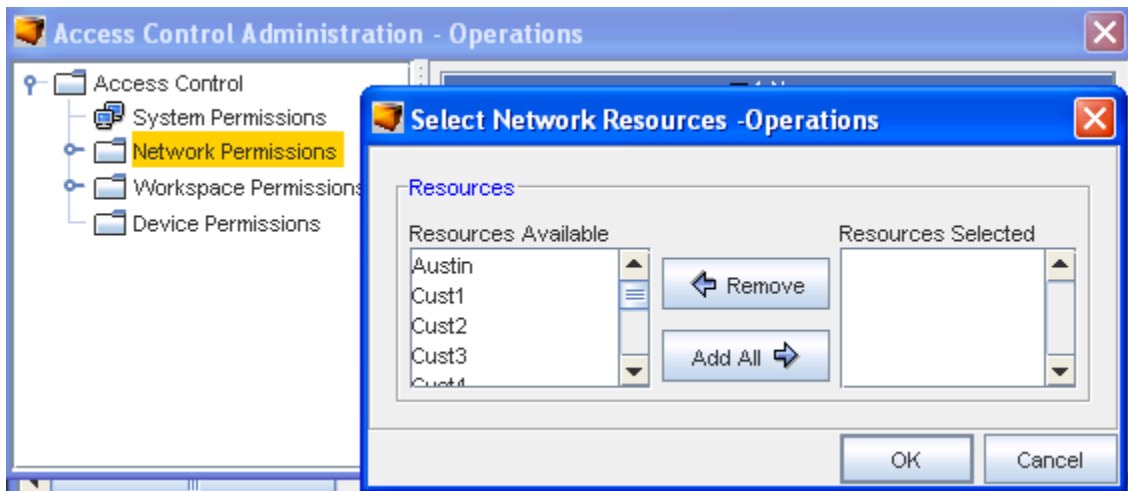
Whether you are setting permissions for a single user or a group of users, the steps are the same. Settings for a single user are set in the **System Users** module, in Set Permissions. Settings for a group are set in the **System Group** module, in Set Permissions.

The Network Permissions function allows you to complete the following actions for the user or group:

- Associate users or groups to manage networks
- [Setting Network Permissions](#)

To associate a user or group to networks,

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand **Global -> User Management**.
- 3 Select **System Users or System Groups** . The right pane contains all available user/groups.
- 4 Selecting a **user/group**, then click **Permissions**. The [Setting User and Group Permissions](#) window opens.
- 5 In the tree menu, select **Network Permissions**. The right pane populates with any networks currently associated with the user/group.



- 6 At the bottom of the window, click **Manage**. The Select Network Resources - [User ID] window opens.

- 7 The Resources Available column is a list of all system networks. Select the **networks** to which the user or group will have permissions.

---

**Note** A sequence of networks can be selected by holding down the Shift-key while clicking networks. Or, multiple, non-sequential networks can be selected by holding the Ctrl key while clicking network.

---

- 8 When you have finished selecting networks, click **Add or Add all** .
- 9 If you are removing permissions to a network, in the Selected Resources column, select the **networks** to which the user will no longer be associated, then click **Remove All**.
- 10 Once you have completed selecting the networks for the user, click **OK**. The Select Network Resources - [User ID] window closes.

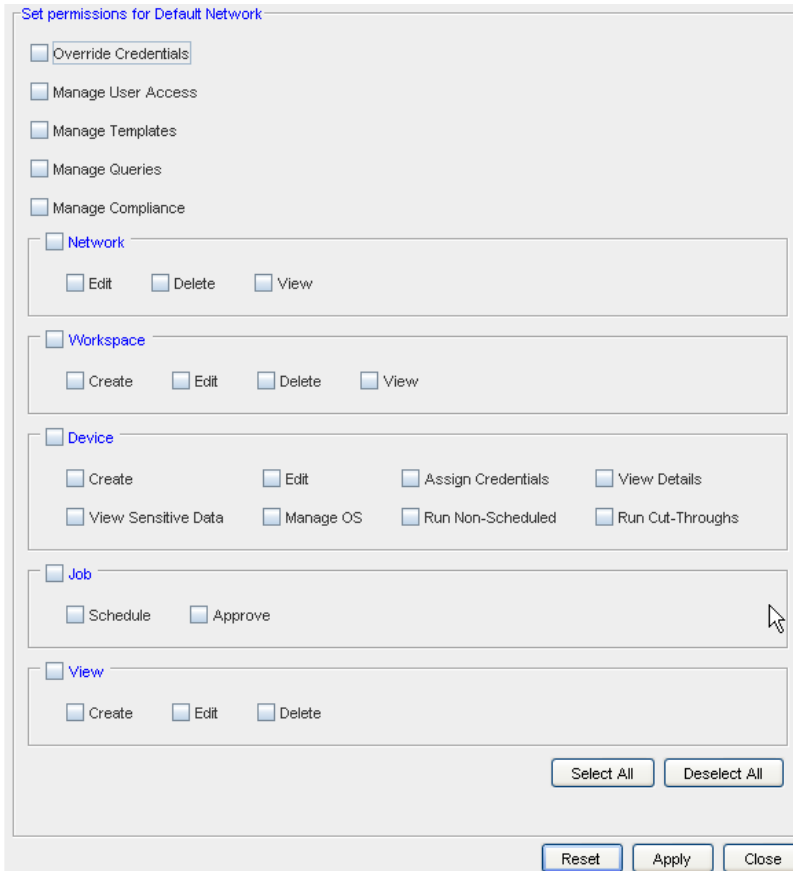
You can now proceed with assigning network permissions for the user or group.

### Setting Network Permissions

The Network Permissions window contains specific permissions for the Network, related Workspaces, Templates Devices, Jobs, and Views. Each area is segmented into specific permissions.

To set network permissions for a user,

- 1 After selecting a user/group, click **Permissions....** The [Setting User and Group Permissions](#) opens.
- 2 In the tree menu, select **Network Permissions**. Available networks display in the right pane. Expand Network Permissions, and select the **network** for which permissions will be set. The right pane populates and will look like the following:



- 3 Select the **areas** for which the user are to have access.
- 4 If the user/group does not require one or more of the included task permissions, click that related check box to de-select the option.
- 5 Repeat **steps 3 and 4** for each area to which the user/group requires access.
- 6 If a user/group requires access to all network options in the Access Control Administration window, at the bottom of the window, click **Select All**.
- 7 When finished, click **Apply**. The window remains open allowing you to set other permissions. Or... If you are not making changes to the other permission level settings, click **Close**.

Section	Description
<b>Override Credentials</b>	Allows you to set the permission for the user to update the existing credentials
<b>Manage user access</b>	Allows access to designate user access
<b>Manage Templates</b>	Allows access to Create or Modify templates that reside in the Automation Library. By default, you can View existing templates.
<b>Manage Queries</b>	Allows access to manage the Queries in the Automation Library
<b>Manage Compliance</b>	Allows access to manage Compliance

Section	Description
<b>Network</b>	Allows the user/group to Edit, Delete or View networks details. By default, if you are provided Edit or Delete permissions, View is automatically set.
<b>Workspace</b>	Allows the user/group to Create, Edit, Delete or View workspaces. By default, if you are provided Create, Edit or Delete permissions, View is automatically set.
<b>Device</b>	<ul style="list-style-type: none"> <li>■ This allows the user/group to <b>Create</b> and <b>Edit</b> devices.</li> <li>■ The <b>View Details</b> check box gives the user/group the ability to see the device properties.</li> <li>■ The <b>View passwords</b> check box allows user/group to see the passwords that must be used to access the device properties.</li> <li>■ <b>Manage OS</b> check box allows the user/group to make changes to the OS of the device.</li> <li>■ <b>Assign Credentials</b> , <b>Run Non-Scheduled</b>, and <b>Run Cut-Throughs</b> allows users to execute these operations if selected.</li> <li>■ Access to Configlet, Interface, and Command editor also can be controlled through <b>Edit</b> devices option.</li> <li>■ Access to Pre-Post Configuration Analysis can also be controlled through <b>Edit</b> devices option.</li> </ul> <p><b>Note</b> By default, when a user/group is given permissions to View Networks and Workspaces, they are able to view their devices.</p>
<b>Job</b>	<ul style="list-style-type: none"> <li>■ Allows the user/group to <b>Approve</b> or <b>Schedule</b> jobs that are created for the device config.</li> <li>■ All non-sysadmin users are having <b>Schedule</b> a job access to edit only their job.</li> <li>■ <b>Manage Users/Groups</b> option present in System Permission can control whether non-sysadmin user has rights to <b>Schedule</b> other users job.</li> <li>■ All non-sysadmin users are having <b>Approve</b> access can approve only their job.</li> <li>■ <b>Manage Users/Groups</b> option present in System Permission can control whether non-sysadmin user has rights to edit/approve other users job.</li> </ul>
<b>View</b>	Allows the user/group to <b>Create</b> , <b>Edit</b> or <b>Delete</b> Views of the network

To change network permissions for a user,

Once network permissions for a user/group have been set, they can be edited as the role of the user/group changes. Permissions are changed by editing the set of permissions currently selected for the user.

- 1 After selecting a user/group, open the **Access Control Administration - [User ID]** window.
- 2 Select **Network Permissions** . The right pane populates with the current permission settings for the user/group.
- 3 Select a **Network**. The right pane populates with permission settings.

**Important** To clear all existing check marks from the check boxes, click **Reset**.

- 4 Make the changes by selecting and de-selecting from the available options in the **Set Permissions for Network** window.
- 5 When finished, click **Apply**. The window remains open allowing you to edit other permissions. If you are not making changes to the other permission level settings, click **Close**. The System Administration window remains.

## Working with Default Network Permissions

You can select to set the default for Network Permissions.

- 1 Select **Default Network** from the Network Permissions expanded link.

The screenshot shows a window titled "Set permissions for Default Network". It contains several sections, each with a header checkbox and a list of sub-permissions:

- Override Credentials
- Manage User Access
- Manage Templates
- Manage Queries
- Manage Compliance
- Network
  - Edit
  - Delete
  - View
- Workspace
  - Create
  - Edit
  - Delete
  - View
- Device
  - Create
  - Edit
  - Assign Credentials
  - View Details
  - View Sensitive Data
  - Manage OS
  - Run Non-Scheduled
  - Run Cut-Throughs
- Job
  - Schedule
  - Approve
- View
  - Create
  - Edit
  - Delete

At the bottom right of the window are two buttons: "Select All" and "Deselect All". At the bottom center are three buttons: "Reset", "Apply", and "Close".

From here, you can set the needed permissions using the check boxes provided.

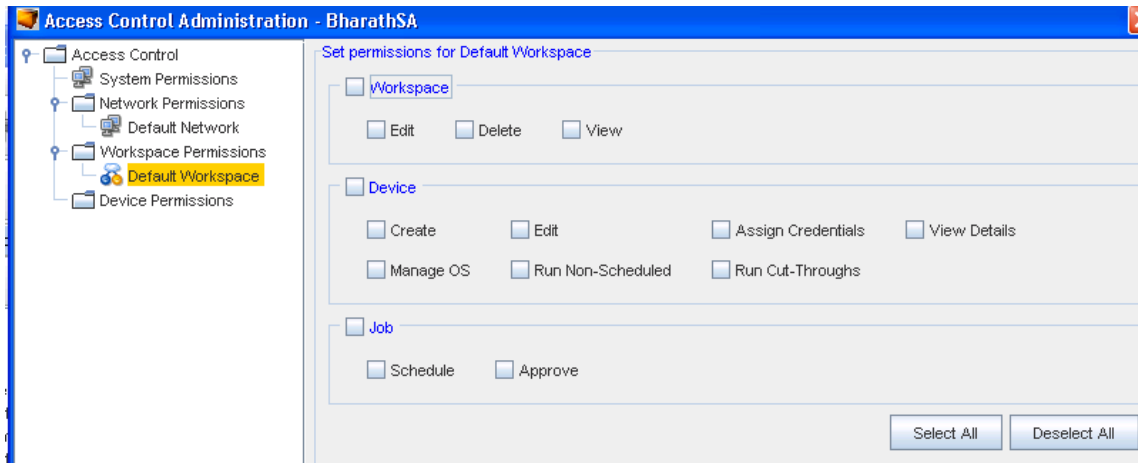
- 2 Select from the separate sections of this window to include the Network, Workspace, Device, Job and View settings.
- 3 You can also **Select All**, to select all the options on this window. You can also chose **Deselect All** if there are existing selections within the check boxes, then proceed to make your own selections.
- 4 Click **Apply** after you have made your selections.

Permissions are now set for this Default Network.

## Working with Default Workspace Permissions

You can select to set the default for Default Workspace Permissions.

- 1 Select **Default Workspace** from the Workspace Permissions expanded link.



From here, you can set the needed permissions using the check boxes provided.

- 2 Select from the separate sections of this window to include the Workspace, Device and Job settings.
- 3 You can also **Select All**, to select all the options on this window. You can also chose **Deselect All** if there are existing selections within the Check boxes, then proceed with making your own selections.
- 4 Click **Apply** after you have made your selections.

Permissions are now set for this Default Workspace.

### Setting Device Level Permissions

Device level permissions determine the actions that the user or group is able to complete on a device and its details. Although the user or group (as a whole) has permissions set up to the group, the permissions per device are set up individually. The device setup is a two-part task:

- Selecting the devices the user or group is to have access to
- Setting the permissions explicitly for the device

---

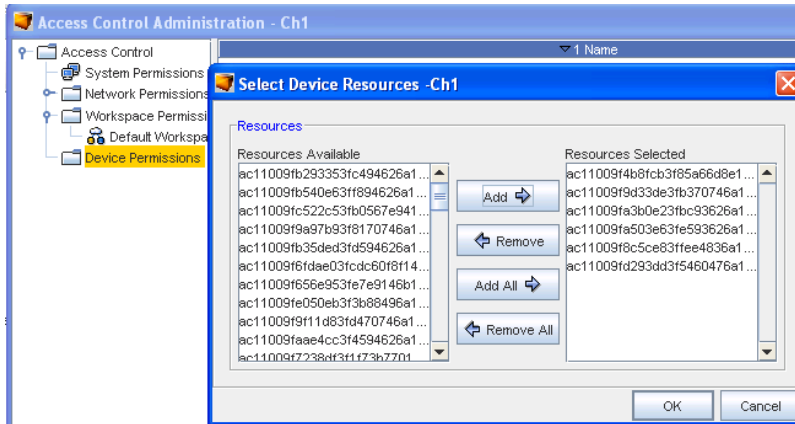
**Note** Prior to setting device level permissions, keep in mind that device level permissions **override** all other permission levels.

---

First step: To assign devices for user or group access,

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand **Global -> User Management**.
- 3 Select **System Groups** . The right pane contains all available groups.
- 4 Select a group, then click **Permissions**. The [Setting User and Group Permissions](#) window opens.

- 5 In the tree menu, select **Device Permissions**. The right pane populates only if the user or group has been given permissions to other devices.
- 6 Click **Manage**. The Select Device Resource window opens.



- 7 In the Resource Available column, select the **Devices** to which the user or group are to have permissions.
- 8 Click **Add**. The selected devices are moved to the Resources Selected column.

---

**Note** A sequence of devices can be selected by holding down the Shift key while selecting devices. Or... Multiple, non-sequential devices can be selected by holding the Ctrl key while selecting devices.

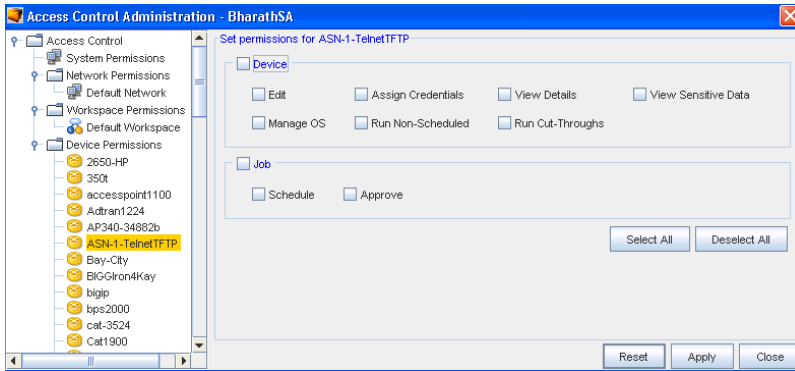
---

- 9 Repeat **steps 7 and 8** for each device to which access is required.
- 10 If a user requires access to all devices , without making a selection, click **Add All**.
- 11 When finished, click **OK**. The Select Device Resource window closes.

The right pane reflects the devices that were selected in the Select Device Resource window. You can now select the explicit device permissions for the group.

Second step: Set device level permissions,

- 1 In the navigation pane, expand the **Device Permissions** folder. The devices listed are the same devices that were just selected in the Select Device Resource window.
- 2 Select a **Device** by double-clicking on the device name. The right pane populates with the Set permissions for [device name] options.



These options represent the permissions that the user or group have for this specific device. There are two sections in the area:

- All permissions in both areas
  - One or more permissions from each area
  - Permissions from only one area
- 3 To select all options in an area, click the **check box** next to Device or Job.  
Or, to provide select options in each section, click the check box next to the required options.
  - 4 To provide the user or group with all device permissions, click **Select All**. All options are checked. (This action can be reversed by clicking the De-select All button.)
  - 5 When you have selected the appropriated options, click **Apply** at the bottom of the window. The Access Control Administration - [User ID or Group Name] window closes.
  - 6 Repeat the above steps for each device.

**Device** The Device section provides permissions for access to the config to Edit, View device passwords, View details, and Update the OS of the device. It also allows permissions for Assign Credentials, work with Run Non-scheduled tasks, and complete Run Cut-Throughs.

**Job** The Job section provides the user or group with permission to Schedule and/or Approve jobs for the device.

### The user or group can be assigned to:

**Important** If you have assigned a device to a user or group to manage, the user or group is unable to complete any tasks specific to the device until you have set the explicit permissions.

## Working with Authentication Servers

### Authentication Servers Overview

Authentication servers provide a means to allow users one-stop access to the Network Configuration Manager application without the need to build another password server in your environment.



Network Configuration Manager supports four authentication server options:

- Native Registry
- TACACS+
- RADIUS
- LDAP

For validation to occur, prior to being setup in Network Configuration Manager, each user must be created on the **Authentication Server**. The instructions provided here are on the authentication server configuration details.

When a user is created, the method of authentication is selected. Based on this selection, when the user attempts to log into Network Configuration Manager, the user's User ID, and if needed, Password, are validated via the selected server.

---

**Important** For information on how to set up users on your authentication server, you must refer to the authentication server's user guide.

---

There are two sets of configurable server details, Primary and Secondary. For validation to occur using the selected authentication server, at least one set of Server and Port details must be entered.

If you are using a single server address, the Secondary set should be left empty. In addition, for additional user security a lock out feature is available. To limit the number of attempts a user can try to access Network Configuration Manager, you can use this feature. For more information, see [User Lock Out Security](#)

### Setting up the Native Registry

Native Registry is a combination of a User name and Password that is entered for a user when they are created in Network Configuration Manager. The setup of the *Native Registry* actually occurs at the time the user is created. For more information, see [Creating Users](#).

The User name/Password details are stored locally in Network Configuration Manager. Actual changes to the User name/Password are completed by editing the user profile .

---

**Note** The details located within the Authentication Server module are for security access settings only.

---

The number of failures can be designated so the user is locked out of the system after entering the wrong user ID/password combination by a set number of attempts. When a user is locked out of Network Configuration Manager an authorized user (such as the System Administrator) must go into the Edit user feature, and unlock the users access.

To setup Native Registry validation,

- 1 From the menu bar, access **Tools** -> **System Administration**. The System Administration window opens.

- 2 Select **Global**.
- 3 Expand **User Management** , then select **Authentication Servers**.
- 4 Select **Native Registry** . The right pane refreshes with the Native Registry access security details.



- 5 Check the **Lock Users** check box. The Number of consecutive fails allowed text box activates.
- 6 Enter the **number of attempts** the user can try before being locked out of Network Configuration Manager.
- 7 When finished, click **Apply**. All entries are accepted.
- 8 Click **Close** to close this window.

### Setting up the TACACS+ Server

Authentication servers provide a means to allow users one-stop access to the Network Configuration Manager application without the need to build another password server in your environment.

A TACACS+ Server is an external server that is used to **validate users** when they log into Network Configuration Manager. Prior to any user being able to log into Network Configuration Manager, they must be listed on the server.

If you are using a TACACS+ Server, Network Configuration Manager allows you to map to two servers, a Primary and Secondary server, to validate user information. In the following example, the window has two areas:

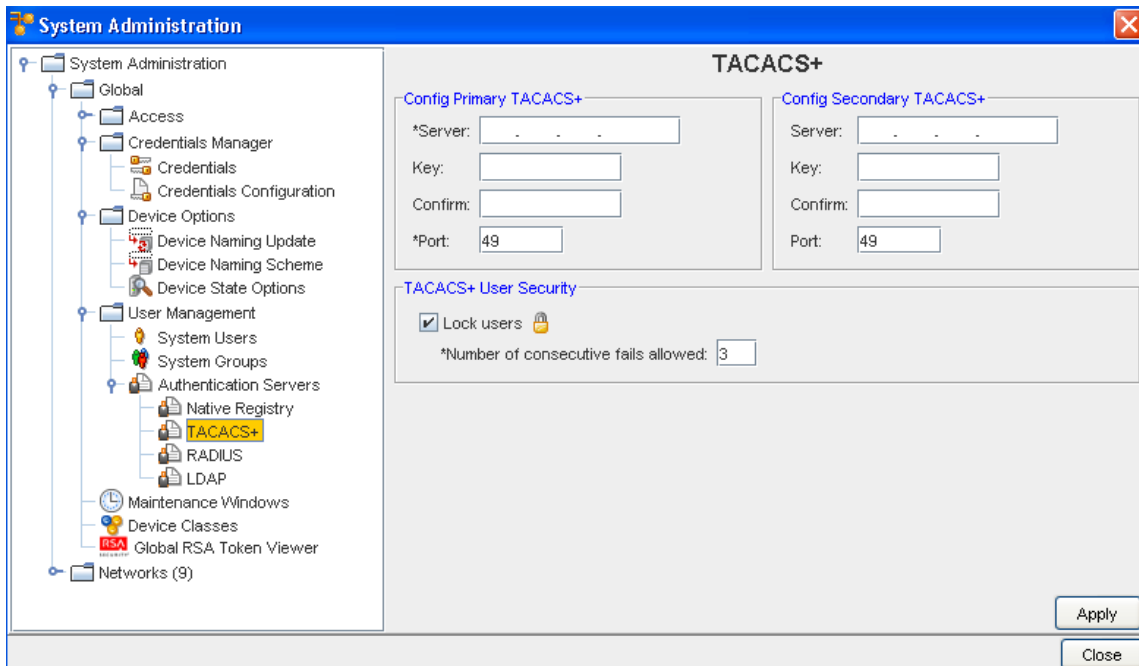
- 1 TACACS+ Server configuration area for Primary and Secondary server setup
- 2 TACACS+ User Security

If your company has only one server, enter it into the Config Primary TACACS+ configuration section. To properly configure a server, the following information is required:

- Server Address
- Port Number

To setup the TACACS+ Server configuration,

- 1 From the menu bar, access **Tool -> System Administration**.
- 2 Select **Global**.
- 3 Expand **User Management** , then select **Authentication Servers**.
- 4 Select **TACACS+** . The right pane refreshes with the TACACS+ Server configuration details.



- 5 In the Server text field, enter the **Server Address** .
- 6 If there is a key for the server, enter the **Key**.
- 7 Next, enter the Key again for confirmation into the **Confirm** field.
- 8 Enter the **Port**.
- 9 Repeat steps 5 through 8 for the **Secondary** server.
- 10 To set the User Lock Out, see [User Lock Out Security](#) and follow the instructions. If you are not setting TACACS+ User Security, click the **Apply** button at the bottom of the window. All entries are accepted.
- 11 To exit the window, click **Close**.

### User Lock Out Security

Each authentication server mechanism has a user security lock out feature. This feature allows you to set whether users can be locked out of the system (after entering an incorrect User ID and Password combination) by a **set number** of attempts.

Each User Security section looks similar to the following.



Once checked, this option applies to all users validated by the server.

To set the user lock out settings,

- 1 Check the **Lock Users** check box. The Number of Consecutive fails allowed text box activates.
- 2 Enter the **number of attempts** the user has before being locked out of Network Configuration Manager.
- 3 When finished, click **Apply**. All entries are accepted.

---

**Important** When a user is locked out of the Network Configuration Manager, an authorized user must open the [Locking and Unlocking Users](#) feature.

---

### Setting Up RADIUS Authentication Modules

RADIUS is an authentication and accounting server for terminal servers that speak to the RADIUS protocol. Network Configuration Manager works with RADIUS to validate user access. All user/password details are stored on your RADIUS server. Network Configuration Manager is then mapped to the server to retrieve this information for validation.

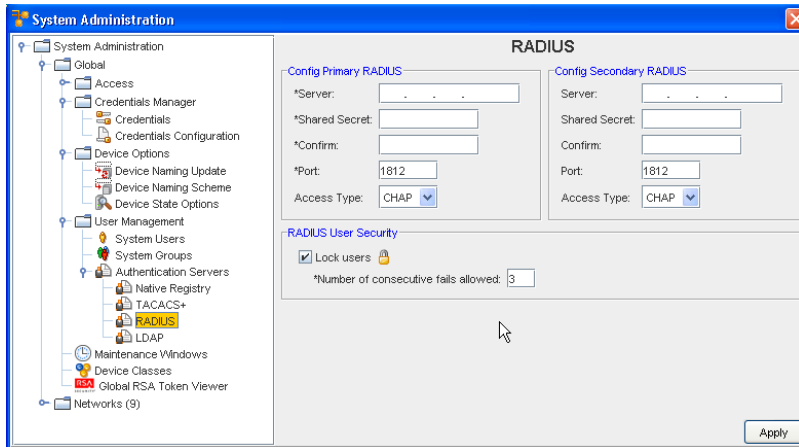
---

**Note** Network Configuration Manager now implements RADIUS requests using Password Authentication Protocol (PAP), or Challenge Handshake Authentication Protocol (CHAP) as the **Access Types**.

---

To setup Network Configuration Manager access using RADIUS,

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand **Global -> User Management**.
- 3 Expand **Authentication Servers**, then select **RADIUS**. The right pane displays similar to the following.



The RADIUS window allows you to designate two server addresses. At least one (the Primary) set of server details must be filled in.

- 4 Enter the **Server** address.
- 5 Enter the **Shared Secret** .
- 6 Enter the Shared Secret once again in the **Confirm** field.

---

**Note** The Shared Secret is a text string which is a "secret" (in the raddb/clients file) shared by both the NAS and the server. It is used to authenticate and to encrypt/decrypt packets.

---

- 7 Enter a **Port**.
- 8 Select an **Access Type** from the drop-down arrow listing. You can either select Password Authentication Protocol (PAP), or Challenge Handshake Authentication Protocol (CHAP) as the Access Type.
- 9 If you are not setting [Locking and Unlocking Users](#), click **Apply**. All entries are accepted.
- 10 To exit the window, click **Close**.

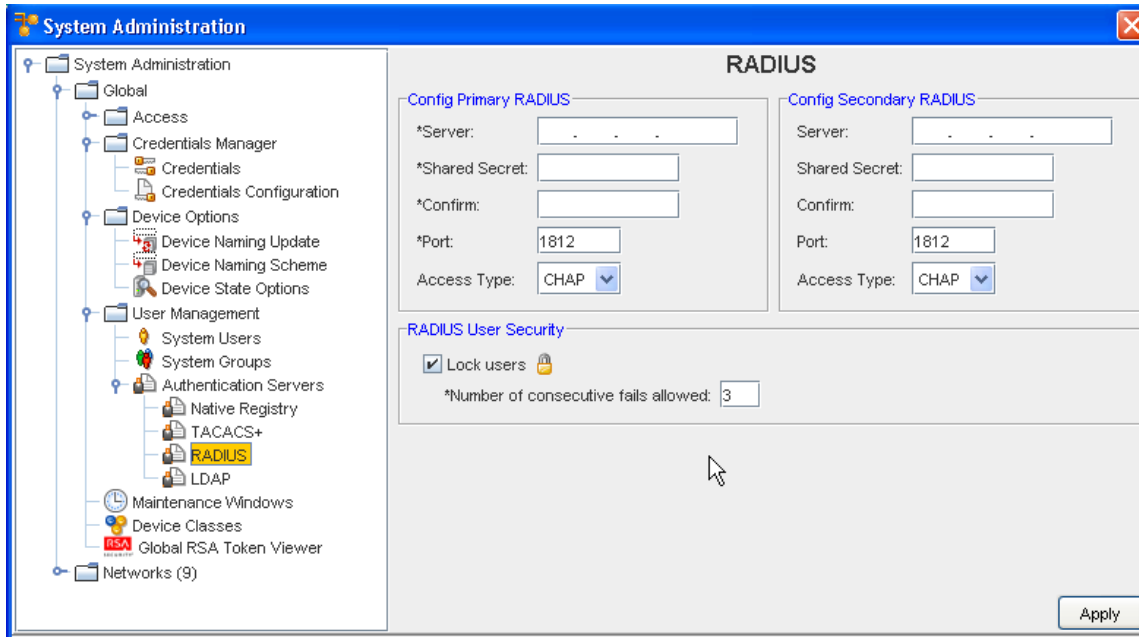
### Editing RADIUS Authentication Modules

The RADIUS settings that can be edited are:

- The Primary server settings
- The Secondary server settings
- [User Lock Out Security](#)

To edit the primary and secondary RADIUS,

- 1 From the menu bar, access **Tools** -> **System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand **Global** -> **User Management**.
- 3 Expand **Authentication Servers** , then select **RADIUS**. The right pane will look similar to the following.



All fields in the RADIUS config window can be edited. Only the Config Primary RADIUS section is required to be filled for the authentication to work properly.

- 4 Make any changes to the existing data. If you are setting up a secondary configuration, enter the **Server address, Shared Secret, Confirm, and Port**.
- 5 Make a selection from the **Access Type** drop-down arrow.
- 6 If you are not setting the RADIUS User Security, click **Apply**. All entries are accepted. If you are activating the RADIUS user security, click within the **Lock users** check box, enter the **number** of fails allowed, then click **Apply**.
- 7 To exit the window, click **Close**.

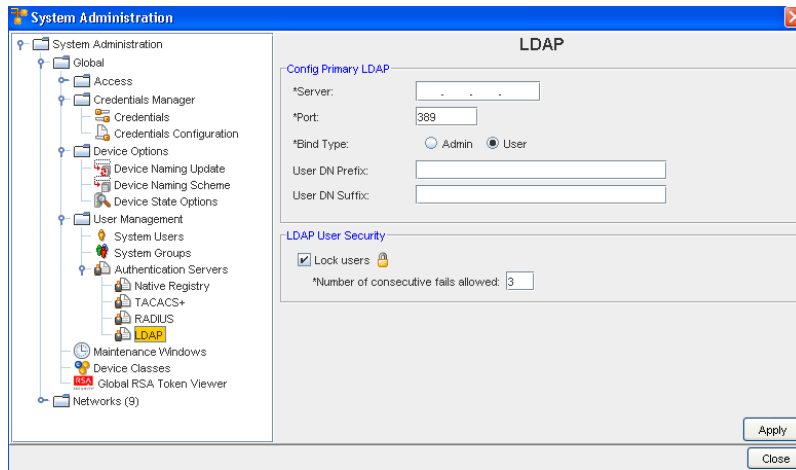
### Setting Up LDAP Authentication Modules

LDAP is a set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is more simple. LDAP supports TCP/IP, which is necessary for any type of Internet access.

All user/password details are stored on your LDAP server. Network Configuration Manager is then mapped to the server to retrieve this information for validation.

To setup Network Configuration Manager access using LDAP,

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand **Global -> User Management**.
- 3 Expand **Authentication Servers**, then select **LDAP**. The right pane appears similar to the following.

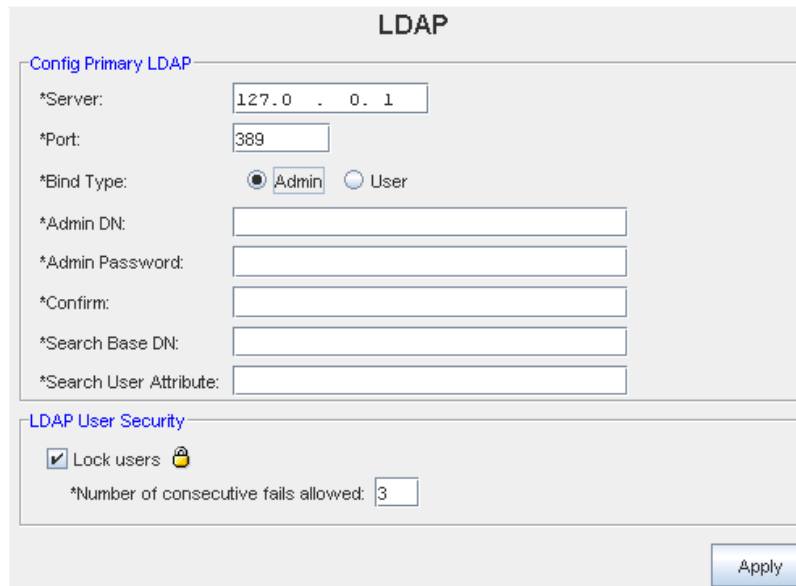


- Enter the **Server** address.
- Enter a **Port**.
- Select a **Bind Type**. You can select Admin (if you have Admin Privileges) or you can select User.
- If **User** is selected, complete the remainder of this window by entering the needed information. Go to **Step 7** to continue.
- If **Admin** is selected, more information is needed, and an additional section for this information is displayed within the LDAP window (shown in the following graphic).

---

**Note** You must have **Administration Privileges** to use the Admin LDAP Bind Type feature.

---



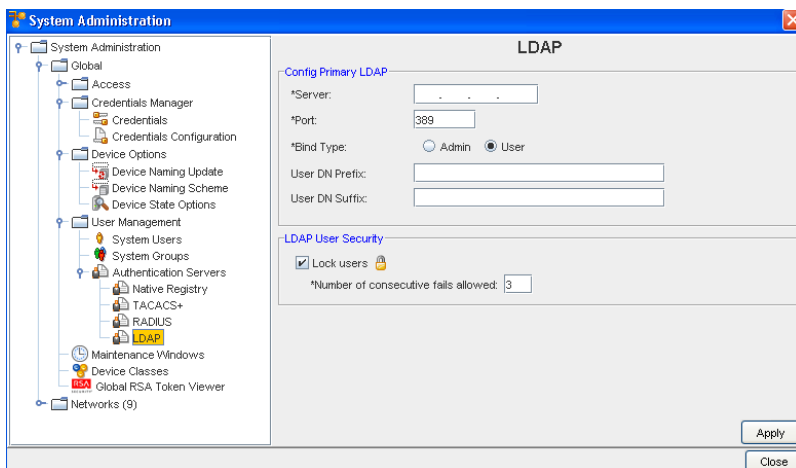
- Enter the **Admin DN (Distinguished Name)**
- Enter the **Admin Password** , and then enter and **confirm the Admin Password** .
- Enter the **Search Base DN (Distinguished Name)**

- Enter the **Search User Attribute**
- Go to **Step 8** to continue.
- Enter a **User DN Prefix** , then enter the **User DN Suffix**.
- The DN Prefix is a prefix added to the username to form the user Distinguished Name (DN).
- The User DN Suffix is a suffix added to the username to form the User Distinguished Name (UDN).
- This is useful if you prompt a user for a username and you do not want the user to have to enter the fully distinguished name. Using this property and prefix, the user DN is formed as String userDN = prefix + username + suffix.
- If you are not setting **User Lock Out Security**, click **Apply**. All entries are accepted.
- If you are setting the lock users information, enter the **number** of consecutive fails allowed then click **Apply**.
- To exit the window, click **Close**.

### Editing LDAP Authentication Modules

To edit the LDAP authentication module,

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand **Global -> User Management**.
- 3 Expand **Authentication Servers** , then select **LDAP**. The right pane appears similar to the following.



The LDAP window allows you to designate one server address. The Server, Port, User DN Prefix, and User DN Suffix fields are required.

- Admin DN (Distinguished Name)
- **Admin Password** , and then enter and **confirm** the **Admin Password**
- Search **Base DN (Distinguished Name)**



- Search **User Attribute**
- Continue with **Step 8**.

### LDAP

**Config Primary LDAP**

\*Server:

\*Port:

\*Bind Type:  Admin  User

\*Admin DN:

\*Admin Password:

\*Confirm:

\*Search Base DN:

\*Search User Attribute:

**LDAP User Security**

Lock users

\*Number of consecutive fails allowed:

- 4 Make changes to the **User DN Prefix** and the **User DN Suffix** data.
- 5 Make any needed changes to the LDAP User Security section.
- 6 Click **Apply**. All entries are accepted.
- 7 To exit the window, click **Close**.
  - Make any changes to the existing information in the **Server** address.
  - Make any changes needed to the **Port**.
  - If **User** was selected as the Bind Type, continue on with **Step 7**.
  - If **Admin** was previously selected for the Bind Type, the window appears as follows. Make any changes to this additional information:

## Global - Maintenance Windows

### Global - Adding a Maintenance Window

Maintenance windows allow organizations to set certain time windows in which specific jobs or tasks can be run. When Maintenance windows are set for a job or task type, they can only be overridden by their Network or System Administrators.

A Maintenance window can be added at the System (Global) Level, or at the Network Level.

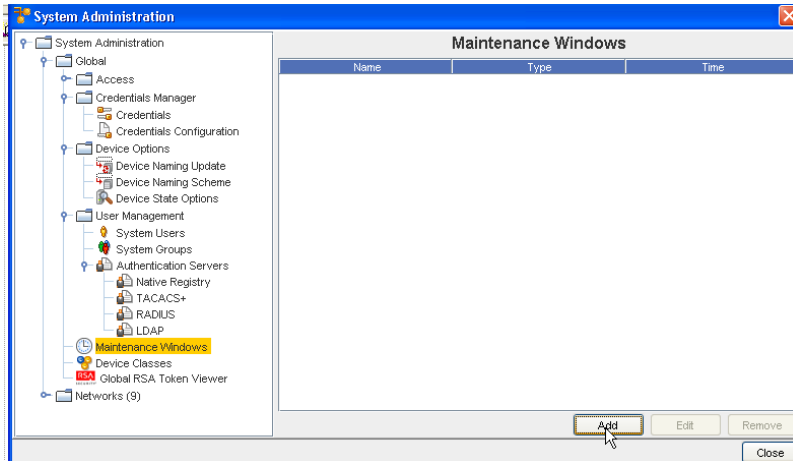
---

**Note** You can now define a window for each activity that can be completed against a device, thus ensuring that only those activities can only be completed during that designated window.

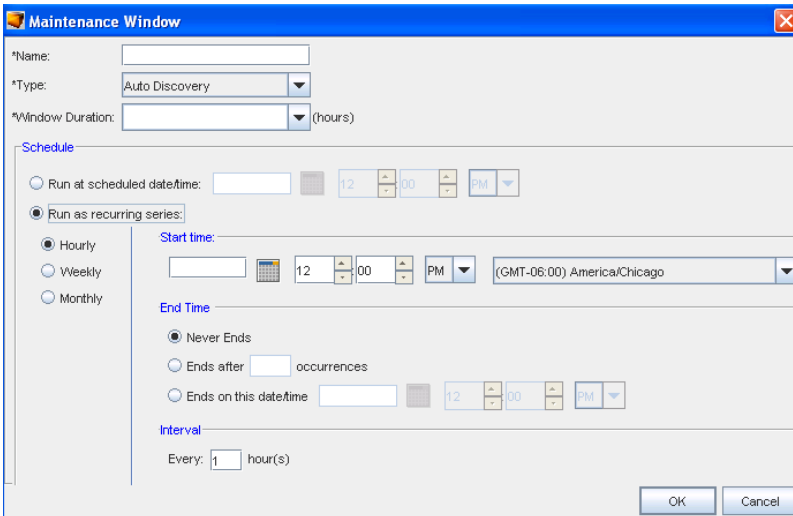
---

To add a scheduled maintenance window,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Global -> Maintenance Windows**.
- 3 Click **Add**.



- 4 Enter a **unique name**.
- 5 Select a **Type** from the drop-down listing.



- 6 From the next drop down ( **Window Duration**), select the time allocated updates.

---

**Note** Time can be allocated in 30 minute increments. As small as a .50 timespan, to an 11.5 hour timespan.

---

- 7 Next, at the Schedule portion of the window:
- 8 Set the **exact date** and time for the run to occur.

- 9 Select a **recurring schedule** using the **Run As Recurring series** option. When the recurring schedule is selected, the new **time zone** drop-down options are available. Make your selection from the drop-down options. The time zone you select must be the **client's time zone** . The new time zone field is propagated with the client time zone automatically when creating a new Maintenance Window or recurring scheduled job.
- 10 Click **OK**. The maintenance window closes, and the information is now stored within the Maintenance Windows.

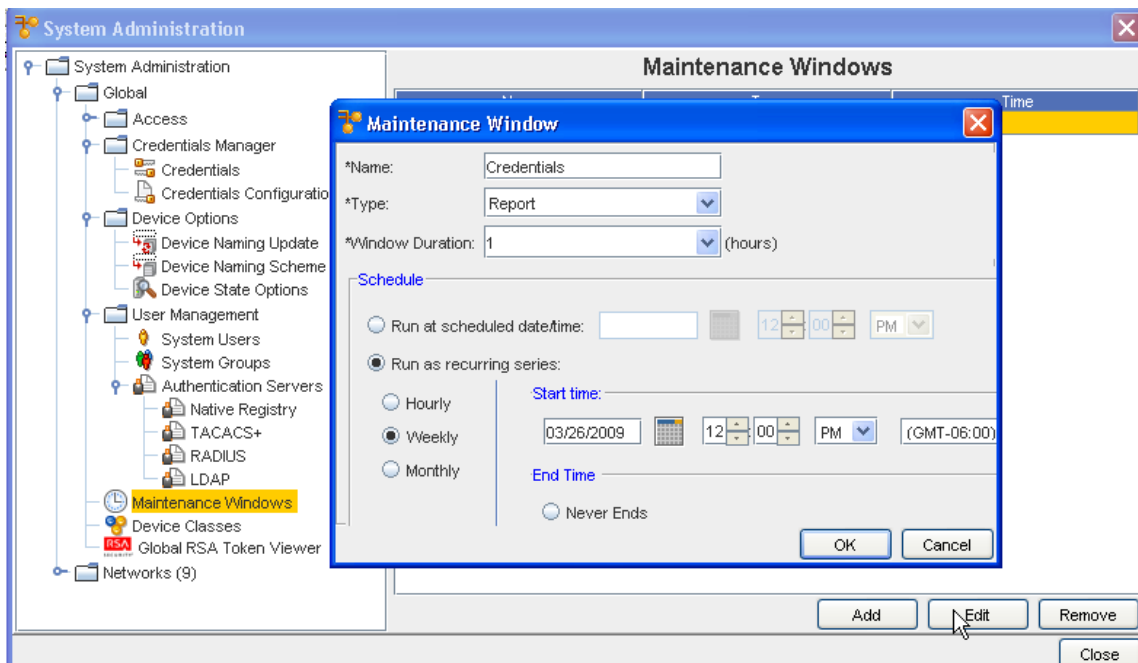
## Global - Editing a Maintenance Window

A Maintenance window can be added at the System (Global) Level, or at the Network Level.

**Note** You can now define a window for each activity that can be completed against a device, thus ensuring that only those activities can only be completed during that designated window.

To edit a scheduled maintenance window,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Global -> Maintenance Windows**.
- 3 Click **Edit**.



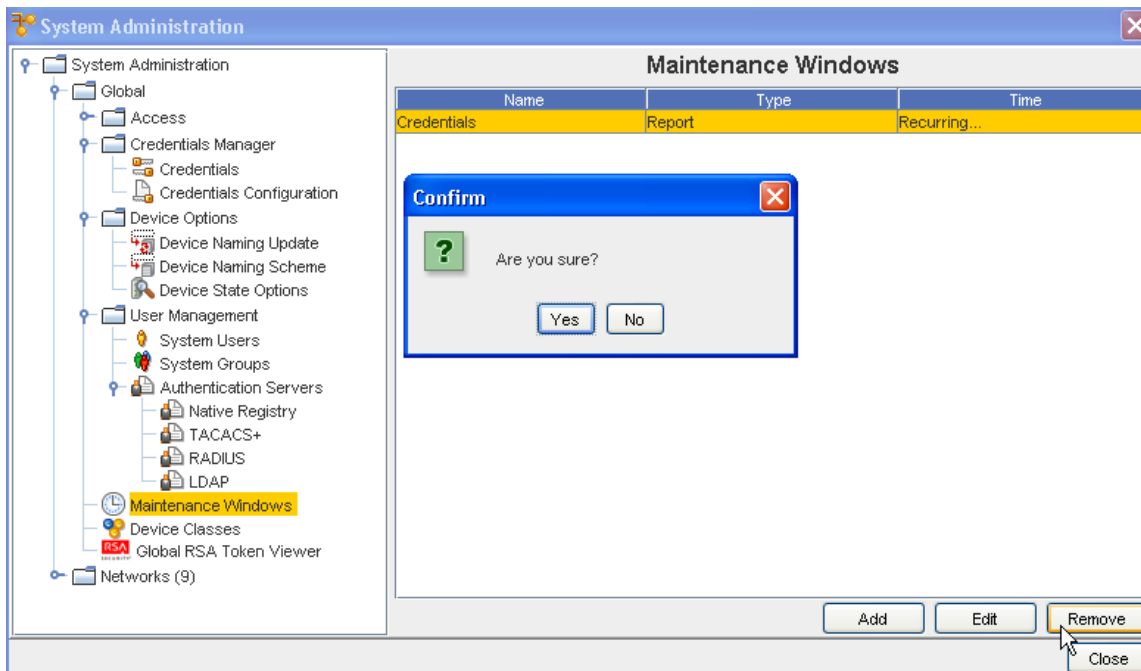
- 4 At the Maintenance Window, make any necessary edits.
- 5 Click **OK**. The maintenance window closes, and the information is now stored within the Maintenance Windows.

## Networks- Removing a Maintenance Window

When a schedule is no longer needed for your networks it can be deleted from the list. By removing a maintenance schedule, any network with the associated schedule takes on the settings of the System (Global) maintenance schedule (if one has been previously set).

To remove a scheduled maintenance window,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Global -> Maintenance Windows**.
- 3 Select the schedule (maintenance window), then click **Remove**. The confirmation window displays.



- 4 If okay, click **Yes**. Or, to cancel this action, click **No**.

The Maintenance Window updates with the selected item removed from the list.

## Global - Device Classes

### Device Class Management Overview

Device Classes permit you to set the significant device classes in your network, as well as setting preferred device communication mechanisms. Communication and mechanisms can be ordered, added, or removed for each device class.

You can also decide whether to use SNMP to manage devices, provide device information (MIB), or prevent SNMP from being used in your network.

Device class management is used to streamline the communication access to all devices, regardless of network assignment.

Device classes are logical organizations of devices according to their type. Examples of device classes can include:

- Cisco IOS Routers
- Cisco IOS Switches
- Cisco IOS Layer 3 Switches
- Juniper
- Nortel ARN
- Nortel BayStack BPS
- Nortel Passport 8600

A device class has a one-to-one correspondence with the device driver that manages devices within that class. To provide device services to a device, the device **must** be assigned to a device class that will provide the correct functionality for that device.

Typically, the device class is assigned to a device when it is discovered or added to the system. The system automatically follows a series of rules for assigning the proper driver to a device. Normally, no user intervention is needed in this process.

However, occasionally you may want to move a device from one device class to another device class. For example, if you have an advanced or custom version of a device driver that provides additional capabilities for your environment, and you want to use this alternate device class for managing a particular device. In this case, you can **override the automatically assigned device class** on a device-by-device basis.

### Configuring Device Class Attributes

Device classes also have attributes associated with the class. Changing the attribute on a class changes that attribute for all devices within that class. The following are attributes that can be changed on a Device class-by-Device class basis.

#### Auto-Managed

Device classes can be marked for auto-managed. When a Device class is marked for auto-manage, whenever auto discovery finds a new device and assigns it to a auto-managed device class, it automatically marks the device as managed and pull the configuration(s) from the device.

The auto-managed state for a Device class can be set from the **Managed Supported Device Classes** window in the System Administration tool. See [Managing the Supported Devices Class List](#) for more information.

#### Specify Protocols

Device classes can be marked to enable or disable various protocols from functioning. For example, you can mark a Device class such that it enables SSH and SNMP as communications protocols, but disable Telnet and TFTP. The state of enabled and disabled protocols can be changed on the **Manage Devices** window in the System Administration section. See [Specifying Device Class Protocol](#) for more information.

## Device Class Management Best Practices

- Unless there is a good reason for doing so, do not change the default device class assignment for a particular device. This could cause your device communications to stop functioning properly.
- Use the auto manage devices feature of device classes to automatically pull configurations, and store them in the repository when new devices come online and are made available.
- Auto Manage is also a useful feature when you are adding a large, new network to your system, as it prevents you from having to manually manage every new device that is discovered, one-by-one.
- If you have specific requirements that prohibit you from using specific protocols (such as, if you are disallowed from using TFTP within your network), use the Specify Protocols option to turn off all protocols that violate that requirement.
- If you are running your Device Server and devices over a non-secure network, consider disabling all non-encrypted protocols to preserve the security of your communications stream. This would include turning off SNMP, Telnet, TFTP, and FTP as communications protocols, and relying instead on protocols such as SSH and SCP.

## Specifying Device Class Protocol

To change default communication preferences for a device class, select Specify Protocol. Here you can re-order the preferences of the protocols used, or add and remove protocols from the enabled list. Note that disabling SNMP for all use could result in limited information being gathered for certain device classes.

Your networks may not be configured to handle certain protocols for supported devices. If you choose, you can enable or disable communications to your network devices using specific communication protocol methods.

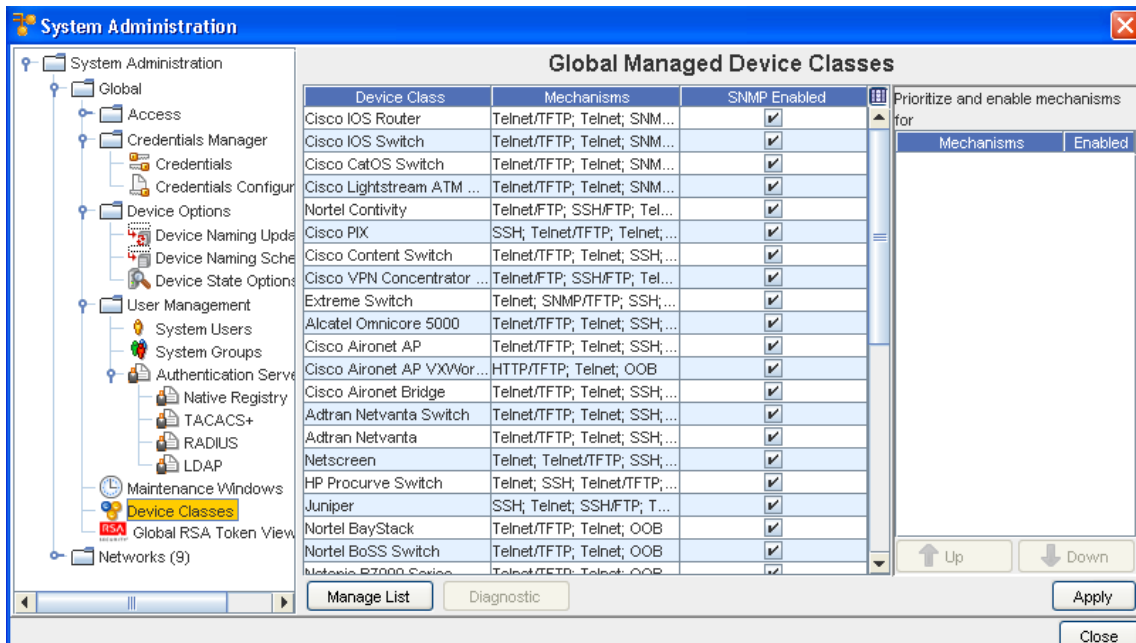
To adjust the device class protocols,

- 1 From the menu bar, select **Tools**.
- 2 From the menu options, select **System Administration**. The System Administration window opens.
- 3 On the tree menu, expand the **Global** -> **Access** folders.

---

**Important** By default, the SNMP check box is enabled.

---



- 4 To make changes to any Device Class, select the **row**, then **un-check** the check box in the SNMP Enabled column.
- 5 Now, select one or more new protocols in the Protocols section. Notice that you can use the Up and Down arrows to reposition the priority of the Protocols.
- 6 Click **Apply**.
- 7 Read the messages presented, and click **Yes** if appropriate.

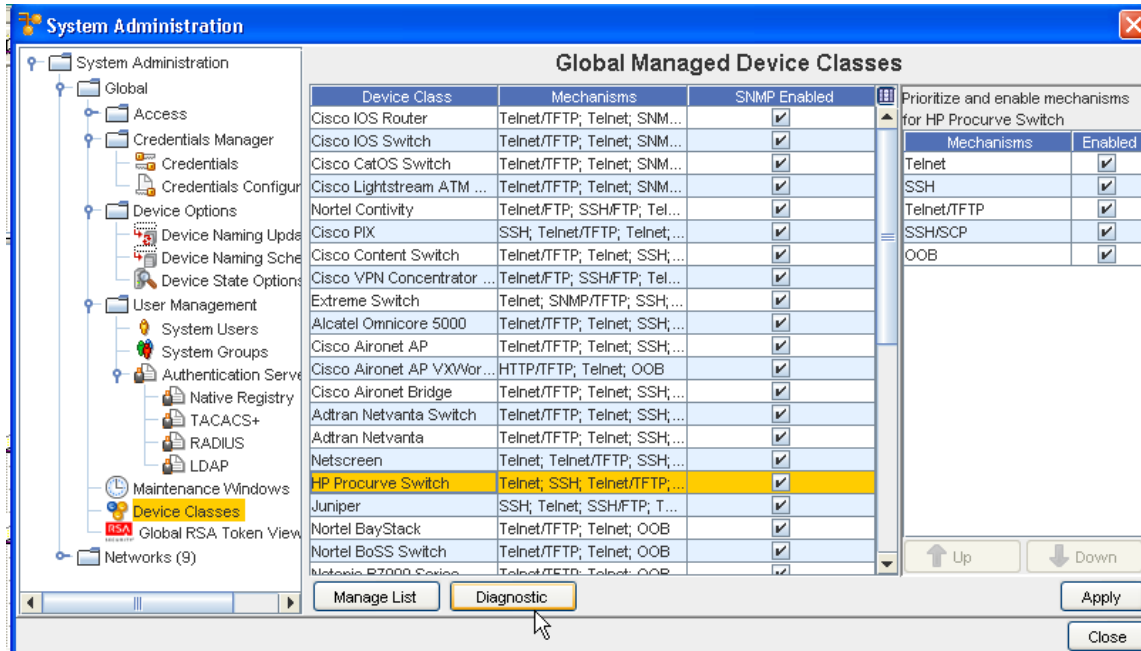
To change the priority of the listed protocols,

- 1 Select a **protocol** from the list. Based on its location in the list, the Up and Down arrows activate.
- 2 Using the **Up/Down arrows**, move the selected protocol to the **new location**. The top-most protocol is used as the default.

## Working with Diagnostics

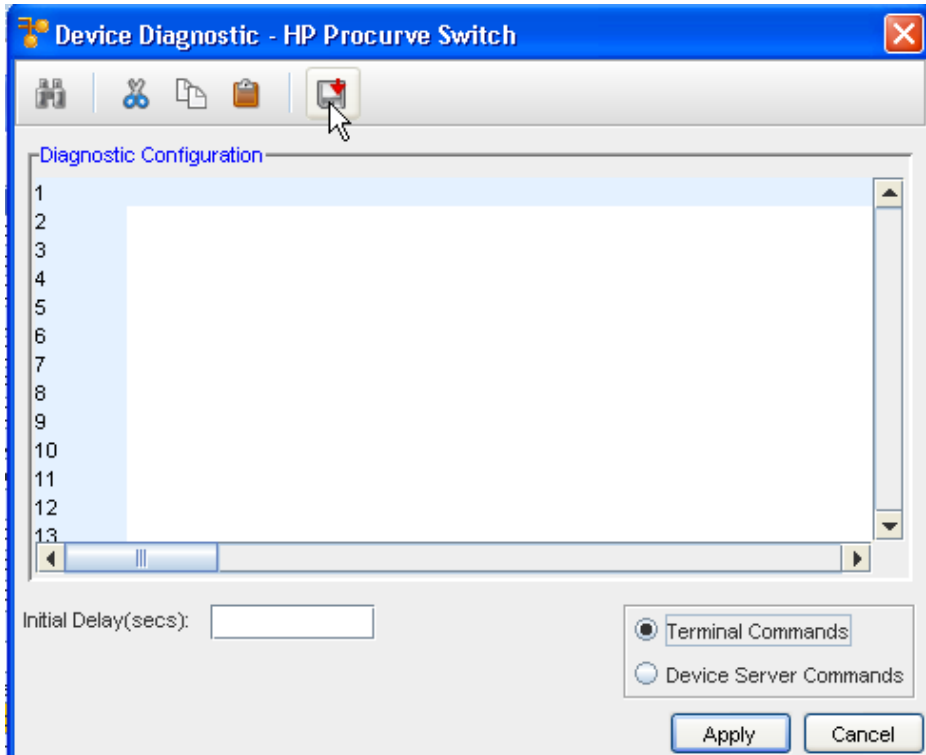
The diagnostic window allows you to define by device class, as set of system commands that are executed and stored with each new configuration revision. Since diagnostics are run and stored for each revision, their information can be compared to determine service deltas after a new deployment.

- 1 With the **Global Managed Devices** window opened, select a **Device**, and then work with the device's diagnostics.



- 2 Click the **Diagnostic** button.
- 3 Note that you can use **Search** tool to find any configuration or string that may be included. You can use the **Copy**, **Paste**, and **Cut** tools to copy any existing configuration, and then paste to another section, or highlight the contents of the config and then cut (or remove) the contents.
- 4 At the Device Diagnostics window, you can insert **Saved Commands** , and make the designation of either a Terminal Command or a Device Server Command. You can also insert a new command.
- 5 Continue through the windows to select the appropriate saved command. When adding Command, designate whether the commands are **Terminal or Device Server** by selecting the appropriate radio button.





- 6 Enter the time (in seconds) if you want an **Initial Delay**.
- 7 Click **Apply** when you have completed working with the device diagnostics.

## Managing the Supported Devices Class List

Network Configuration Manager supports a wide spectrum of Device Classes, but your network needs may not require all the Devices Classes that are supported. With this in mind, Network Configuration Manager allows you to designate which Device Classes are relevant to your network needs.

Following is a partial listing of Device Classes currently supported by Network Configuration Manager:

- Adtran Netvanta
- Adtran Netvanta Switch
- Alcatel Omnicore 5000
- Aruba Wireless Switch
- Checkpoint Firewall
- Cisco Aironet AP
- Cisco Aironet AP VXWorks
- Cisco Aironet Bridge

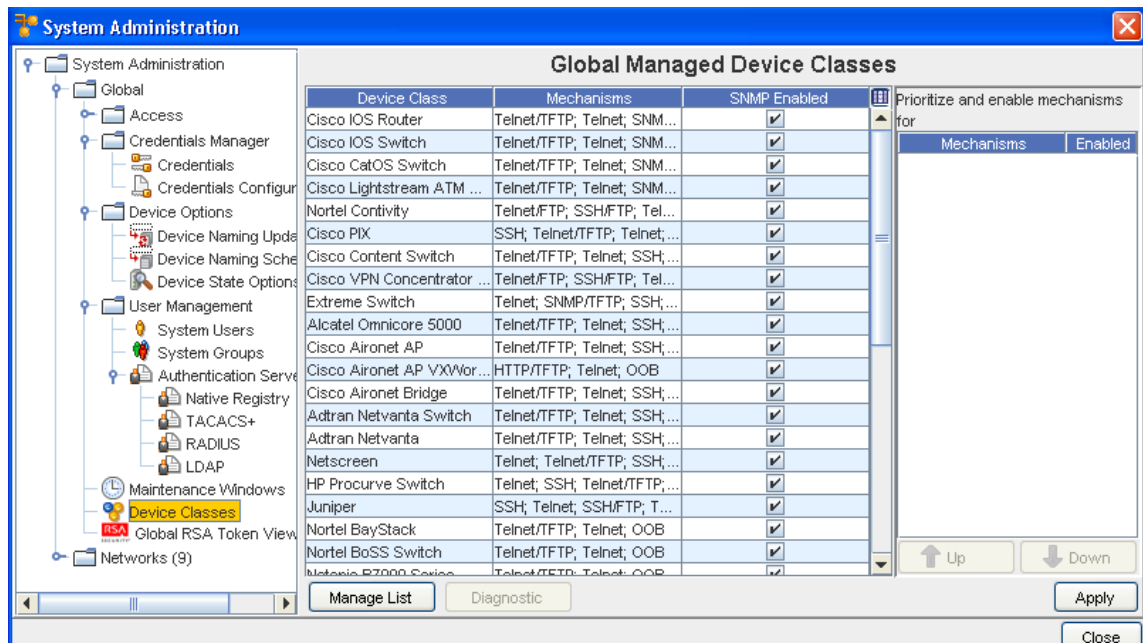
- Cisco CatOS Switch
- Cisco Content Switch
- Cisco IOS Layer 3 Switch
- Cisco IOS Router
- Cisco IOS Switch
- Cisco Lightstream
- Cisco Pix Firewall
- Cisco VPN 3000
- Extreme
- F5 Load Balancer
- F5 Load Balancer Rev 3
- Foundry
- HP ProCurve
- Juniper
- Lucent Access Point
- Marconi ASX
- Netopia R7000 Series
- Netscreen
- Nokia Appliance
- Nortel Alteon
- Nortel ARN
- Nortel Baystack 350/450
- Nortel Baystack BPS
- Nortel Contivity
- Nortel Passport 1648
- Nortel Passport 8600
- Packeteer
- Siemens
- Riverstone Router
- Tasman Router

To select device classes for Network Configuration Manager management,

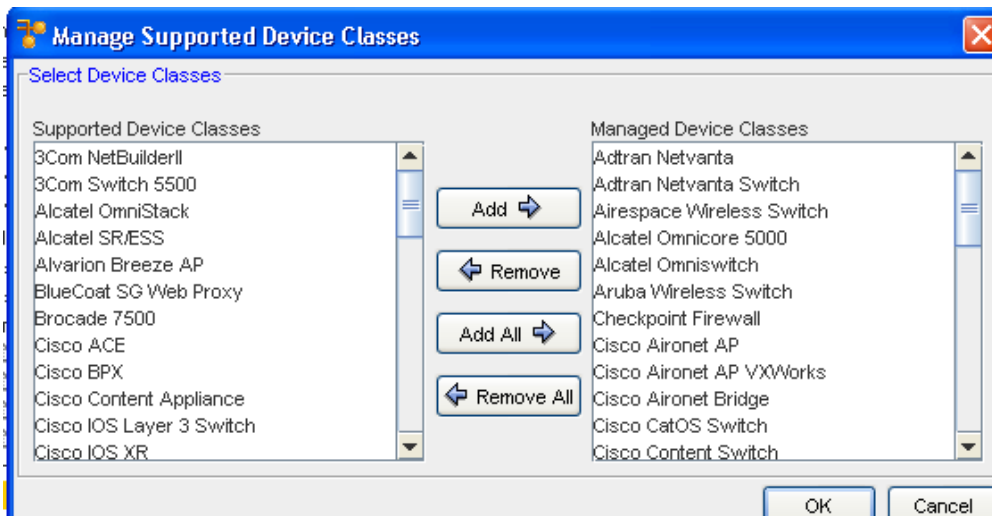
- 1 In the menu bar, select **Tools**.

- 2 From the menu options, select **System Administration**. The System Administration window opens.
- 3 On the tree menu, expand the **Global -> Access** folders.
- 4 Select **Device Classes**. The Global Managed Device Classes configuration window populates the right pane.

The Managed Device Classes window contains the list of supported device classes, and their primary protocol. As each device class is selected, the Enabled and Disabled protocols are shown to the right. For more information on enabling/disabling device protocols, see [Specifying Device Class Protocol](#).



- 5 To see which Device Classes are supported for your networks, click **Manage List**. The Manage Supported Device Classes window opens.



- The Supported Device Classes column is a list of all the support device classes. This list should reflect the same Devices Classes seen in the Global Managed Device Classes window.
  - The Managed Device Classes column is a list of all device classes that have been selected to be supported for your networks by Network Configuration Manager.
- 6 To assign a Device Class to be managed by Network Configuration Manager, in the Supported Device Classes column select the **Device Class**.

---

**Important** A sequence of Device Classes can be selected by holding down the Shift key while clicking selections. Or, multiple, non-sequential Device Classes can be selected by holding the Ctrl key while clicking selections.

---

- 7 When you have finished selecting Device Classes, click **Add** or **Add All** .
- 8 If you are removing Device Classes from being managed, in the Managed Device Class column, select the **Device Classes**, then click **Remove** or **Remove All**.
- 9 Once you have determined which Device Classes are being managed, click **OK**. The Manage Supported Device Classes window closes.

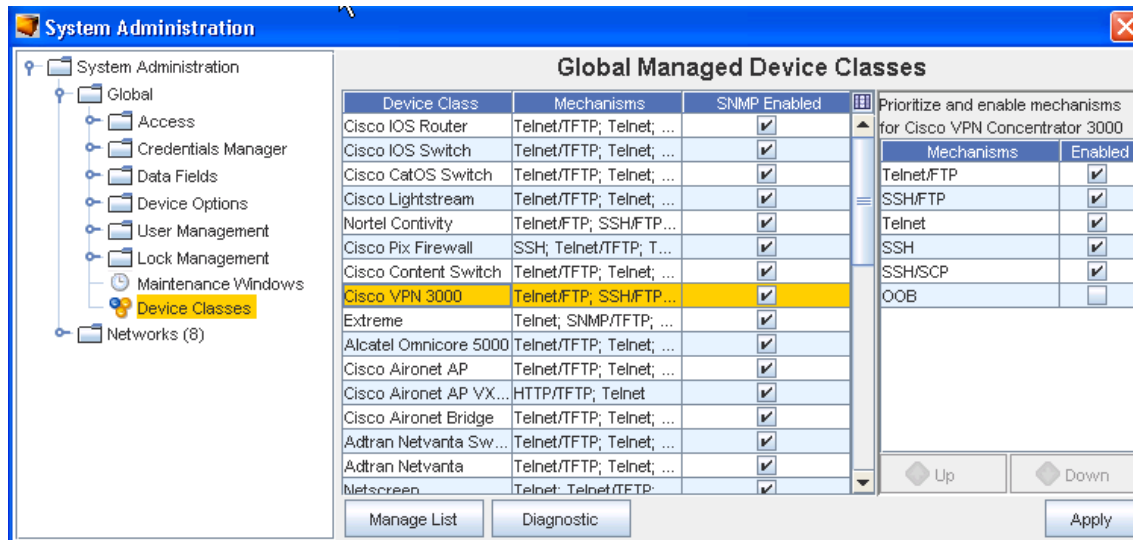
---

**Note** To import devices using the Command Line Interface function, see [Command Using the Command Line Interface](#) for more information.

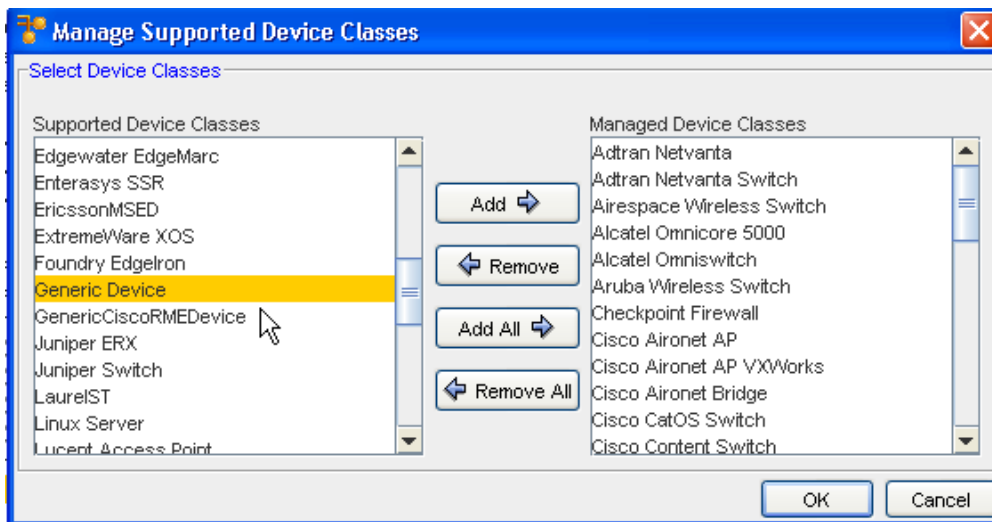
---

## Generic Device Selection - Device Classes

The Generic Device Package discovers devices. You can selectively enable this feature using the Device Classes.



- 1 To use the Generic Device package, from **System Administration -> Global** , go to **Device Classes** .
- 2 Next, select **Manage List**.



- 3 Select **Generic Device** as the only Managed Device Class, then click **Ok**.

**Important!! Use this feature with caution as it discovers a range of items.**

If you encounter a comment resembling the following, then the device did not discover with your list of drivers, and the Generic Device is not configured . The discovery action was not able to discover this specific type of device, and is going to the last driver by default, which is the Generic Driver.

```

Selected job comments:
==== Found driver via SNMPV1 (#100:Generic Device)
+++ Found SNMP V2 Community String (Cust5 N)
==== Active Snmp Version set to SNMP V2
!!! This device package (Generic Device) does not support SSH or Telnet.
---- The device package 100:(Generic Device) is not configured, the device will not be discovered
=====

```

You must now complete a Single-Device Auto Discovery, with this **enabled** until you become familiar with the discovery process used in Network Configuration Manager. If discovery cannot find data, a blank table column may display throughout the application. At a minimum, if the device is reachable, it puts the IP as the Device Name.

To enable a Cut-Through to the device, follow these steps:

- 1 Ensure you use the **Device Classes** (located in the System Administration tool) to manage the Device Classes.
- 2 Now, **discover the device** as you normally would.
- 3 View the results, and make any **Credential updates** .

## Using the Diagnostic Tool

### Diagnostic Tool Overview

With this tool, you can track **Configuration Revisions** and any changes made to Devices.

This diagnostic tool offers the following features:

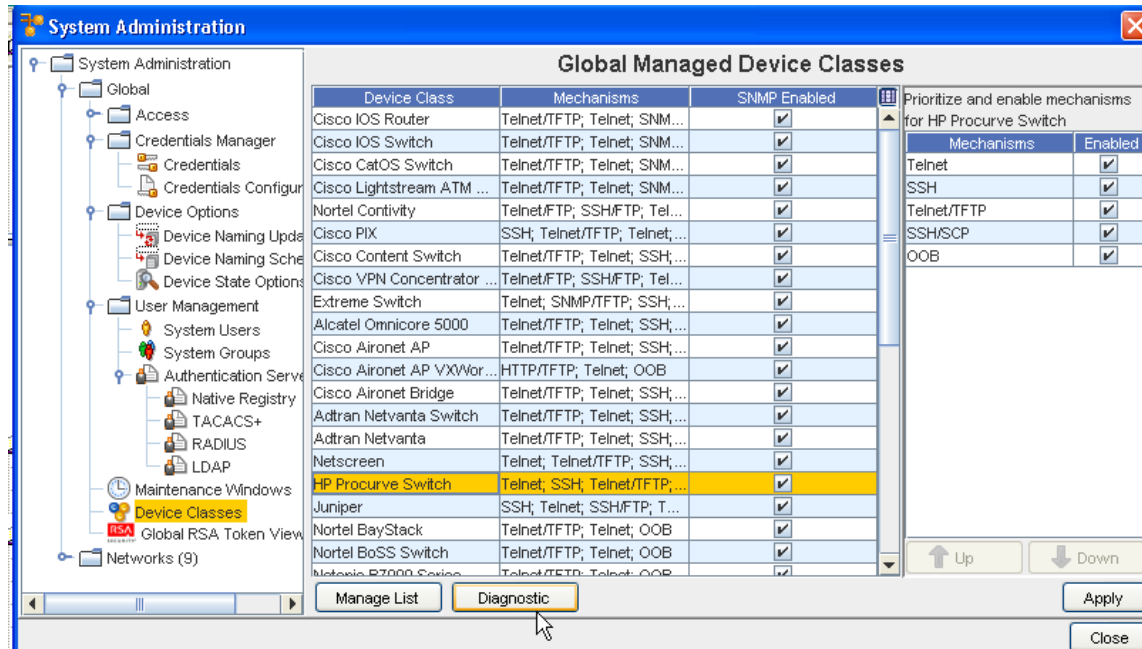
- You can create a set of **commands** to be run as diagnostics for each Device Class, or for each device. Commands can be either Terminal Commands or Device Server Commands .
- You select the specific **Device Class**, and the Devices within that class then have the Diagnostic commands run against them. Whenever a Configuration Revision is created, the Diagnostic Command automatically runs against the Device.
- You can designate how soon after a configuration change has been made to the Devices (within the Device Class) to **automatically run the diagnostic** commands.
- The Diagnostic results are revisioned and **stored**.
- You can **view** the diagnostic data in the History tab (selected from Device Properties).
- You can **compare the results** of two diagnostic revisions.

The diagnostic data is always associated (linked) with a revision. If there are no configuration revisions , there will not be any diagnostic revision data .

To Set up Diagnostics for a Device Class follow these steps,

**Note** You can also set up diagnostics for a specific device using the Set-up Diagnostic quick command.

- 1 To begin working with the Diagnostic tool, go to **Tools** on the Network Configuration Manager menu bar.
- 2 Next, select **System Administration** from the list of tools displayed. From the System Administration window, select **Device Classes**, then click the **Diagnostic** button.



## Setting Up (Creating) Diagnostic Commands

Diagnostic Commands are created to detect changes in Configurations to the Devices.

**Note** Before setting up diagnostics, make note of the following information.

If diagnostics are setup as Device Server Commands (for example, dasllet) the dasllet code must take care of handling more prompts and entering a code snippet (shown below, such as enable Mode etc., in the case of enable mode commands).

This is the same behavior as when you are setting up commands using the **Quick Commands** function (for example, it is the responsibility of the DASL code writer to ensure correctness).

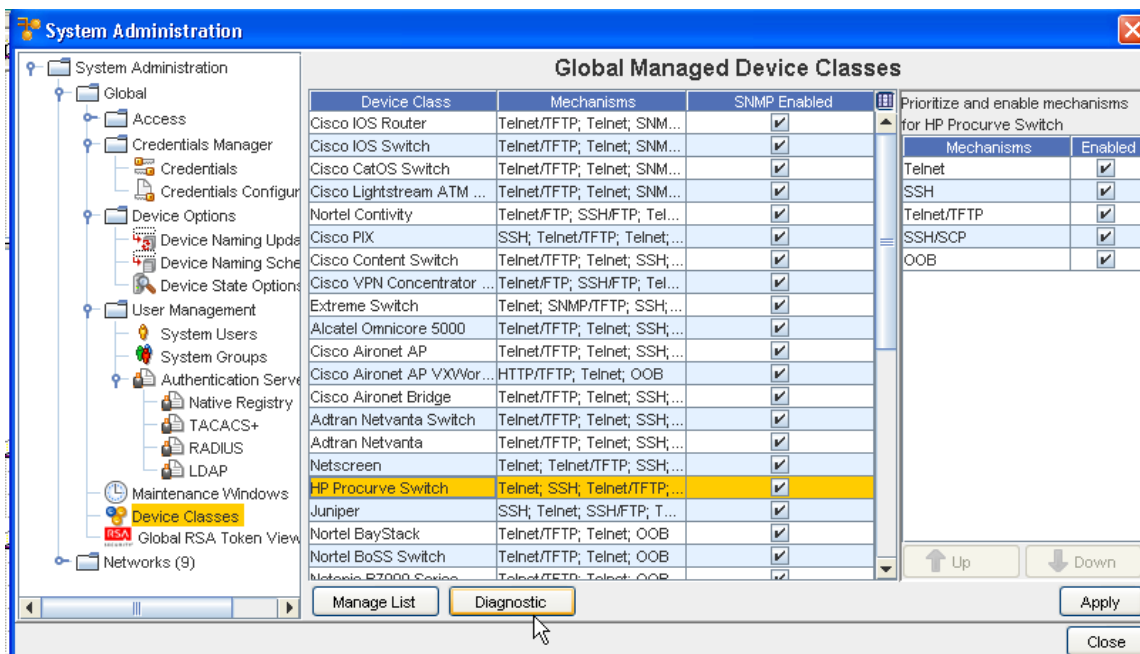
Code snippet:


```
var session=getSession(MECHANISM);
ciscoEnableMode(session); # or send privpass equivalent code
startCapture(session);
send(session,"term length 0\n");#take careof more prompts
```

```
expect(session,2,stdEnablePromptState);
send(session,"show run\n");
expect(session,20,stdEnablePromptState);
RESULT=endCapture(session);
```

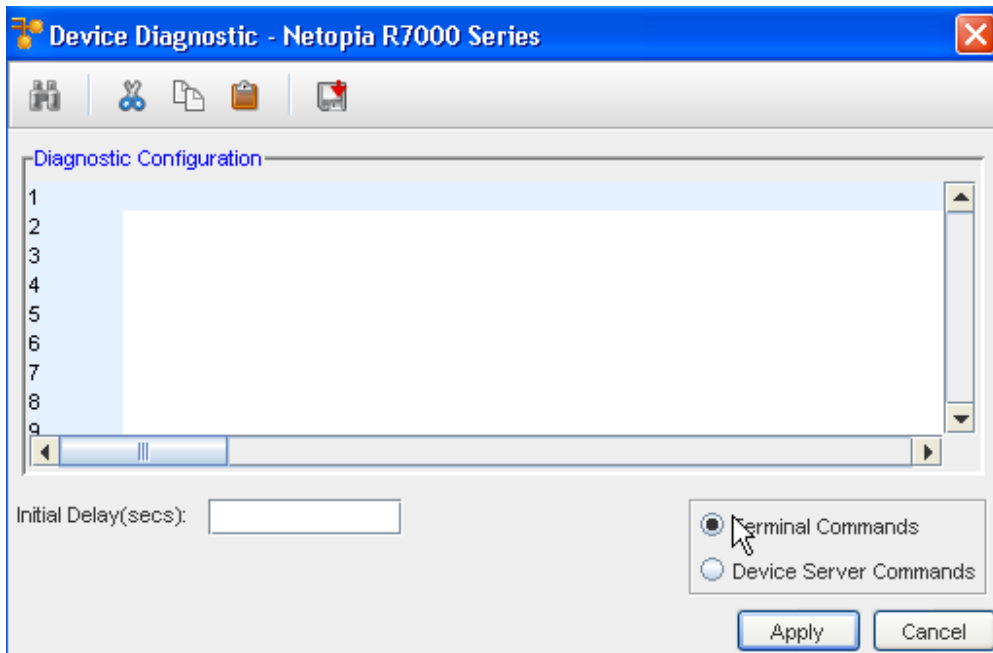
To begin setting up diagnostic commands,

- 1 First, go to **Tools** on the menu bar, then select **System Administration** from the list of tools displayed.
- 2 **Select Global**, then select **Device Classes** . From the list of Global Managed Device Classes, make your selection by highlighting the **name** of the device class.



- 3 Once you have selected the Device Class, click the **Diagnostics** button.
- 4 At the DeviceDiagnostic window, determine if you want the command to be a Terminal Command or a Device Server Command , and click the appropriate radio button. The following graphic shows the **Terminal Commands** radio button is selected.
- 5 After selecting the command type, enter the **command** into the Diagnostic Configuration section using the command icon  to locate a command.



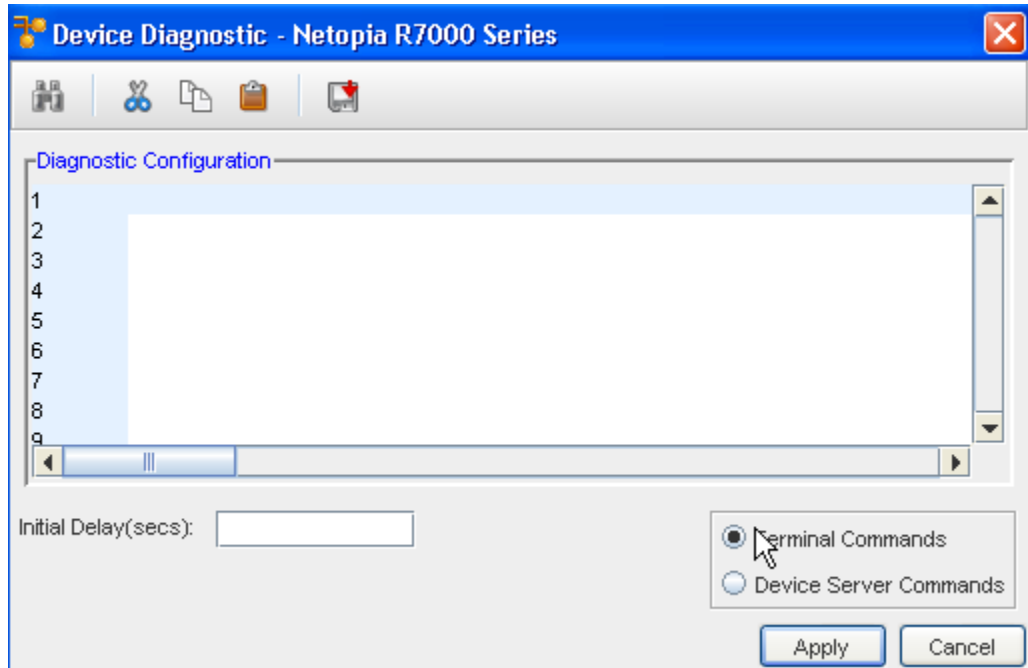


- 6 **Note** At the **Initial Delay (secs):** field, enter the **time** (in seconds). This time designates the number of seconds you want to delay for the diagnostic to run, once a configuration change has been detected. The larger the initial delay number, the longer it takes for the actual revision to be applied.
- 7 Click **Apply** when you have completed entering the delay time.
- 8 Now, back at the Global Managed Device Classes window, click **Apply**.
- 9 At the confirmation message, click **Yes** to apply the diagnostic commands.






## Cutting, Pasting, Copying and Inserting Diagnostic Commands

From the Device Diagnostic window, you can complete the following tasks:

- Search Command text
- Enter Commands
- Cut Command text
- Paste Command text
- Copy Command text
- Insert Existing Commands



Use the menu bar at the top of the **Diagnostic Configuration** section to work with the commands.

Task	Results
 <p><b>Search</b> - Use the Search icon to search for text within the commands displayed.</p>	<p>The Find window opens, allowing you to enter criteria. You can select to <b>Find</b>, <b>Replace</b>, or <b>Replace All</b> within the diagnostic commands displayed.</p>
 <p><b>Cut</b> - Use the Cut icon to highlight, then cut any existing diagnostic commands you do not want to display or apply.</p>	<p>The text you highlighted is now removed from within the diagnostic commands text.</p>
 <p><b>Copy</b> - First highlight the text you want to copy, then use the Copy icon to copy command text to another section of the Diagnostic Configuration section.</p>	<p>The text you highlighted and copied is now copied, and waiting to be pasted within the commands text.</p>
 <p><b>Paste</b> - Use the Paste icon to paste the copied command text.</p>	<p>The text you previously copied is now pasted into the commands text.</p>
 <p><b>Insert Command</b> - Use the Command icon to open the <b>Select Item</b> window, and chose an existing (saved) command, then insert the saved command.</p>	<p>The existing saved command you selected from the <b>Select Item</b> window is now inserted into the Diagnostic Configuration command text section. See <a href="#">Creating a Command</a> for more information on the Command icon.</p>

## Global - RSA Token Viewer

### RSA Tokens Overview

RSA tokens provide a means to allow users **two-factor authentication** access to the Network Configuration Manager application. RSA SecurID<sup>®</sup> two-factor authentication is based on something you know (a password or PIN), and something you have (an authenticator), providing a much more reliable level of user authentication than reusable passwords.

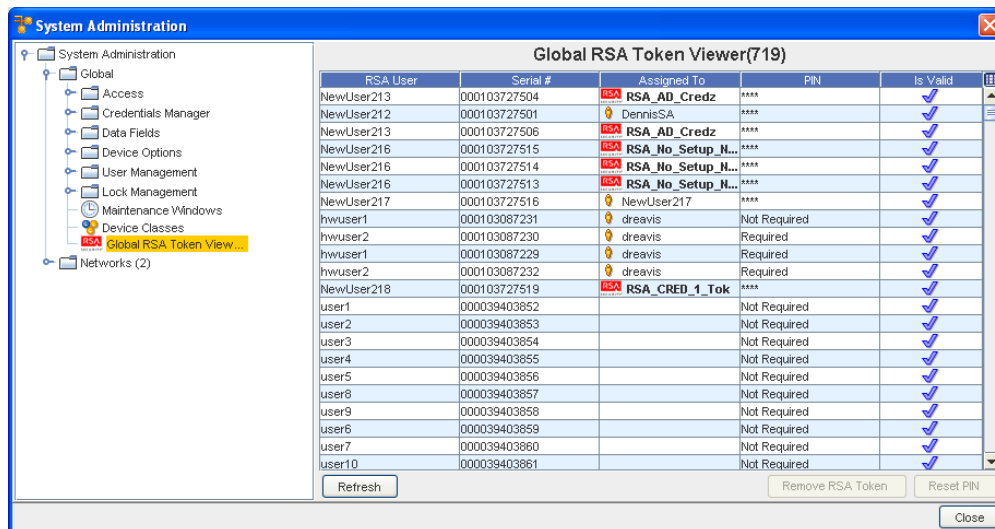
In addition, for additional user security, a lock out feature is available. To limit the number of attempts a user can try to access Network Configuration Manager, you can use this feature. For more information, see [User Lock Out Security](#)

### Global - Global RSA Token Viewer

The Global RSA Tokens Viewer window allows organizations to view associated devices for an RSA Token, remove an RSA Token, and reset the PIN associated with an RSA token.

#### Viewing the Global RSA Tokens Viewer Window

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Global -> Global RSA Tokens Viewer**.



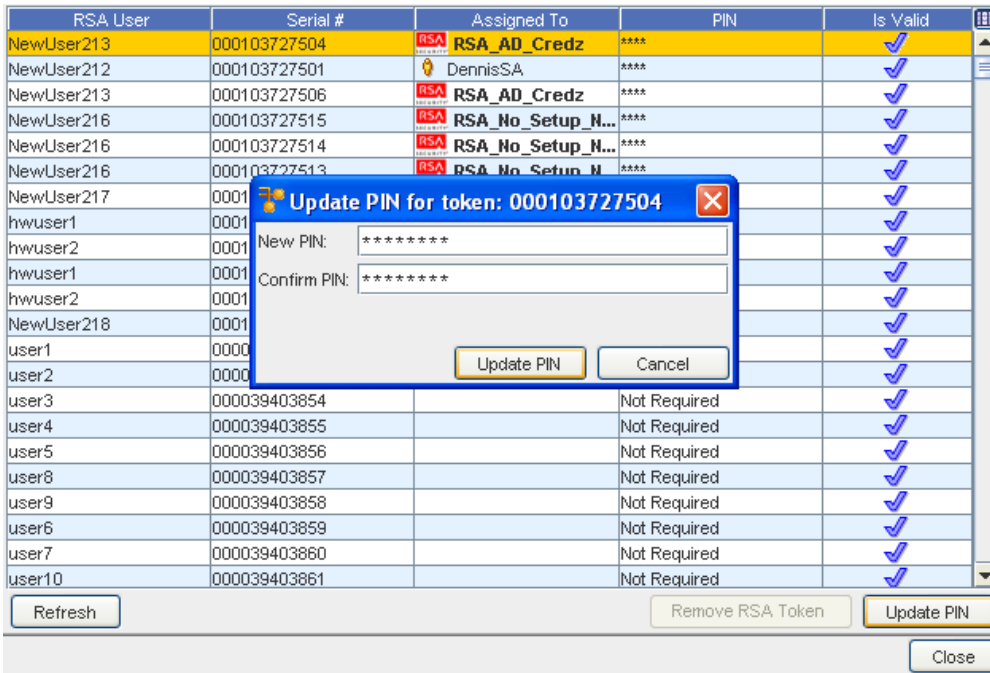
#### Removing RSA Tokens from the Global RSA Token Viewer Window

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Global -> Global RSA Token Viewer**.
- 3 Click the **Remove RSA Token** button.
- 4 Click **Yes** to confirm the removal of the RSA credential.

#### Updating the PIN for an RSA Token from the Global RSA Tokens Viewer Window

- 1 From the menu bar, select **Tools -> System Administration**.

- Next, select **Global** -> Global RSA Token Viewer.
- At the bottom of the Global RSA Tokens Manager pane, select **Update PIN** . The Update PIN window (for the user you selected) now opens.



- At the Update PIN screen, enter a valid **PIN** in the New PIN box.
- Enter the **PIN** again in the Confirm PIN box.
- Click the **Update PIN** button.

See:

[About RSA](#)

## Working with Network Settings

### Network Settings Overview

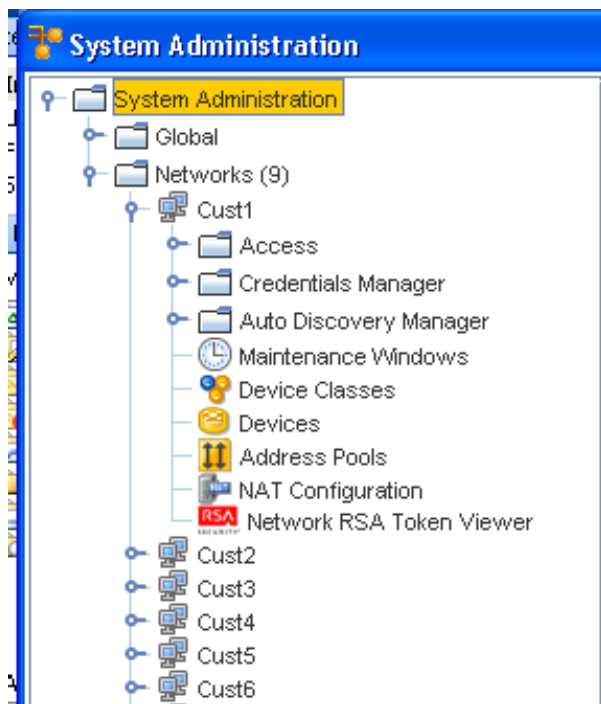
From this area within System Administration, you can create new Networks, set Network level communication protocols, create Network credentials, and run Auto Discovery jobs to manage devices within the Network. Also from this area, you can set Network priorities, schedule Network pull jobs, and create production network baselines.

Network settings are used to configure Network Configuration Manager access and communication settings. Network Configuration Manager uses permission levels that permit you to strengthen the security of, and access to, your networks.

Network Configuration Manager has the flexibility to implement settings and changes down to the device level and the global settings level (a standard to which all networks, and their devices comply).

The **Networks** section allows you to complete the following:

- Creating networks
- Running Auto Discoveries
- Overriding Device Classes
- Communications
- Maintenance windows
- Creating IP Address Pools
- Establishing network-local credentials and out-of-band servers



The System Administration window has a traditional two frame view. On the left in the Navigation Pane, are the entry points to the major sections of the System Administration module, including:

- Access - which can be expanded to include:
  - Out-of-Band Servers
  - Device Servers

This allows you to configure device servers and out-of-band server settings, and which devices will be Auto Managed when the devices are Auto Discovered on the servers. You can also reassign a device to another device server from this view.

Here are the remaining components of Networks in the System Administration too:

- Credentials Manager
- Auto Discovery
- Maintenance Windows
- Device Classes
- Devices
- Address Pools
- NAT Configuration
- Network RSA Token Viewer

Within the above components, you are able to complete the following tasks:

- Configure any **Out-of-Band servers**
- Determine which **Device Servers** are associated with your network
- Set which devices are automatically managed by Network Configuration Manager when **Auto Discovery** runs
- Configure cross network **shared and local** credentials
- Add, edit and delete **Data Fields**
- Manage **users and groups** and their network permissions
- Manage the **Authentication Servers**, and determine user security
- Manage the **locking features**

## Creating Networks

The ability to create networks in Network Configuration Manager is reserved for users with *System or Network Administration privileges*.

After a network is created, but before any devices can be discovered into the network, you need to:

- Associate a network with one or more device servers that will manage the devices in the network
- Assign groups and users to your network
- Create auto-discovery jobs

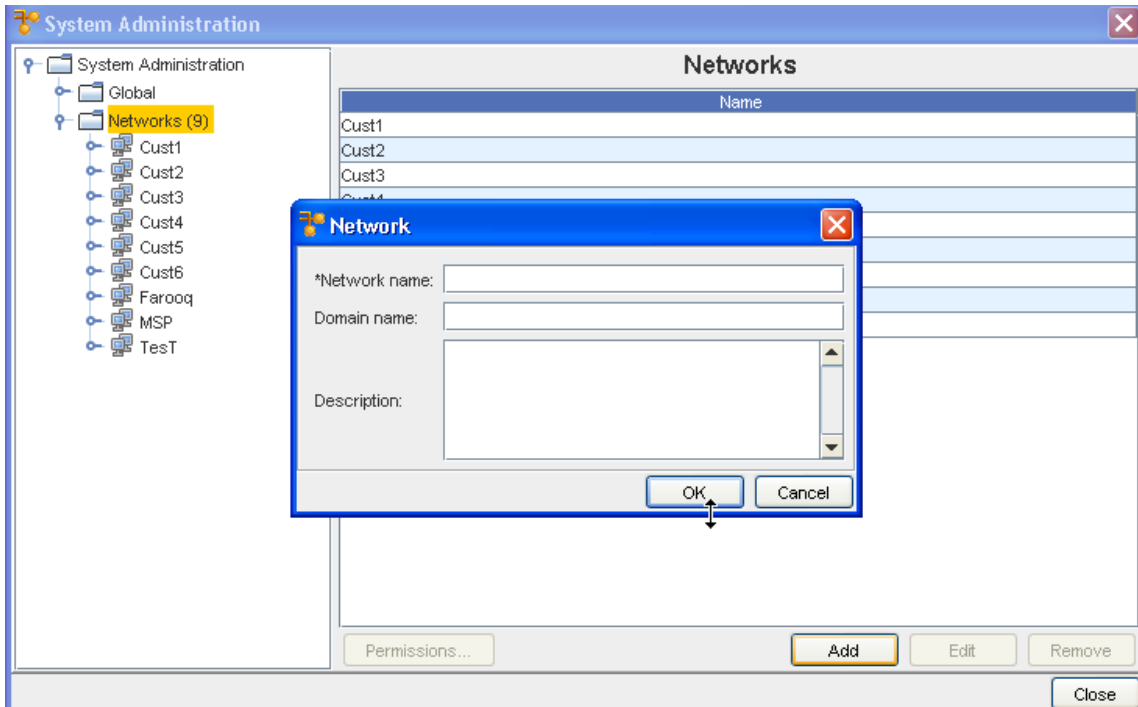
---

**Important** Depending on the way you setup your networks, the networks can be created *before* adding users and groups, or you can create the users and groups *before* creating the networks. Either way is acceptable.

---

To create a new network,

- 1 From the menu bar, select **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, click **Networks**. In the right pane, a list of all current networks displays and the Add button is activated at the bottom of the window.



- 3 Click **Add**. The Network window opens.
- 4 At a minimum, you must enter a **Network Name**.
- 5 Optionally, enter a **Domain Name** and **Description** of the network.
- 6 When finished, click **OK**. The Network window closes. The navigation pane refreshes and the new network is added to the list of networks.

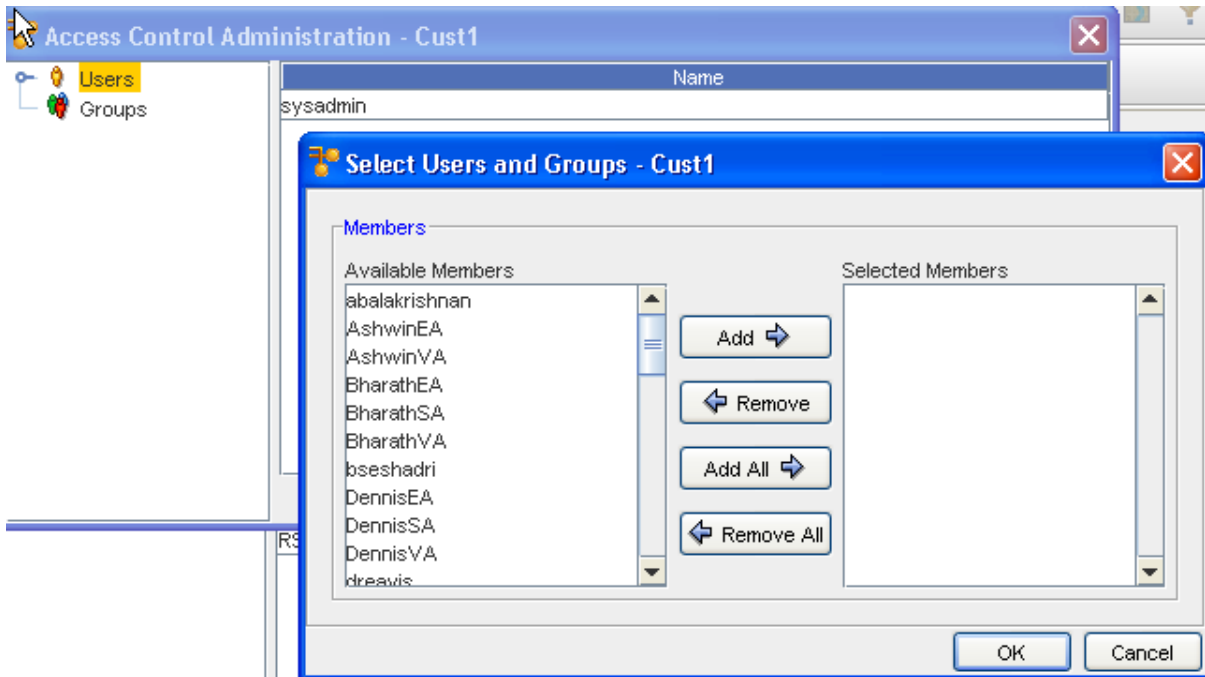
You can now add one or more device servers to manage your network devices.

## Setting Network Permissions

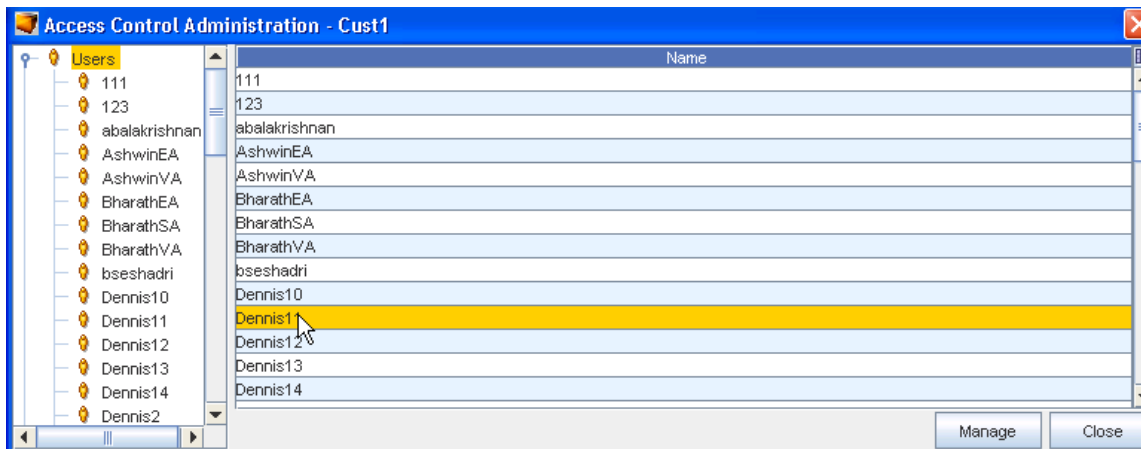
Setting permissions at the Network level for a specific user/group, overrides all other permissions assigned to the network for the specified users/group.

To set network permissions for a user/group,

- 1 After selecting a network, click **Permissions....** The Select Users and Groups - [Network Name] window opens.



- 2 In the navigation pane, select the **User or Group** whose permissions are to be defined.
- 3 Select the User name or names, then click Add.
- 4 Now, click and expand on the Users name in the left panel.



The right pane populates, and displays as follows:

The permissions set in the right pane dictates the actions that the user/group can complete at the

network level. Each action has been grouped according to the module where it resides.



Set permissions for BharathEA

Override Credentials

Manage User Access

Manage Templates

Manage Queries

Manage Compliance

Network

Edit  Delete  View

Workspace

Create  Edit  Delete  View

Device

Create  Edit  Assign Credentials  View Details

View Sensitive Data  Manage OS  Run Non-Scheduled  Run Cut-Throughs

Job

Schedule  Approve

View

Create  Edit  Delete

Override

Select All Deselect All

Reset Apply Close

By default, if the highest level check box is selected, the user/group receives permissions for **all actions** within the group. For example, in the above graphic, View has been selected at the highest level and each included tasks is also selected.

- 5 Select the **areas** for which the user is to have access.
- 6 If the user/group does not require one or more of the included task permissions, click that related check box to de-select the option.
- 7 Repeat **steps 3 and 4** for each area where the user/group requires access.
- 8 If a user/group requires access to all network options in the Access Control Administration window, at the bottom of the window, click **Select All**.
- 9 When finished, click **Apply**. The window remains open allowing you to select other users (or groups) and then set other permissions.

Override Credentials	Allows user/group to set this override for an individual use. This allows the user to update credentials for a job or non-scheduled tasks. For example, when one user must complete an operation or task for another user.
Manage User Access	Allows user/group to manage the access each user has
<b>Manage Templates</b>	Allows user/group access to Create or Modify Templates that reside in the Automation Library. By default, you can view existing templates.
<b>Manage Compliance</b>	Allows user/group to Manage the Compliance attributes
Manage Queries	Allows the user/group to Create, Update, and Delete existing queries
<b>Network</b>	Allows the user/group to <b>Edit, Delete</b> or <b>View</b> networks details. By default, if you are provided Edit or Delete permissions, View is automatically set.
<b>Workspace</b>	Allows the user/group to <b>Create, Edit, Delete</b> or <b>View</b> workspaces. By default, if you are provided Create, Edit or Delete permissions, View is automatically set.
<b>Device</b>	<p><b>Note</b> By default, when a user/group is given permissions to view Networks and Workspaces, they are able to view their devices.</p> <p>Allows the user/group to <b>Create</b> and <b>Edit</b> devices. The <b>View Details</b> check box gives the user/group the ability to view the device properties.</p> <p>The <b>View Password</b> check box allows user/group to View the passwords that must be used to access the device properties.</p> <p><b>Manage OS</b> check box allows the user/group to Modify the OS of the device.</p> <p><b>Assign Credentials</b>, complete <b>Run Cut-throughs</b>, and <b>Run Non-Scheduled Jobs</b></p>
<b>Job</b>	Allows the user/group to <b>Approve</b> or <b>Schedule</b> jobs that are created for the device config
<b>View</b>	Allows the user/group to <b>Create, Edit</b> or <b>Delete</b> Views of the network
<b>Override</b>	Selecting this option allows the user/group to Override any permissions that are set on levels with the permissions defined here

Or, if you are not making changes to the other permission level settings, click **Close**.

## Editing Networks

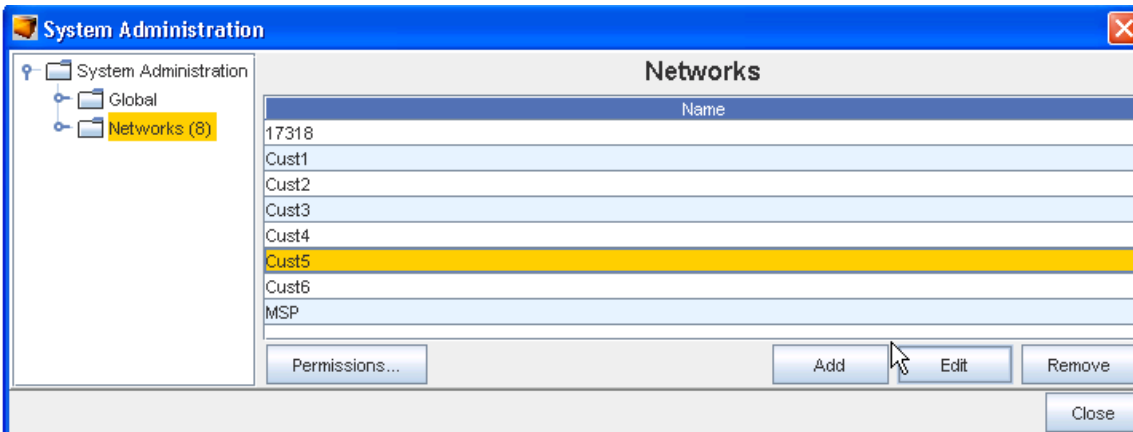
When networks are created, only basic information about the network is entered, such as the name and the domain. After you have created a network, additional information can be entered.

**Note** Network Properties can be managed for a network from inside of System Administration by any user with System or Network Administration privileges.

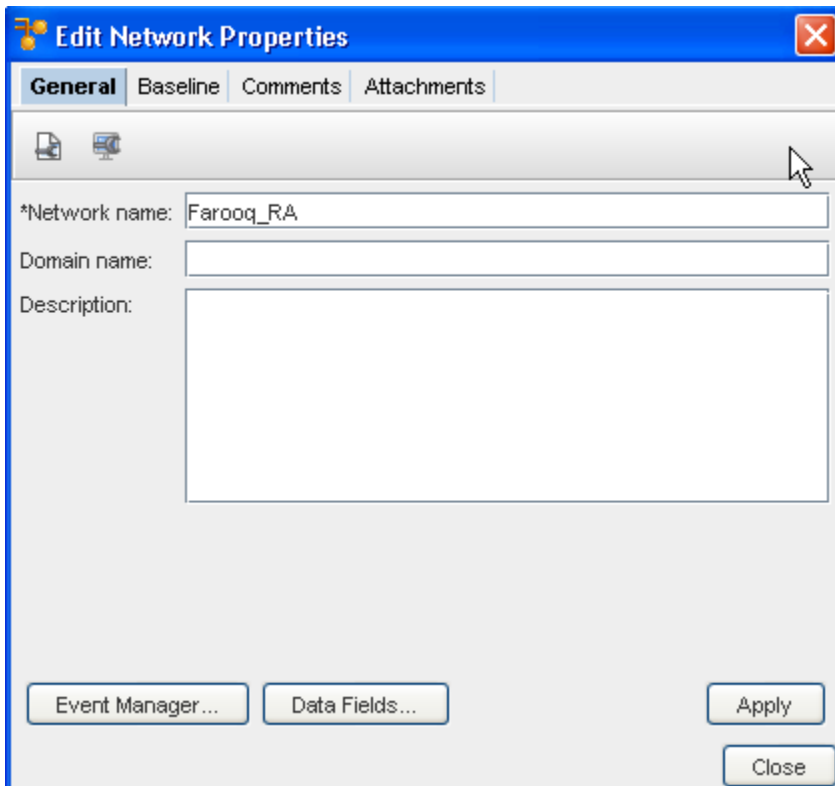
To edit network properties,

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, open **Networks**. In the right pane, a list of all current networks is displayed.

- 3 Click the **network name** . The Edit button is activated at the bottom of the window.



- 4 Click **Edit**. The Edit Networks Properties window opens.



- 5 At the Edit Network Properties window, make the needed changes to the information contained within each tab.
- 6 Click **Apply**, then **Close** when you have completed your changes.

Data Fields

## Removing Networks

When networks are removed, the devices that are managed by the networks are returned to an *Unclassified state*, unless they are also being managed in other networks.

If a network is managed by another network, the status of the device will remain as *Managed*. Be sure to consider the ramifications to a device before deciding to delete a network.

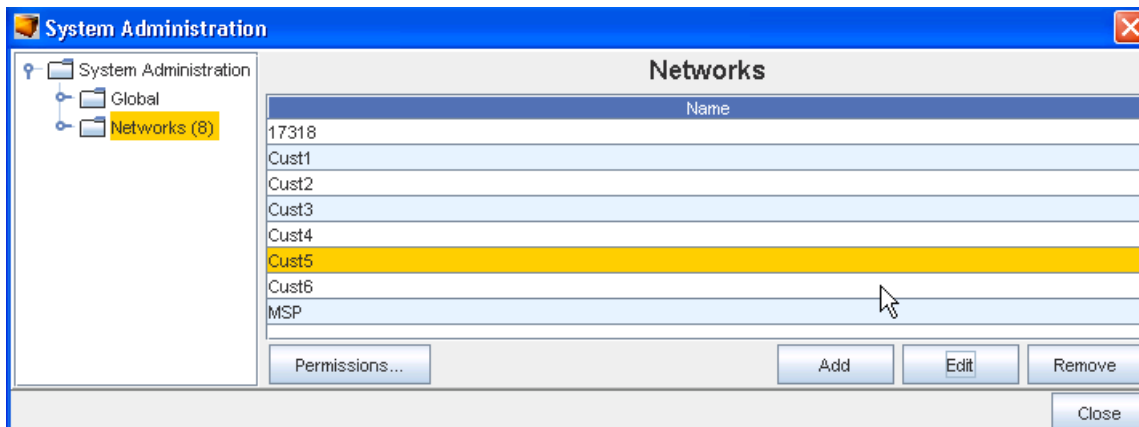
---

**Note** Once a network is deleted, there is no retrieval mechanism to restore the network. Take care when deleting networks.

---

To delete a network,

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, click **Networks**. The right pane refreshes with the list of current networks.



- 3 In the right pane, select the **network** to be removed. At the bottom of the window, the Edit and Remove buttons activate.
- 4 Click **Remove**.
- 5 If Okay, click **Yes**. If **Yes** is selected, the network is removed from the list of networks in the navigation pane.

## Managing Network Access Permissions

When a network is created by the System Administrator, users and groups must be assigned permissions to the network before they can complete any network tasks.

If network permissions are not set by the user/group, then the general permissions assigned to the user/group is used by default.

---

**Note** Each user/group is assigned their own permissions when they are set up in Network Configuration Manager. These default permissions can only be changed by overriding them, and setting specific permissions.

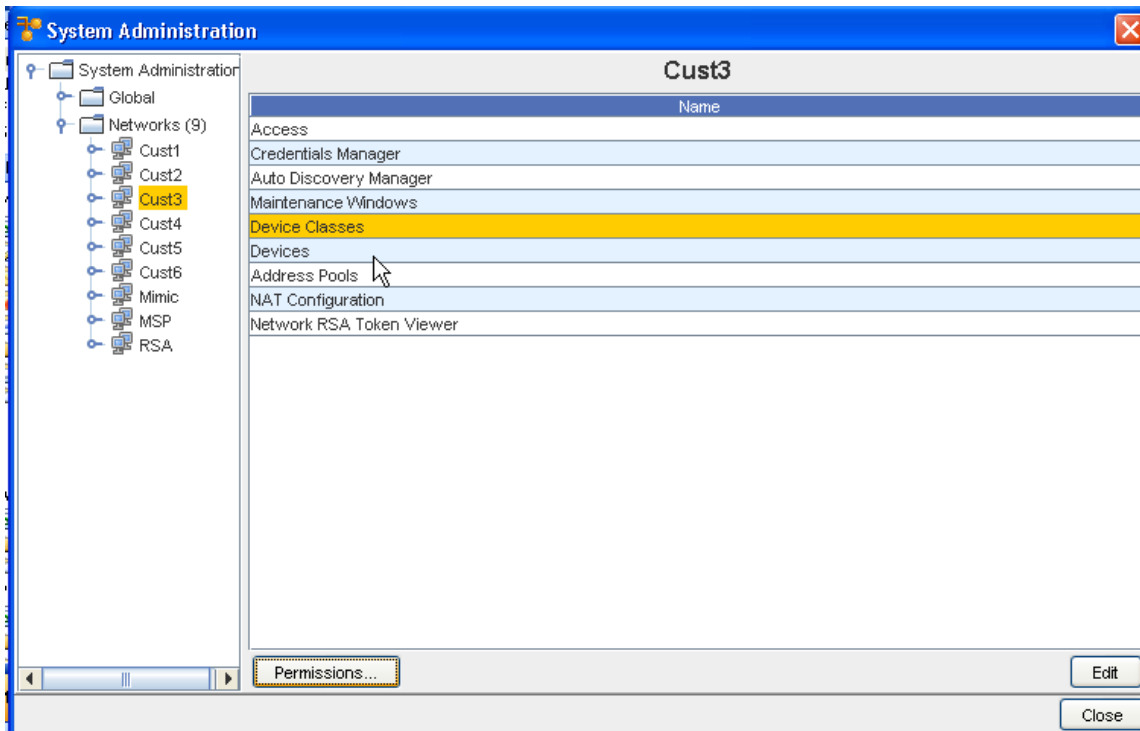
---

Setting network permissions for users/groups is a two step process:

- Select the user/group who is to have access to the network
- Select the network permissions for the user

To designate users and groups to have Network permissions,

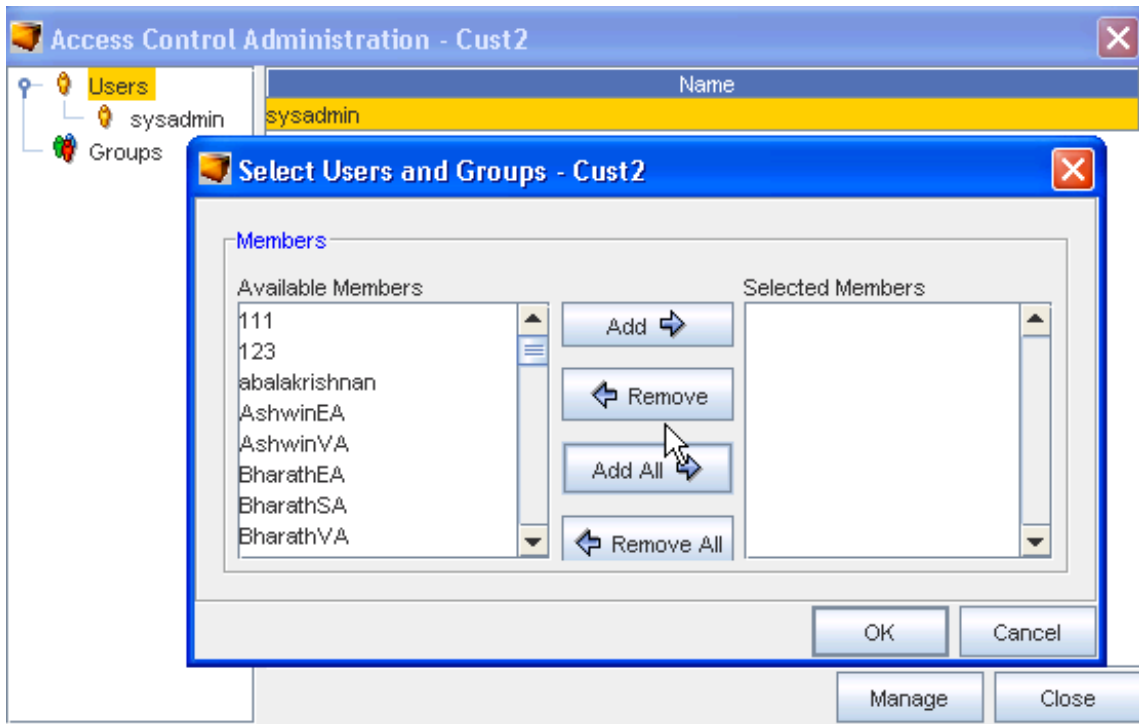
- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand **Networks**. The right pane contains all available networks. Select the **network** from this list. Or... In the navigation pane, select the **Network**. The right pane contains the Network sub-menus.
- 3 In the lower left portion of the window, click **Permissions**. The Access Control Administration - [Network Name] window opens.



There are two groups:

- Users
- Groups

All users and groups that are available in Network Configuration Manager are in the tree menu. Depending the network selection, the right pane contains a list of all Users or Groups currently associated to the network.



- 4 After selecting Users or Groups, click **Manage**. The Select Users and Groups [Network Name] window opens.
  - Users and groups that do not have permissions are listed in the **Available Members** column.
  - All users and groups with permissions are listed in the **Selected Members** column.

By default, your own user name is listed as a user. All others that have been given permissions are categorized, and listed in one of the two groups.

- 5 To give users or groups permissions to the workspace, click the **name of the user or group** in the Available Members column.

---

**Note** A string of users/groups can be selected by holding down the Shift-key while selecting users/groups. Or, select multiple, non-sequential users/groups can be selected by holding the Ctrl key while selecting users/groups.

---

- 6 Click **Add**. The selected users and groups are moved to the **Selected Members** column, and now have permissions to the workspace. Or... To remove a user or groups permissions, in the **Selected Members** column, select the name or group.
- 7 Click **Remove**. The selected users and groups are moved to the Available Members column and no longer have permissions to the workspace.
  - Clicking **Add All** moves all users and groups listed in the Available Members column to the Selected Members column.

- Clicking **Remove All** moves all users and groups back to the Available Members. If you complete this action, remember to put your own user name back into the Selected Members column.
- 8 Once you have assigned the users and groups that are to have access to the workspace, click **OK**. The Select Users and Groups window closes, and your selection is added to the list of Users (or Groups).

The Access Control Administration window refreshes. All users and groups are re-categorized to reflect the changes that were made. You are now able to [Setting User and Group Permissions](#)

## Setting Workspace Permissions for Each User and Group

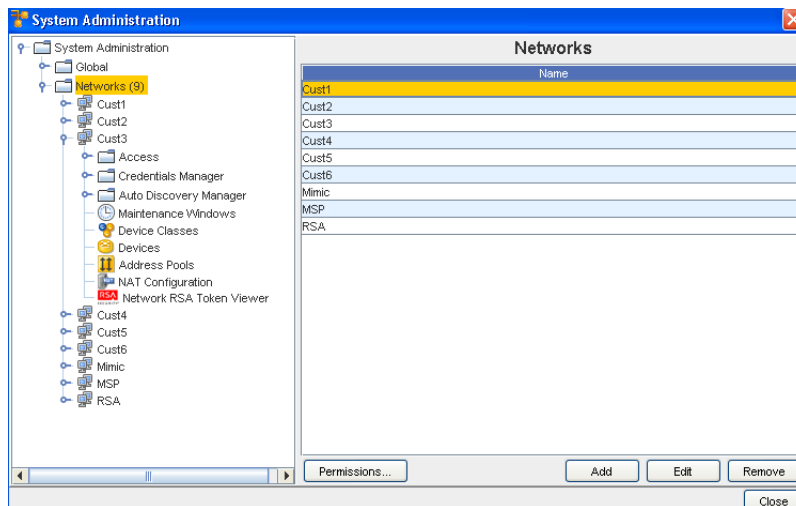
There are two phases for setting permissions for a workspace:

- [Setting Workspace Permissions](#)
- Selecting the permissions that each user and groups will have to the workspace

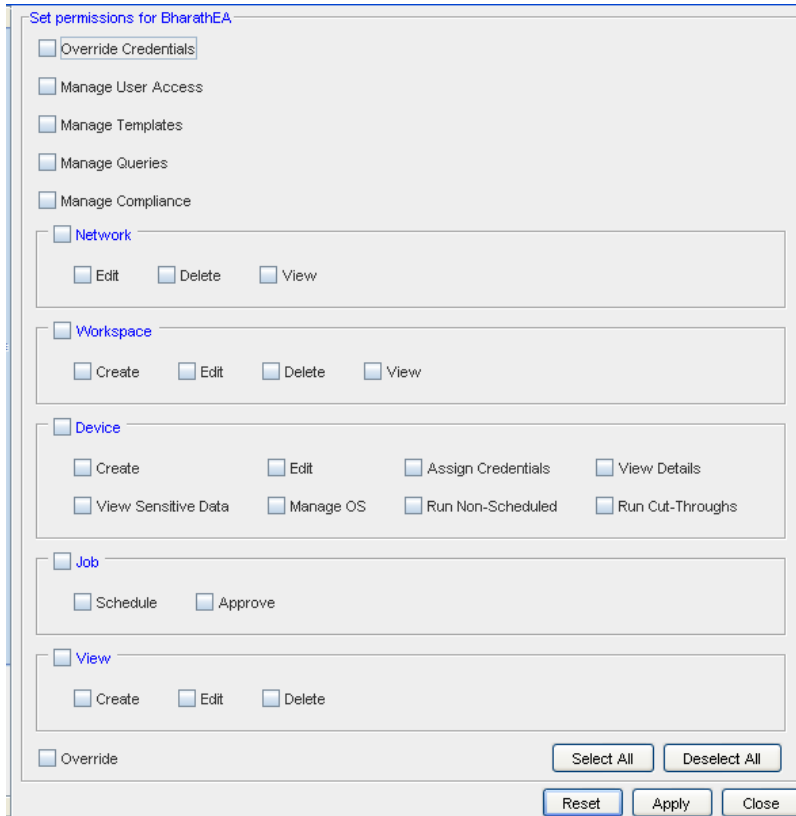
Once you have determined the users and groups that have permissions to your design workspace, you can determine the set of permissions the users and groups will have.

Permissions are set through the Access Control Administration window. For more information on using this window and setting the permissions, see [Setting Workspace Permissions](#)

To set permissions for each user and group,



- 1 From System Administration, select **Networks**. Next, make a selection (in this example, Cust3 was selected from the listing of networks). Now, select **Permissions** to get to the Access Control Administration window. Expand the navigation tree and locate the **user or group**.
- 2 Click the **user or group**. The Set Permissions available for the displays in the right pane.



- 3 By default, all users and groups are provided view access. Using the check boxes, select any additional permissions for the user or group.
- 4 Make your selections for **each task** detailed in this window.

---

**Note** Selecting or clearing the top check box of any category of permissions automatically selects or clears all permissions within the category.

---

- To select all permission, click **Select All**.
  - To clear any existing permissions, and begin your selections with a clean slate, click **Deselect All**.
  - To return to the original set of permissions, click **Reset**.
- 5 Once you have finished setting the permissions, click **Apply**. The Set permissions pane closes, and the Access Control Administration window refreshes.

For a user

## Network - Access

## Network - Out-of-Band Servers

### Out-of-Band Servers Overview



Network Configuration Manager provides an option for setting up *alternative communication methods* using Out-of-Band Servers.

For example, if there is a problem with a device and traffic cannot flow through the network, an *alternate path* can be set using a terminal server to reach the network nodes--even when the network is down!

Out-of-Band servers are used when you need a secure, remote, emergency network access path to **manage** and **troubleshoot device issues** when:

- The device is not on the network
- The device is not network manageable
- The network is down

Network Configuration Manager allows you to set up out-of-band servers at two levels:

- Global level
- Network Level

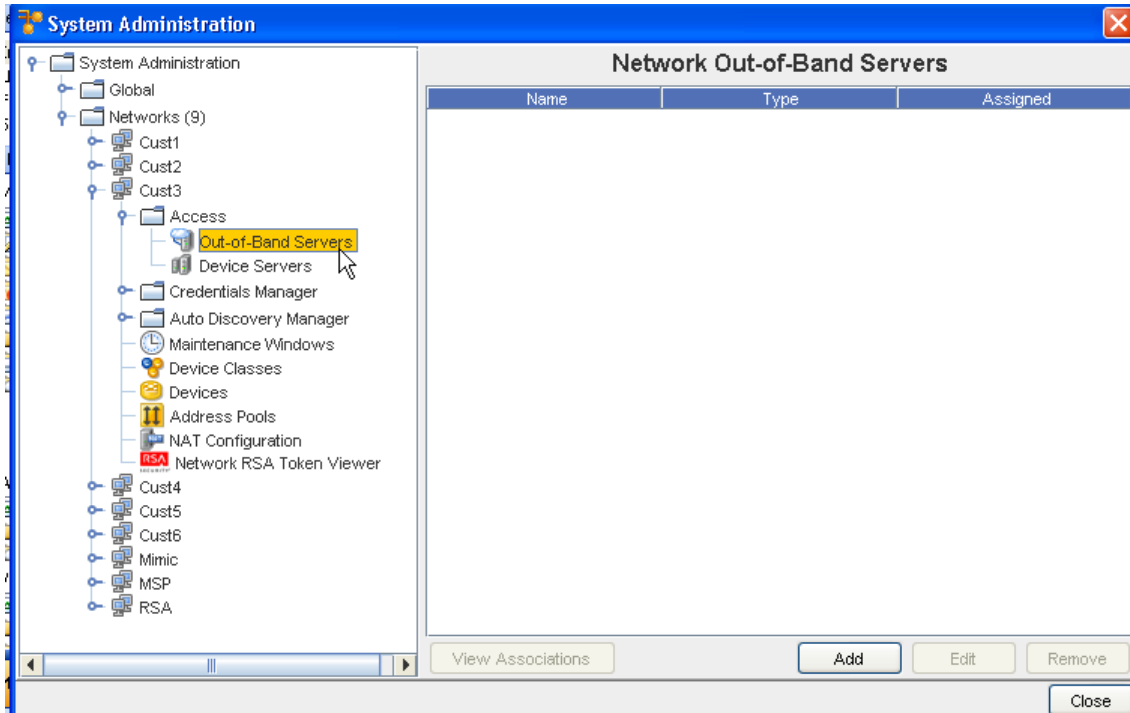
**Network level out-of-band servers** allow you to set up access to out-of-band servers that are used by specific networks only.

When you have configured an out-of-band server for a network, the network defaults to use the network level out-of-band server, unless otherwise indicated.

### Out-of-Band Servers (Networks)

To access the Network Level set up,

- 1 From the menu bar, select **Tools** -> **System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Networks folder**.
- 3 Double-click the **network name**.
- 4 Expand the **Access** folder.
- 5 Click the **Out-of-Band Servers** . The Network Out-of-Band Servers window opens in the right pane.

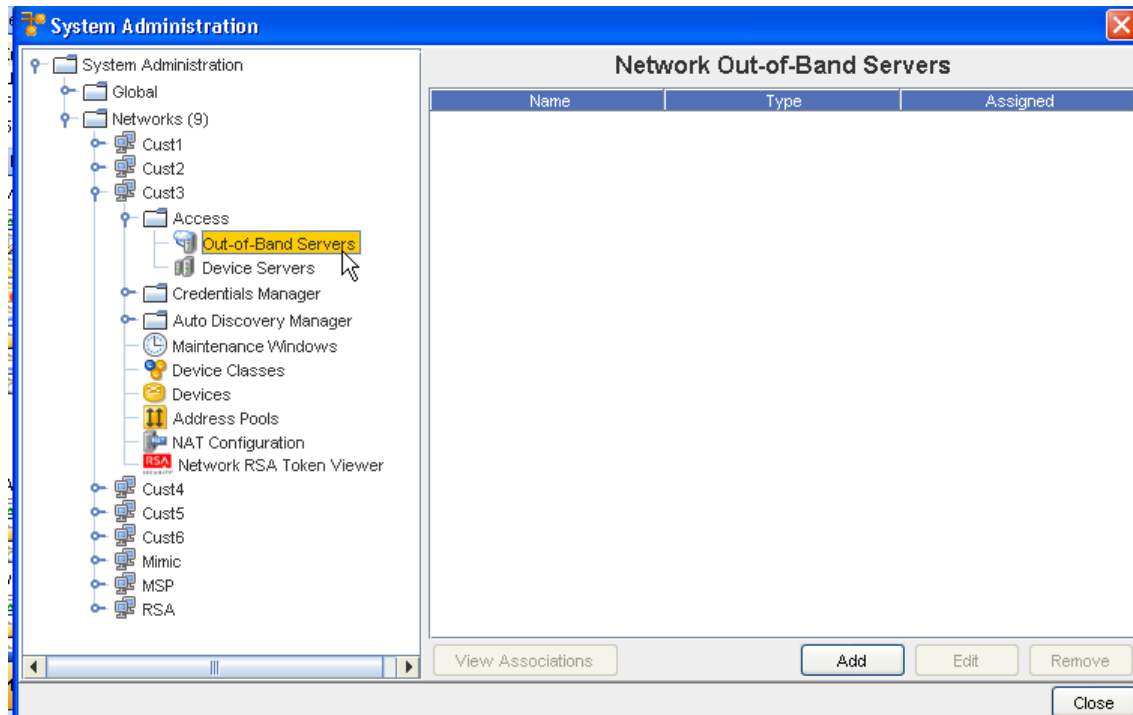


From this window you can View Associations, Add a server, Edit existing servers, or Remove an out-of-Band Server.

### Network - Viewing Associations

To view Associations,

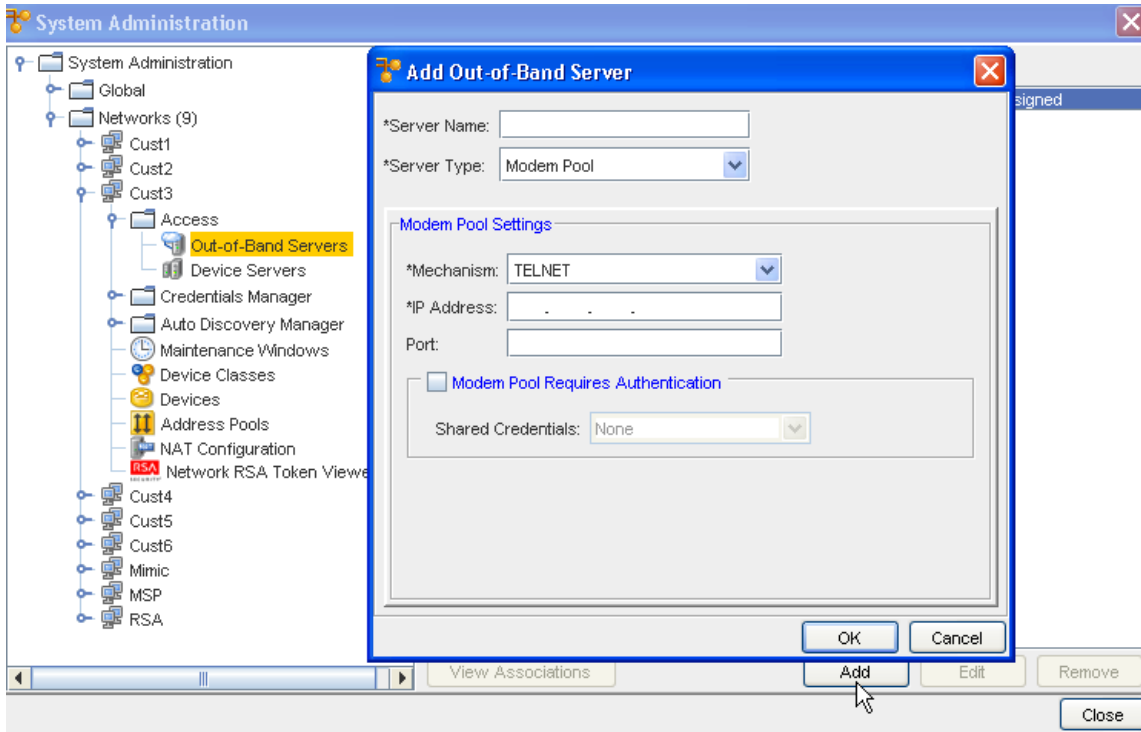
- 1 From the **Network Out-of-Band Server** window, click **View Associations**.
- 2 The View Associations window for that Server opens, allowing you to view the Devices associated with the server. You can resort the order of Devices and Device Classes using the up arrow. Click **Cancel** to leave this window.



## Network - Adding Out-of-Band Servers

To Add an Out-of-Band Server,

- 1 From the **Network Out-of-Band Server** window, click **Add**. The Add Out-of-Band Server window opens.



The following fields are available. Note that the required fields are identified by an asterisk (\*).

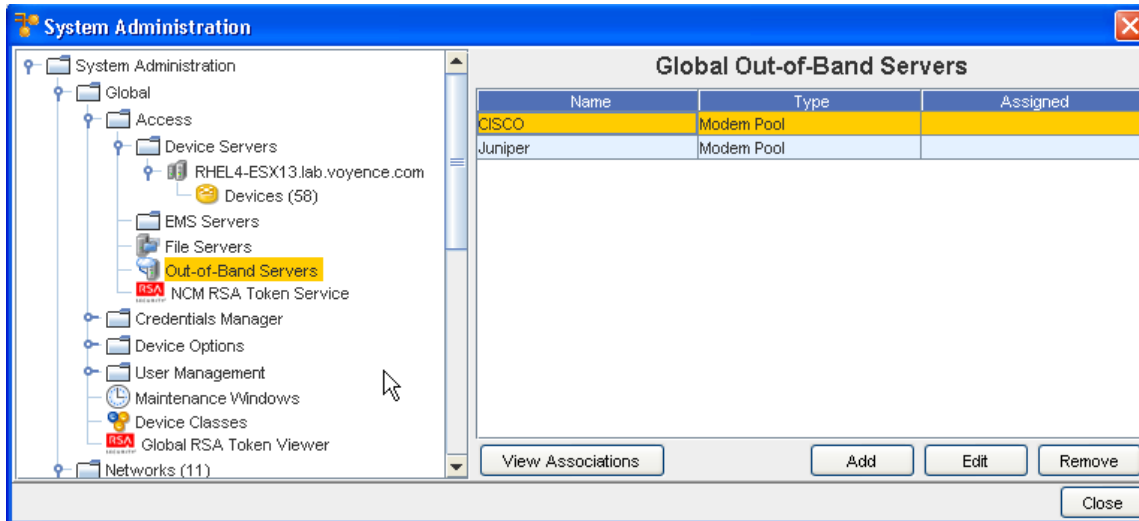
- 2 Complete the setup of the out-of-band server options, as needed.
- 3 When finished, click **OK**. The Add Out-of-Band Server window closes.

Field	Description
Server Name	The name of the server being used for out-of-band access
Server Type	The type of server being used. Current options: - Modem Pool Settings - Terminal Settings
Modem Pool Settings	Based on the selected server type, the available fields are:
Mechanism:	Telnet or SSH
IP Address:	IP address used for connection
Port:	The Port Number
<b>Modem Pool Requires Authentication</b>	The <b>Modem Pool Requires Authentication</b> check box should only be used if you have configured a User name and Password access security in Shared Credentials. You can also select from the listing of <b>Shared Credentials</b> using the drop-down arrow to see the list.

The configured out-of-band server is listed in the Out-of-Band Server window.

## Editing an Out-of-Band Server

- 1 Select a Server from the listing in the **Network Out-of-Band Servers** window, then click **Edit**.



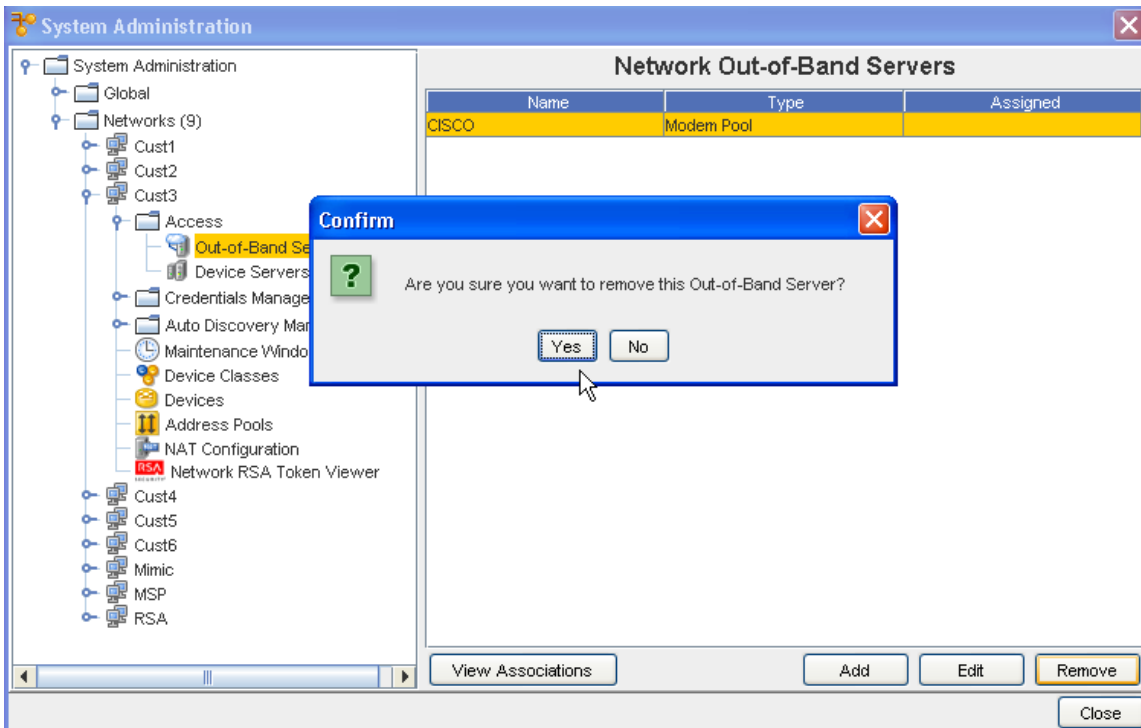
The Edit Out-of-Band Server window opens.

- 2 Make any changes needed to the existing information, then click **Ok**.

## Removing an Out-of-Band Server

To Remove an out-of-band set up at the network Level,

- 1 From the menu bar, access **Tools** -> **System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Networks** folder.
- 3 Double-click the **network name**.
- 4 Expand the **Access** folder.
- 5 Click the **Out-of-Band Servers** . The Network Out-of-Band Servers window opens in the right pane.



- 6 Select the server you want to remove, then click **Remove**.
- 7 Click **Yes** at the confirmation message.

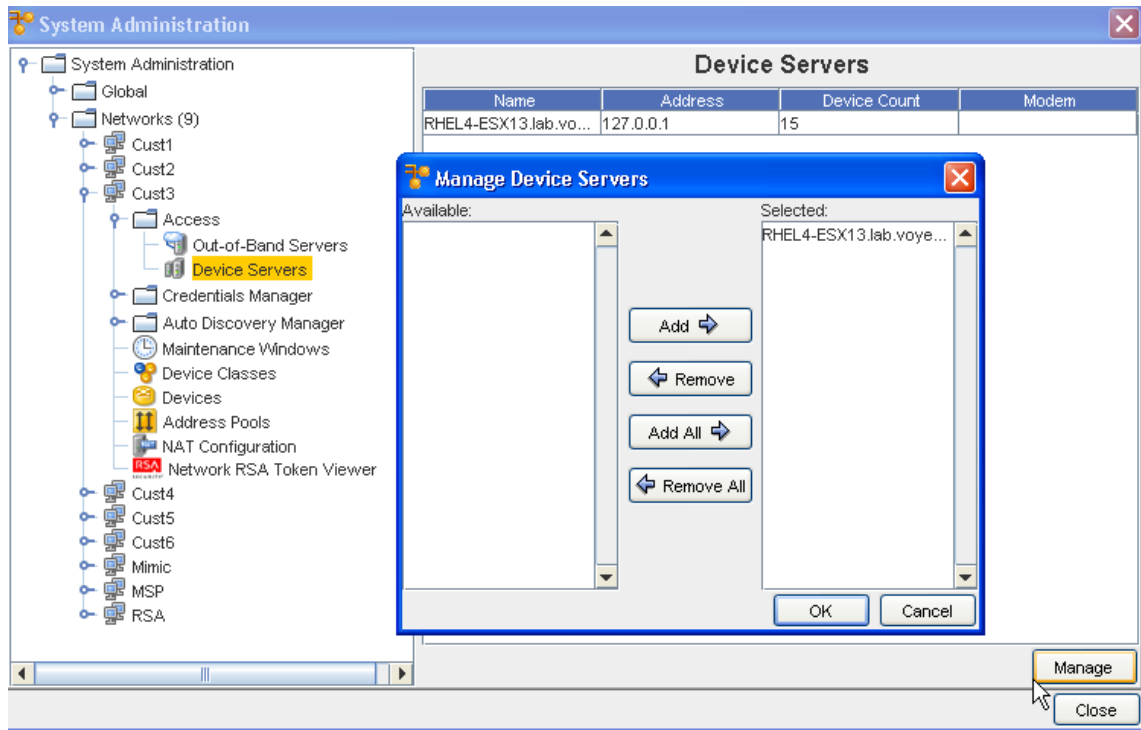
## Network - Device Servers

### Assigning Device Servers

Device Servers provide the control and communications or all network devices.

To assign a device server,

- 1 From the menu bar, access **Tools**.
- 2 From the menu options, select **System Administration**. The System Administration window opens.
- 3 On the tree menu, expand the **Networks -> Access** folders.
- 4 Open the **Device Servers** folder . At a minimum, at least one Device Server is available.



The basic properties of the Device Servers are listed on the right. Except for the number of the devices on the Device Server, these details can be edited on the Properties tab.

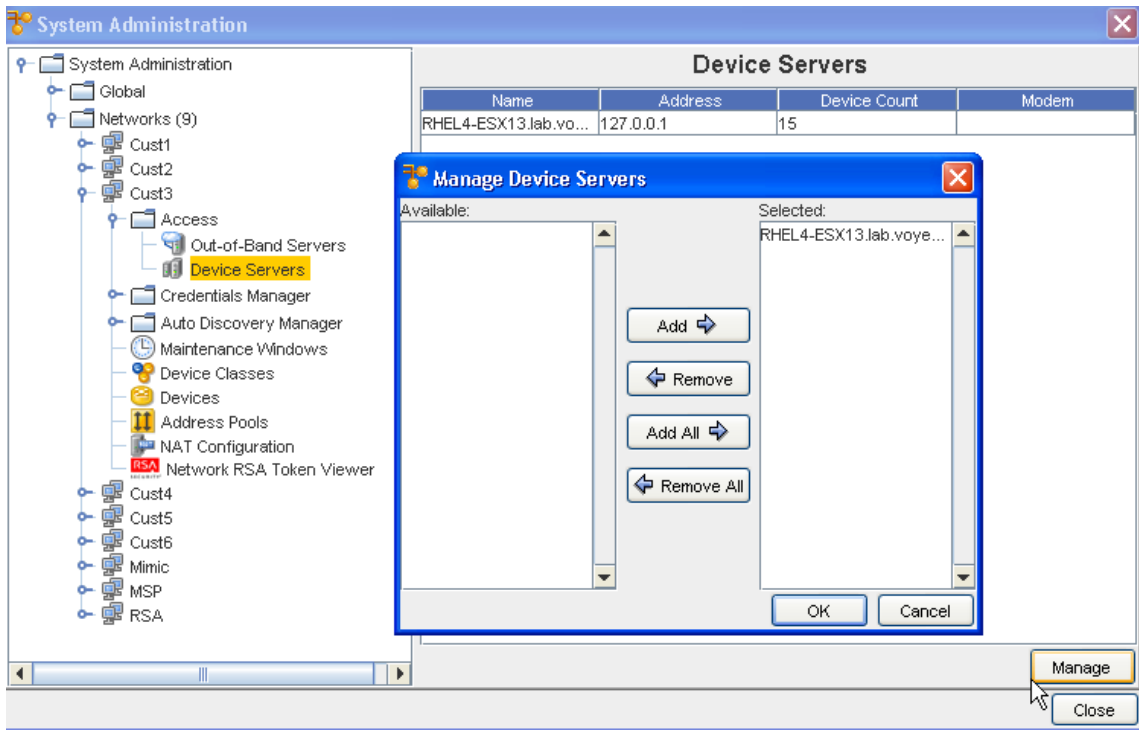
- 5 To access the **Manage** feature, in the right pane, select a **Device Server**, then click **Manage**.
- 6 Select at least one Device Server from the **Available** section, and move the selected servers into the **Selected** section. You can also remove unneeded servers back into the Available pane using the Remove buttons.
- 7 Click **Ok** after moving the selected servers. Servers selected are now listed in the Device Servers window.

## Managing Network Devices

Once Networks are created, they need to have a device server associated to them. The device server is the *container* that holds the devices. You cannot complete an Auto Discovery until you have associated one or more device servers to a network. The device server to device relationship is set when creating an Auto Discovery job.

To associate device servers,

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand **Networks**. The current network list displays.
- 3 Expand the network folder, then click **the network name**.
- 4 Open the **Access** folder. The Access folder contains two options:



- Out-of-Band Servers
  - Device Servers
- 5 Click **Device Servers** . All device servers currently associated with the network display in the right pane.
  - 6 Click **Manage**. The Manage Device Servers window opens.  
The Manage Device Servers window has two columns:
    - Available - Contains device servers that can be associated with the network
    - Selected - Contains device servers that are currently associated with the network
  - 7 In the Available column, select a **device server**.
  - 8 Click **Add**. Or, to remove a device server from the Selected column, in the Selected column, select the **device server**.
  - 9 Click **Remove**. The device server is moved back to the Available column, and is no longer associated with the network. If needed, the device server can be re-associated at a later date.
  - 10 When finished, click **OK**. The Manage Device Servers window closes.  
The System Administration window now reflects the adjusted device servers list.

## Networks - Credentials Manager

### Credential Manager Overview



Credential management permits the secure abstraction of User ID and Password pairs from those who use them. There are four credential types; Account, Community String, SNMPV3, and Privilege Password. Account credentials can consist of a User ID/Password pair and a Privilege Password reference.

Bulk load utilities permit the mass association and change of credential to devices, or from device properties and the right-click menu.

Credential associations show the devices that are currently assigned to each credential.

Additional internal auditing enhancements are now available allowing a System Administrator more insight into who is accessing devices, and what tasks are being completed within the system.

- As the System Administrator, you now have a method of dynamically controlling the credentials used for any device operation, as well as being offered the flexibility to deal with special and exception scenarios to manage certain devices.
- As a System Administrator, you can now determine if credentials are to be governed by Global Credential Configuration settings, or allow Credential Configurations at the Network level to override the Global Configuration settings.

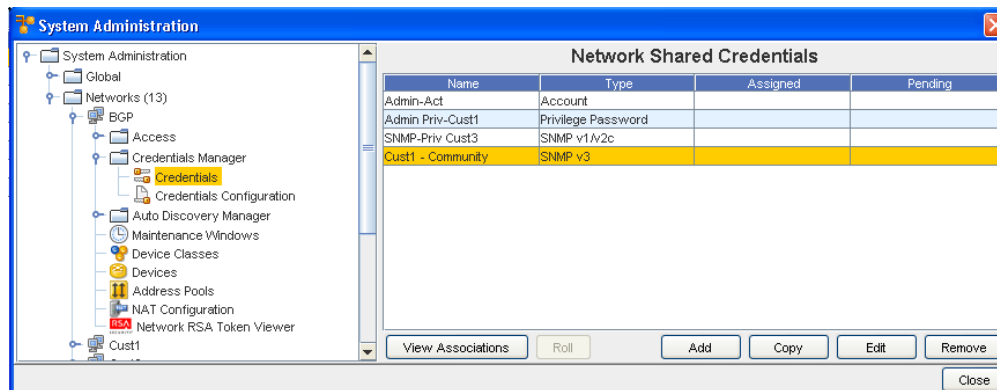
---

**Important** The Network credentials can override the Global configurations providing the user the ability to set Credential Policies for an individual Network.

---

The Credentials Manager has two options that you can view and work with:

- Credentials
- Credentials Configuration



From **Credentials** you can:

- View Associations
- Roll
- Add
- Copy
- Edit

- Remove

From **Credentials Configurations** you can select configuration options:

- Use Static Device Assignment
- Use Login Credentials
- Prompts User

## Credentials Best Practices

- Use credential management to specify how to secure your device communications.
- Use Credentials Configurations to determine the credentials that need to be used for communication with the devices.
- Manage credentials on a network or global basis, **not per device** . This allows you to make changes to a single credential, rather than make changes to each of many individual devices.
- If your Device Server and its devices are within a secured private network, then using unsecured protocols such as Telnet, FTP, and SNMP provides better overall performance and management ease, as well as better device coverage.
- If your Device Server and its devices are not within a single secured private network, then use credential management to disable non-secure protocols, and allow only secure protocols, such as SSH and SCP.

### When using SNMP Communications

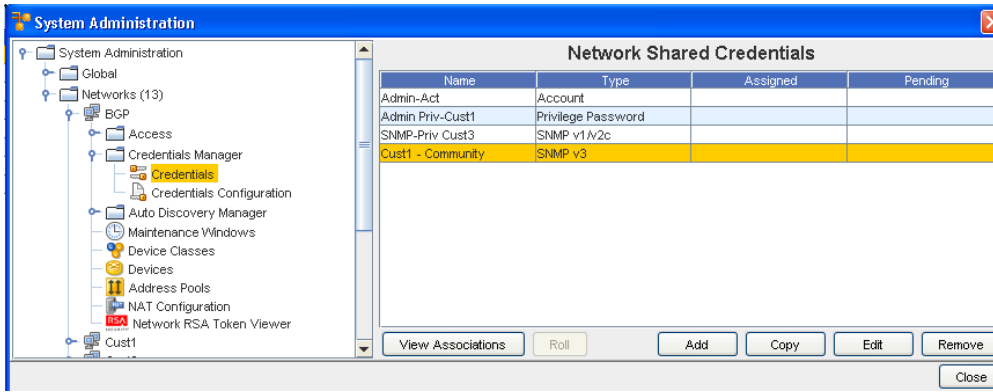
- Enabling SNMP communications provides the best overall quality of device information, with the greatest span of device coverage. The cost is a lower network security on traffic between the Device Servers and the monitored devices.
- Disabling SNMP communications gives you improved network security (by disabling non-secure SNMP traffic). The cost is having less device-specific information available, from a fewer number of device types. Information that is lost could include connection information, memory availability, and system information.

## Setting Network Level Credentials

To set credential access,

- 1 From the menu bar, access **Tools -> System Administration**.
- 2 In the navigation pane, select **Networks**.
- 3 Expand the Networks folder and select the appropriate **network**.
- 4 Expand the Network's folder, then select **Credentials Manager, and then Credentials** .

The Network Shared Credentials window appears similar to the following:

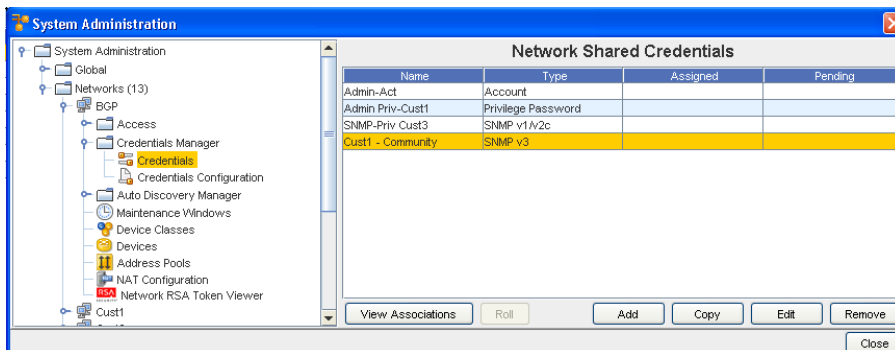


- 5 From here, you can **Add** a new credential, or if there are existing network credentials, you can complete the following actions:
  - [Viewing Network Credentials Associations](#) - to view the associations and review the Devices and the Auto Discovery information
  - [Rolling Credentials](#) - to go to the Roll Candidate Selection screen and select a candidate. Then go to the Credential Roll Job window to schedule the roll.
  - [Copying Network Shared Credentials](#) - to make an exact copy of this credential
  - [Adding Global Shared Credentials](#)- to add a credential
  - [Editing Network Credentials](#) - to make changes to existing information
  - [Remove Network Credentials](#) - to remove (delete) the credentials
  - **Close** - to leave this window

## Viewing Network Credentials Associations

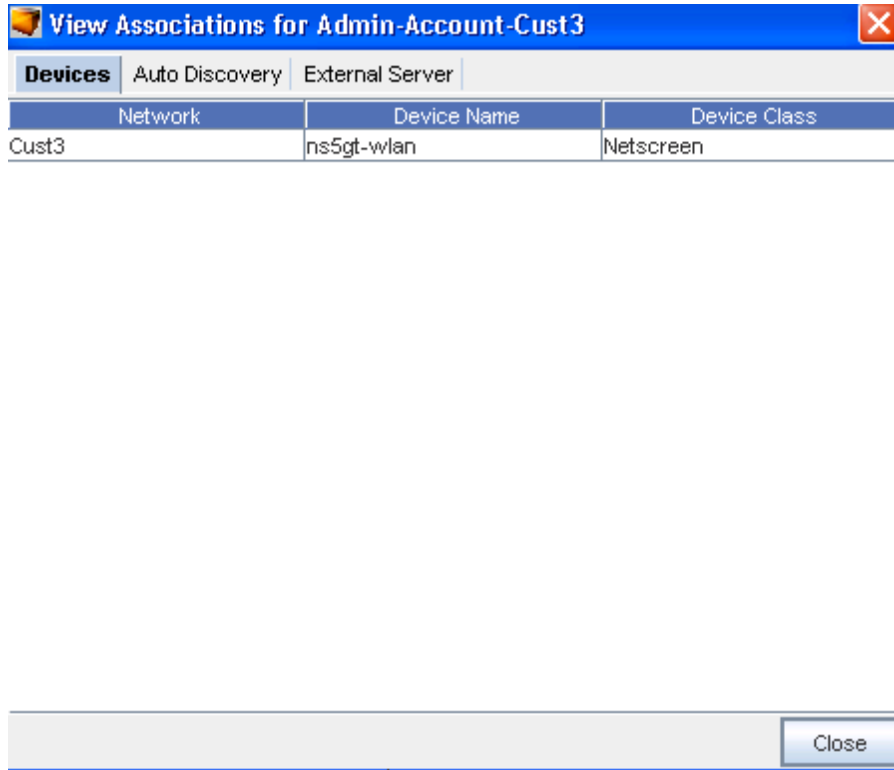
Credential management is provided at the Network level, as well as at the Global level. Network credentials are only available for devices within that specific Network. There is only one credential set used for a device, which can be associated from the list of Network or Global credentials. When assigning credentials, both Network and Global credentials are available in the credential window.

When using the **Network Shared Credentials** window, you can select to complete tasks using the option buttons located at the bottom of the window.



These options include **View Associations**, Roll, Add, Edit, Copy, Remove, and Close.

When you select to **View Associations**, you go to the View Associations window for the Name and Account you selected.



From this View Associations window you can see the:

- Network, Device and Device Class information for that account from the **Devices** tab
- Network, Name and Type from the **Auto Discovery** tab.
- Server Name and Server Type from the **External Server** tab.

---

**Note** After reviewing the information contained within each tab, click **Close** to close this window and return to the Network Shared Credential window.

---

## Rolling Credentials

To simplify account and password updates, credentials can be rolled within Network Configuration Manager. Rolling credentials updates all devices associated with one credential to the login and passwords on a second credential. You can roll credential information for devices, as well as create a job to update the devices configurations with the new login and password.

When using the **Network Shared Credentials** window, you can select to complete tasks using the option buttons located at the bottom of the window.

Using **Roll**, you can now:

- Select to roll from one credential to another credential

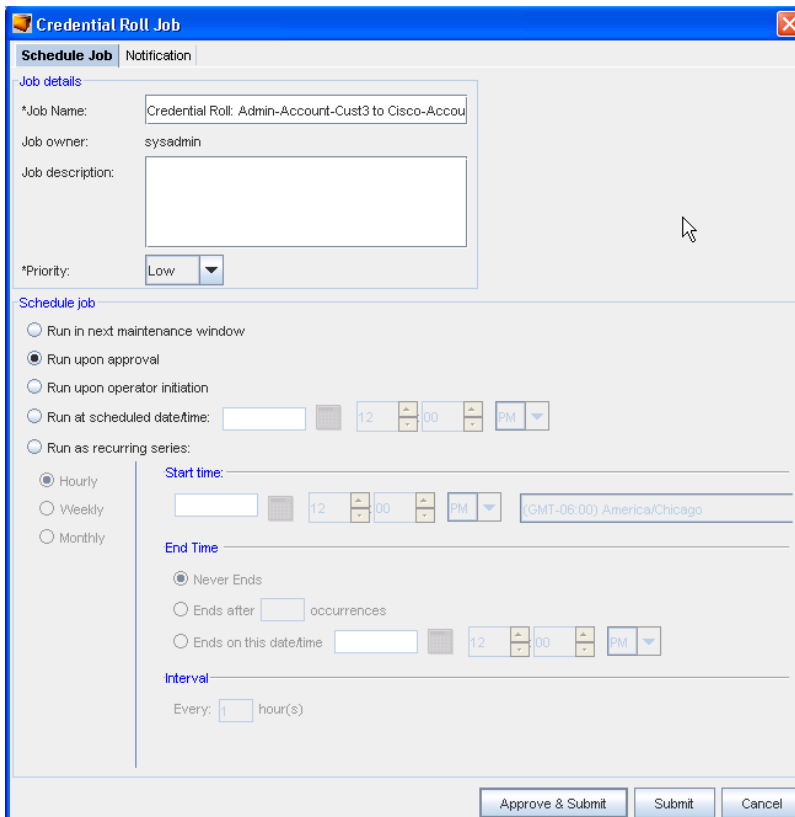
- Manage credentials on devices
- View a history of the credentials and their devices

These options include View Associations, **Roll**, Add, Edit, Remove and Close.

When you select **Roll**, you go to the Roll Candidate Selection, where you can select the Account you want to assign. Using Roll allows you to assign the Account before it is actually scheduled. Once scheduled, the status changes from Assigned to Pending until the scheduled job is run.

You can select to **Roll** from one credential to another credential.

- 1 Click the **Account** name (one or more) in the Roll Candidate Selection window to assign, then click **Ok**.
- 2 At the Credential Roll Job window, make your selections, and complete the information contained within the [Using the Schedule Tab](#) and [Using the Notification Tab to Send an Email](#) tabs. You must also complete and make selections in the **Schedule Job** section.



- 3 Click the appropriate action to **Approve and Submit** or **Submit**.

### Viewing the Credentials Roll Out Log

- 1 In a telnet window, verify your command results by entering change directory ( **cd** ) to **\$VOYENCE\_HOME / logs**, then pressing **Enter**. The log file to review is **credential-rollout.log**.

- 2 You can also go to the System Administrator **Credential** screen in Network Configuration Manager to verify that the credentials on the devices have been changed (rolled).

## Adding Network Shared Credentials

There are five classes of Shared Credentials:

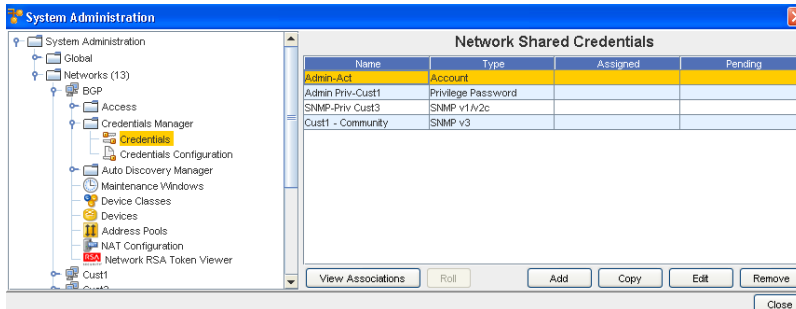
- Account
- Privilege password
- SNMP V1/V2c
- SNMP v3
- RSA

**Note** To import credentials in bulk, see [Using the Command Line Interface](#) for more information.

### Creating Shared Credential - Account Class

To Create a shared credential with the class type of Account, follow these steps:

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Credentials**.



The **Network Shared Credentials** window displays, with a listing of pre-assigned, shared credentials.

At the bottom of the window are the View Associations, Roll, Add, Copy, Edit, and Remove buttons, along with the Close option.

- 3 Click **Add** to display the Add Credential window.
- 4 Enter the **Credential Name** .

- From the **Credential Type** section, select **Account** type from the options shown (using the drop-down arrow to display your selection).

**Important** Depending on the credential type you select, additional information is displayed in the lower portion of the window. For example, when you select Account as the credential type, additional fields display where you enter information. See [Unique Credentials](#) for more

information.

- Complete the following steps:
  - Enter the **User Name** .
  - Enter a **Password**. Confirm the Password.
  - Select the check box if this account is managed by an external authentication server.
- Click **OK** when you have completed these steps.

### Creating Shared Credential - Privilege Password Class

With the **Network Shared Credentials** window displayed showing a listing of pre-assigned, shared credentials:

- Click **Add** to display the Add Credential window.
- Enter the **Credential Name**.
- From the **Credential Type** section, select **Privilege Password** from the options shown (using the drop-down arrow). See [Unique Credentials](#) for more information.

- 4 Enter a **Password**. Confirm the Password you just entered. **Note:** You can also click the **Secure** check box, then click **Generate** to have the application generate a system-only-known password.
- 5 Click **OK** when you have completed these steps.

#### Creating Shared Credential - SNMP v1/v2c

With the **Network Shared Credentials** window displayed showing a listing of pre-assigned, shared credentials:

- 1 Click **Add** to display the Add Credential window.
- 2 Enter the **Credential Name**.
- 3 From the **Credential Type** section, select **SNMP v1/v2c** from the options shown (using the drop-down arrow). See [Unique Credentials](#) for more information.
- 4 Complete the following steps for the **Read-Only** section:
  - Enter the Community String.
  - Confirm the Community String entered.
- 5 Complete the following steps for the **Read-Write** section:
  - Enter the Community String.
  - Confirm the Community String entered.
- 6 Click **OK** when you have completed these steps.



**Add Credential**

\*Credential Name:

Credential Type: **SNMP v1/v2c**

Voyence Unique Credentials    Length:

**Read-Only**

\*Community String:

\*Confirm Community String:

**Read-Write**

Community String:

Confirm Community String:

### Creating Shared Credential - SNMP v3

With the **Network Shared Credentials** window displayed showing a listing of pre-assigned, shared credentials:

- 1 Click **Add** to display the Add Credential window.
- 2 Enter the **Credential Name**.
- 3 From the **Credential Type** section, select **SNMP v3** from the options shown (using the drop-down arrow). See [Unique Credentials](#) for more information.

The screenshot shows the 'Add Credential' dialog box with the following fields and options:

- \*Credential Name: [Text Input]
- Credential Type: **SNMP v3** (Dropdown)
- Voyence Unique Credentials Length: [Text Input]
- Security** Context (Tab)
- \*User Name: [Text Input]
- Security Level: **AUTH\_PRIV** (Dropdown)
- Authentication Protocol: **HMACMD5** (Dropdown)
- Privacy Protocol: **DES** (Dropdown)
- \*Authentication Password: [Text Input]
- \*Reenter Auth. Password: [Text Input]
- \*Privacy Password: [Text Input]
- \*Reenter Privacy Password: [Text Input]
- Generate... (Button)
- OK (Button) Cancel (Button)

When **SNMP v3** is selected as the Credential Type, the information you need to select and enter is divided between two tabs; **Security** and **Context**.

- From the **Security** tab, complete the following steps:
- Enter a User Name
- From the drop-down arrow, select Security Level. Depending on the Security Level you select, Authentication Protocol and Privacy Protocol may not be selectable.
- From the drop-down arrow, select a Authentication Protocol (if appropriate).
- From the drop-down arrow, select a Privacy Protocol (if appropriate).

---

**Note** You can select **AES192W3DESKEYExt** and **AES256W3DESKEYExt** protocols, only for the Cisco specific device(s).

---

- Enter an Authentication Password, then re-enter the password once again.
- Enter a Privacy Password, then re-enter the password once again. Note that you can click Generate to have Voyence create passwords for you.
- Once your passwords are verified, click **Ok**.

The screenshot shows a dialog box titled "Security" with a "Context" tab selected. The dialog contains several input fields and a dropdown menu:

- Context Name: [Text Input]
- Context Engine ID: [Text Input]
- User Group Name: [Text Input]
- View Name: [Text Input]
- View Access: [Dropdown Menu] (Currently set to WRITE)
- Included MIBs/OIDs: [Text Input]
- Excluded MIBs/OIDs: [Text Input]

At the bottom of the dialog, there is a "Generate..." button. Below the dialog box, there are "OK" and "Cancel" buttons.

---

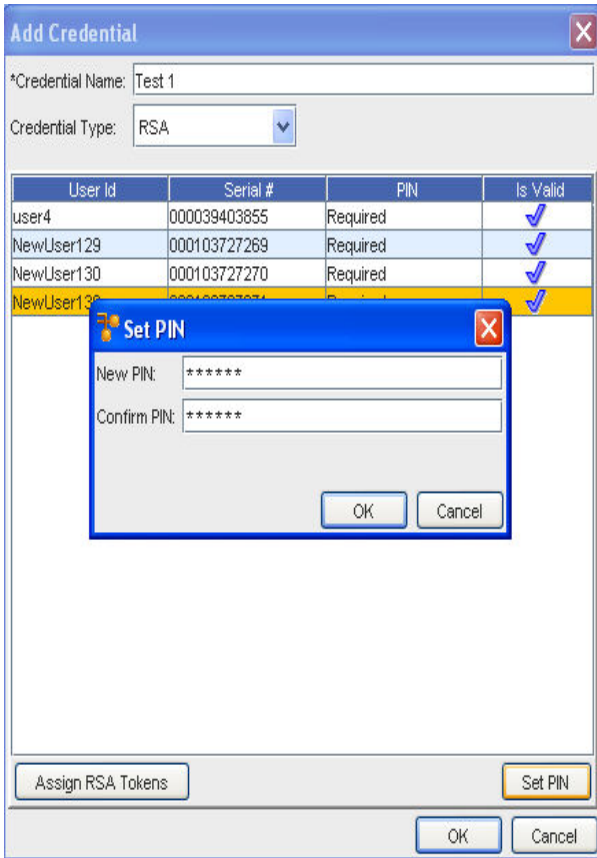
**Note** MIBs refer to **Management Information Bases** , and OIDs refer to **Object Identifiers** .

---

- From the **Context** tab, complete the following steps:
- Enter the Context Name.
- Enter the Context Engine ID.
- Enter a User Group Name.
- Enter a View Name.
- Select a View Access from the drop-down arrow.
- Enter the MIBs/OIDs you want included.
- Enter the MIBs/OIDs you want to be excluded from these credentials.
- Click **Ok** to keep your selections.

### Setting RSA Token PINs

- 1 From the list of RSA tokens, select an **RSA token**. RSA tokens that have not had the PIN set, show as Required under the PIN column.
- 2 At the bottom of the Manage RSA Tokens pane, select **Set PIN** . The Set PIN window (for the user you selected) now opens.



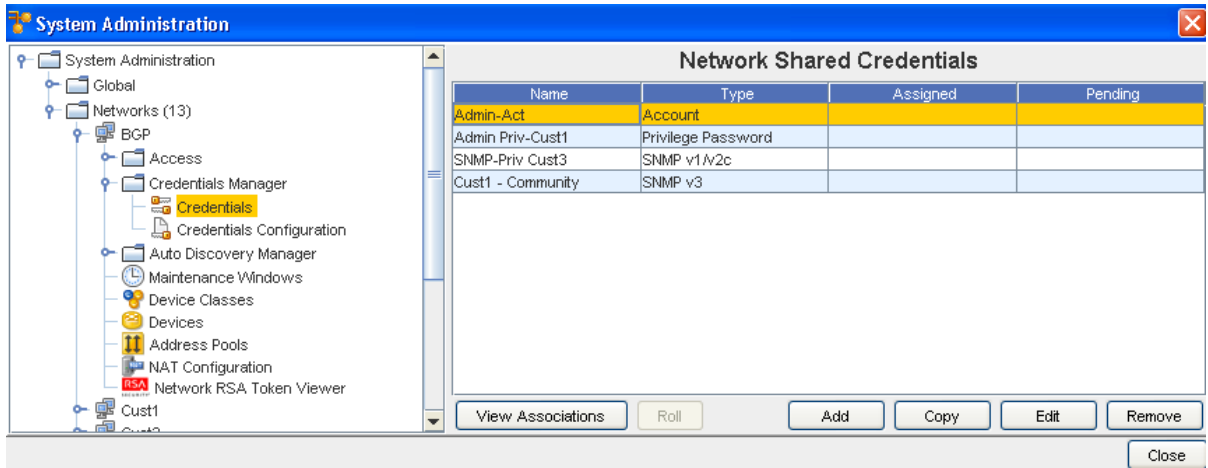
- 3 At the Set PIN screen, enter a **valid PIN** in the New PIN field.
- 4 Enter the PIN again in the **Confirm PIN** field.
- 5 Click **Ok**.

## Copying Network Shared Credentials

### Creating Shared Credential - Account Class

To Copy a shared credential with the class type of Account, follow these steps:

- 1 From the menu bar, select **Tools -> System Administration**.



The **Network** Shared Credentials window displays, with a listing of pre-assigned, shared credentials.

At the bottom of the window are the View Associations, Roll, Add, Copy, Edit, and Remove buttons, along with the Close option.

- 2 Click **Copy** to display the Copy Credential window.
- 3 Enter the **Credential Name** .
- 4 Click **Ok**. Now, the copy of the Credential you selected is now in the list of Network Shared Credentials.

**Copy Shared Credential**

\*Credential Name:

Credential Type:

Voyage Unique Credentials Length:

**Read-Only**

\*Community String:

\*Confirm Community String:

**Read-Write**

Community String:

Confirm Community String:

## Editing Network Credentials

To edit Network Shared Credentials,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Credentials**.

**System Administration**

**Network Shared Credentials**

Name	Type	Assigned	Pending
Admin-Act	Account		
Admin-Priv-Cust1	Privilege Password		
SNMP-Priv-Cust3	SNMP v1/v2c		
Cust1 - Community	SNMP v3		

The **Network Shared Credentials** window displays, with a listing of pre-assigned, shared credentials.

- 3 Select a credential from the list, then click **Edit** to display the Edit Shared Credential window.
- 4 Make any changes to the existing information, based on the Credential Type you selected when you created the credential.
- 5 Click **OK** to save your edits.

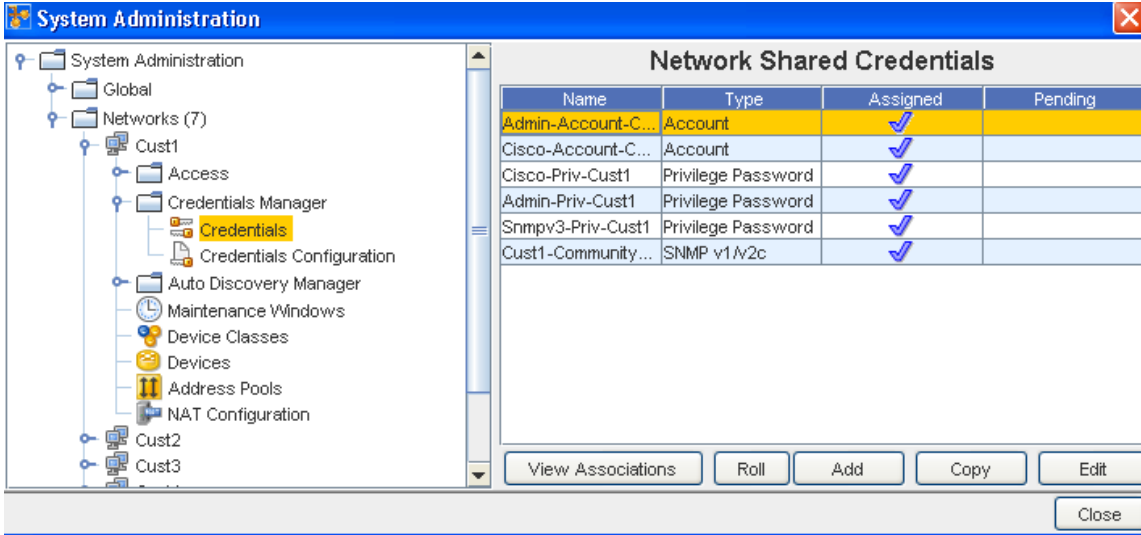
#### Notes:

- The updating credentials process requires that an account be associated with a device. This account is used to establish the initial session into the device to make the credential updates.
- This manual process creates an association with the credential and the local device to represent the username/password that is present on the device.
- If an Autodiscovery is made with an established account credential, the manual process of association is not required. The Communication tab on a device contains the account association for the Primary In-Band mechanism.

## Removing Network Credentials

To remove Network Shared Credentials,

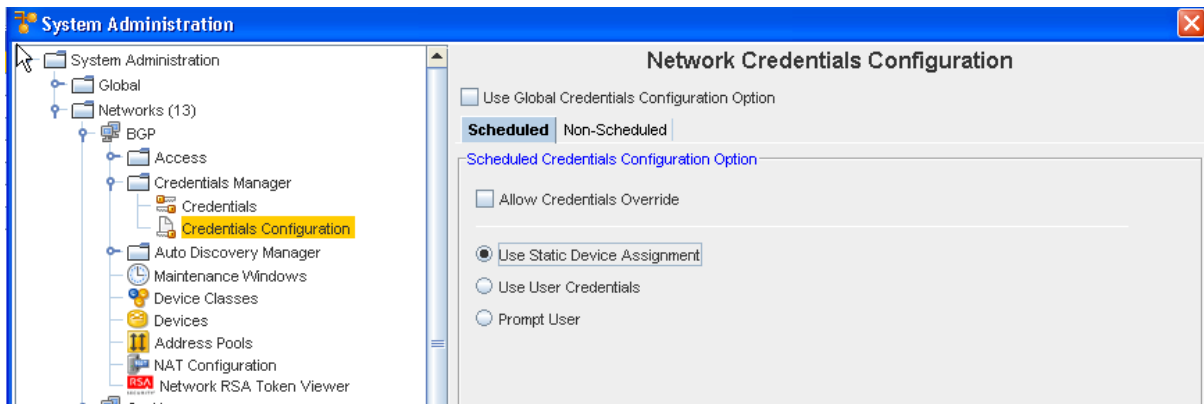
- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Credentials**. The **Network Shared Credentials** window displays, with a listing of pre-assigned, shared credentials.



- 3 Select the network credential you want to remove from the list.
- 4 Next, click **Remove**.
- 5 At the confirmation message, click **Yes** to remove this network shared credential.

## Using Network Credentials Configuration

Access to the Credentials Configuration is through the **Credentials Manager** .





## At the Network Credentials Configuration Level

At this level, you are provided the options to determine the credentials that need to be used for communication with the device. This includes scheduled jobs, as well as synchronous operations targeted on a device, such as cut-through, quick commands, and more.

- The **Scheduled** tab refers to the jobs that can be scheduled to run (with the exception of Auto Discovery and Pulls).
- The **Non-Scheduled** tab refers to those operations (Cut-Through, Quick Commands, and Save Commands, for example) that are not scheduled.

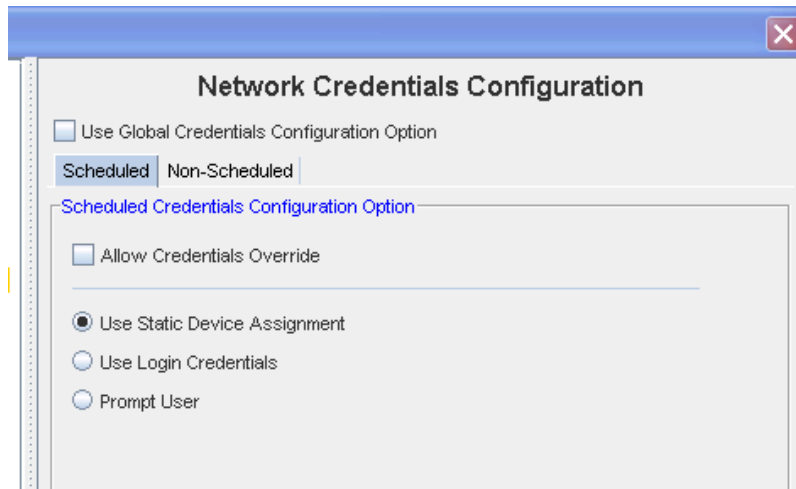
When the **Use Global Credentials Configuration Option** is not selected, your options can be selected from the Scheduled and Non Scheduled tabs. If selected, there are no other options available to you from these tabs.

You can select from the following options:

### The Scheduled Tab

#### Users Static Device Assignment

- **Uses Static Device Assignment** - If Uses Static Device Assignment is selected- this indicates to the system to use the Shared Credentials assigned at the device level within a network. This is the default option.

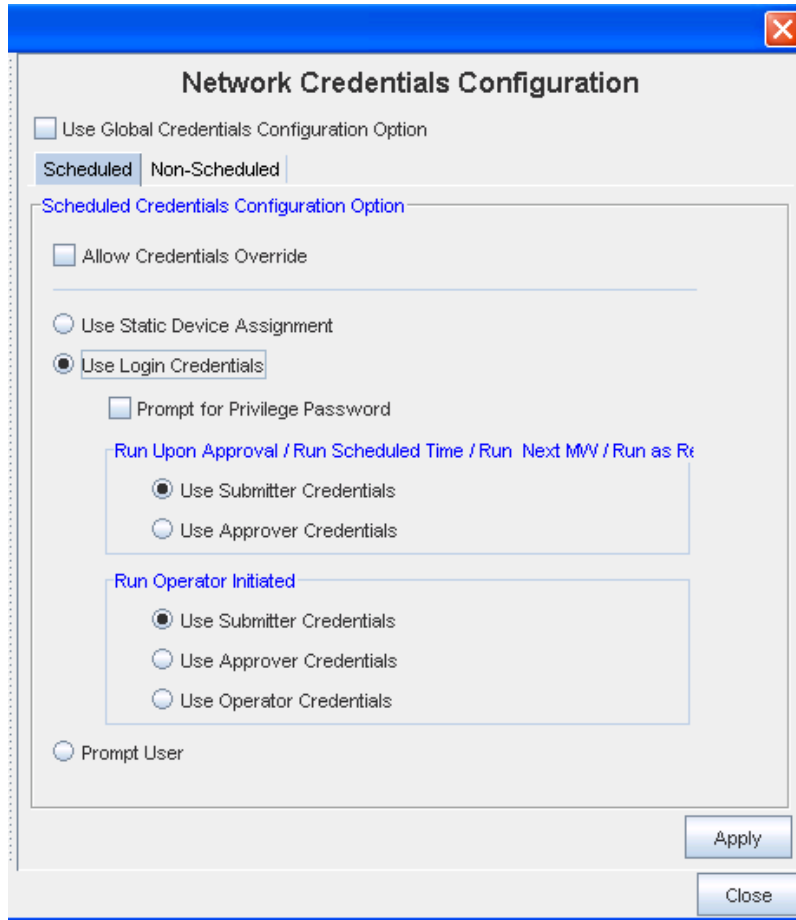


#### Use Login Credentials

- **Use Login Credentials** - When **Use Login Credentials** is selected - this indicates to the system to use the user's application login account as the device credentials (the account name/account password).

You have the choice to select any of the options of when the user's are now prompted to enter account and password information before completing tasks.

- You can select to **Use the Global Credentials Configuration Option**
- You can also select to **Allow Credentials Override**



**Important** In some cases where a job may be scheduled in the future, the user's login credentials may need to be preserved until the job executes (to construct the device server request). These credentials must be discarded immediately after the task request is sent to the device server. You must pay attention to jobs with "Preserve Order" selected, as each task execution depends on the success of the previous task in the list (the credentials must be preserved until the last task executes).

- You can select to **Prompt for Privilege Password**

To determine whose credentials are to be used for jobs, the following options are available for each run option as applicable, **one** of which must be selected:

- **Use Submitter Credentials** – In case of scheduled operations, the system uses the submitter's credentials. This includes any job submission through "Submit" button on the scheduler.
- **Use Approver Credentials** – In case of jobs, the system uses the approver's credentials. This includes any job submission through –Approve&Submit– button on the scheduler or the "Approve" icon on the Schedule Manager.
- **Use Operator Credentials** (in case of jobs whose run option is "Run Operator Initiated") – In case of jobs, the system uses the credentials of the user attempting to manually execute the job.

In case of non-scheduled operations, the login credentials of the user executing the operation will be used and above options are redundant.

If Prompt User is selected from this window , see the following information.

### Prompt User

- **Prompts User** - When Prompts User is selected - this indicates to the system that the user is to be prompted for the credentials before the device operation , based on the following options: Account Password, and Privilege Password.

To determine whose prompts are to be used for jobs, the following options are available for each run option as applicable, **one** of which must be selected:

- Run on Approval
- Prompts on Submit - Prompts at the time the job is submitted for "Pending Approval"
- Prompts on Approval - Prompts at the time the job is Approved
- Run Operator Initiated
- Prompts on Submit - Prompts at the time the job is submitted for "Pending Approval"

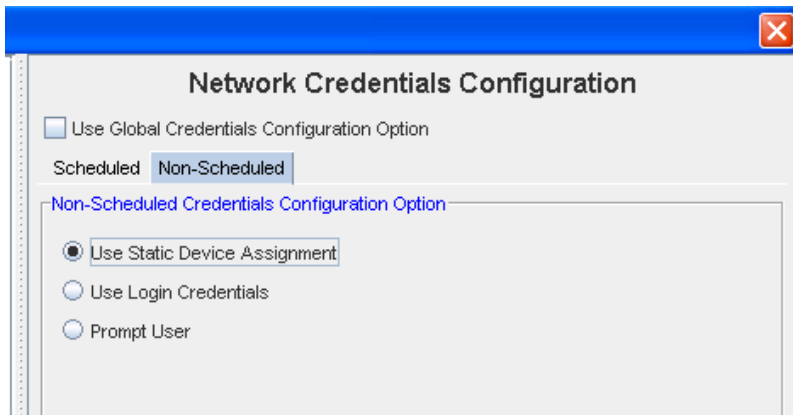
- Prompts on Approve - Prompts at the time the job is Approved
- Prompts on Manual Execute - Prompts at the time the job is manually executed.
- Run Scheduled Time / Run Next MW / Run as Recurring Series
- Prompts on Submit - Prompts at the time the job is submitted for "Pending Approval"
- Prompts on Approval - Prompts at the time the job is Approved

**Note** You also have the option of selecting **Invalidate Credentials on Job Modification** . If this is selected, after a job is **edited**, any credential associated with that job is now invalid.

- 1 After making your selections from the various options, click **Apply** to apply your credential choices.
- 2 Read the system message carefully to fully understand your selection to apply the changes you have made, then select **Yes to Continue**.
- 3 If applicable, click **Yes** at the Confirmation message.

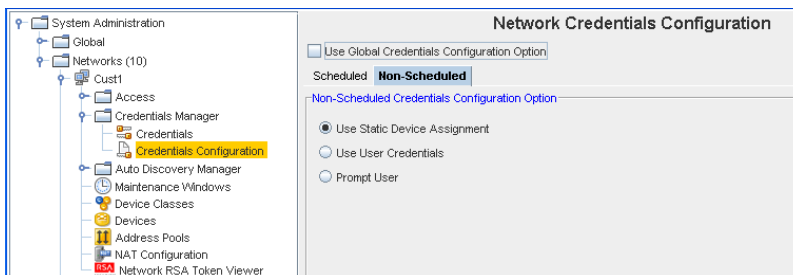
### The Non-Scheduled Tab

The **Non-Scheduled** tab refers to those operations (Cut-Through, Quick Commands, and Save Commands, for example) that are not scheduled to run.



### Users Static Device Assignment

- **Uses Static Device Assignment** - If Uses Static Device Assignment is selected- this indicates to the system to use the Network Shared Credentials assigned at the device level within a network. This is the default option.

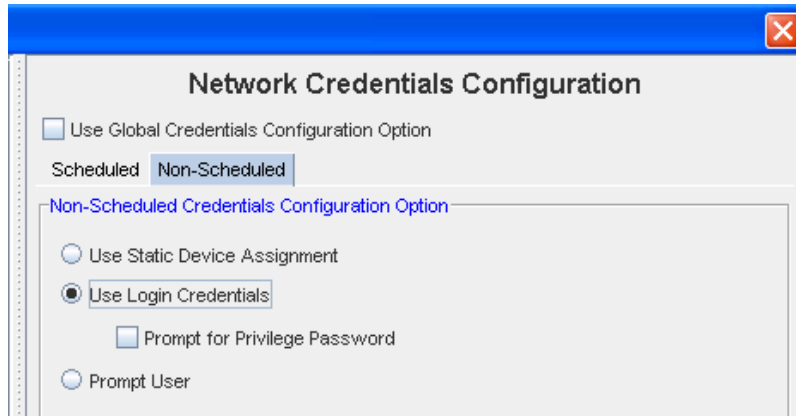


## Use Login Credentials

- **Use Login Credentials** - When **Use Login Credentials** is selected - this indicates to the system to use the user's application login account as the device credentials (the account name/account password).

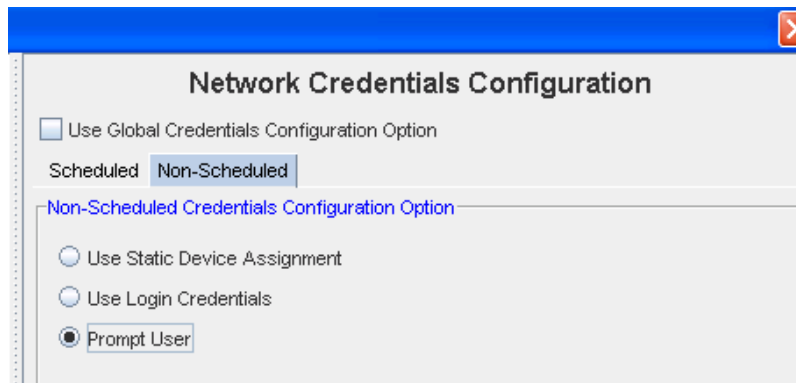
You can select to have the user prompted for their **Privilege Password** information before completing tasks.

- You can also select **Prompt User** from this window.



## Prompt User

**Prompt User** - When **Prompt User** is selected - this indicates to the system that the user is to be prompted for the credentials before the device operation, based on the following options: Account Password, and Privilege Password.



## Auto Discovery

### Auto Discovery Overview

Network Configuration Manager has a robust Auto-Discovery capability which can find the devices on a network, categorize them, and determine the communication methods available for management of the devices.

Before your network devices can be managed in Network Configuration Manager they must first be discovered. The process by which devices are entered into the application for management is known as **Auto Discovery**. Auto Discovery associates network devices with a Network Configuration Manager device server and your networks.

- Auto Discovery jobs can be created and scheduled by System and Network Administrators, and are associated with individual networks.
- Jobs are maintained under the **Network** folder in the System Administration module. Each network has its own Auto Discovery module.
- If you have more than one network configured in Network Configuration Manager, Auto Discovery should be scheduled for each network.
- Auto Discovery can be set to run on a scheduled cycle, eliminating the need to "remember" to run Auto Discovery.
- Auto Discovery uses the Schedule Manager to push scheduled Auto Discovery jobs to the networks. Scheduling allows Auto Discovery to run at the best time, based on your network's requirements.
- Only devices in the *IP range* of an Auto Discovery job are attempted to be discovered. When a device is discovered, Network Configuration Manager identifies its device type, based on the supported device types within the system.
- If the device is **not** one of the types listed as significant in the Auto-Managed devices window, the device is ignored.
- Only devices with IPs in the include range of an Auto Discovery job that are of a device type listed in Auto-Managed Devices, will be managed into the network.

---

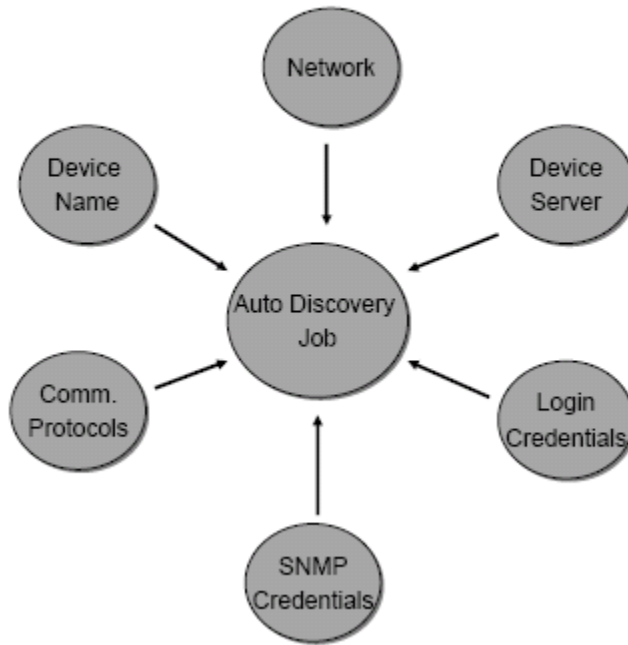
**Important** Auto discovery jobs cannot be created until at least *one device server* is associated with the network

---

### Auto Discovery Associations

The following graphic displays the associations with Auto Discovery

## Networks – Auto Discovery Associations



### Detecting Duplicates

Voyence uses a **"2 out of 3 rule"** to determine if a discovered device is new. The three items tested are:

- SysObjectID
- IP address
- Name or Serial Number

Depending on the device class of the device the "name" is the HostName, SysName, or serial number of the device.

The device server compares the found "Name" with its internal database of managed devices. If there are no matches, the device server compares the discovered IP address with the list of IP addresses in its internal database.

---

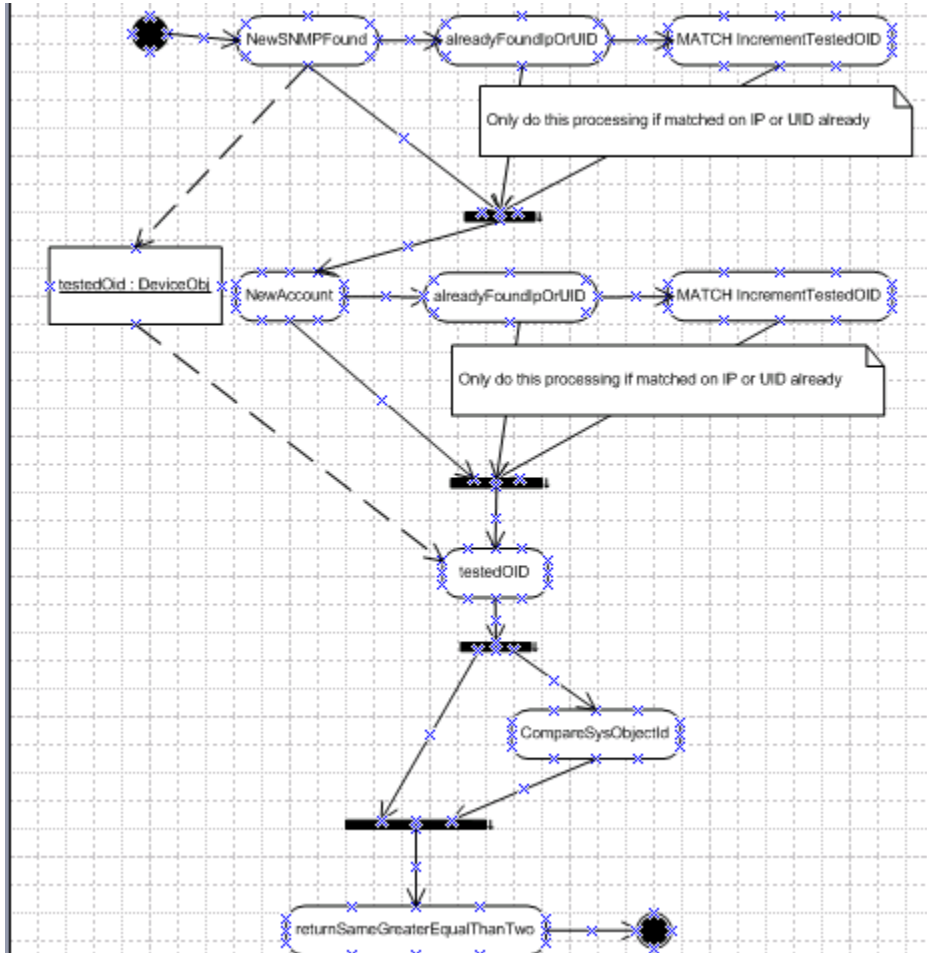
**Note** The internal database on the device server includes all the IP addresses for the devices it is managing, not just the management addresses. This ensures that a device is not just discovered via another interface.

---

If either the device name or the IP address is matched to a device in the internal database, the system compares the discovered SysObjectID with the SysObjectID of the matched device.

If these are a match, it is assumed that the discovered device is a duplicate, and it is assigned the matched device's IDX. If the SysObjectID's do not match, but both the device name AND IP addresses match, the device is assumed to be a duplicate, and is assigned the matching devices IDX.

If none of the three (or only one of the three) items match an existing device, the device is assumed to be a new device, and the device server assigns a new IDX number to the device.



### Auto Discovery Job Types

There are **three types** of auto discovery jobs that can be run on a network:

- Ping Sweep
- SNMP Sweep




- Multi-hop Discover
- **Ping-Sweep** – Takes a range of IPs. Pings each device twice to see if the device is active, then runs an SNMP-Sweep on each of the responding devices.
- **SNMP-Sweep** – Takes a range of IPs. (Note that SNMP's are not needed to discover Cisco devices.) This SNMP Sweep discovery type takes a range of IPs and attempts to discover each device IP. It uses an SNMP query first. If the SNMP string is incorrect, or the device just does not respond, it also attempts to login to the device, and try to discover it with account information.
- **Multi-hop Discover** – Takes the IP of a core seed router and a range. Pulls route and arp table information from the seed router, takes each IP in this list, and repeats the process until it exhausts the list of unique IPs in the range. A heavy load can be seen on routers in large networks, so this discovery type should not be used except as last resort in environments where users have no of what exists in their network.

Depending on the type of auto Discovery completed, details must be entered defining the Auto Discovery job. These details are located on four tabs.

- Properties
- Seed Addresses
- Ranges
- Credentials

---

**Note**  Do not use SNMP v3 Credentials for Auto Discovery if you have PIXes.

The Seed Addresses tab is only available when running a Multi-hop discovery.

---

Once devices are located, they are placed into the Auto Discovered network as managed devices, and system jobs are run in the scheduler to pull the configurations and hardware specs for the new devices.

Although devices enter a network as managed, they can be reclassified. The three device classifications available in Network Configuration Manager are:

<b>Managed</b>	Indicates devices that are associated with networks. Managed devices reside in the central repository, and are under the control of authorized network users.
<b>Unmanaged</b>	Indicates devices that have been discovered, but are not managed by a network and flagged, so that they are not rediscovered in subsequent Auto Discovery runs. All revision history about a device is lost when it is placed into an <i>unmanaged</i> state.
<b>Unclassified</b>	When a device is removed from all networks, it's state is changed to Unclassified. Unclassified devices cannot be managed until placed back into a network. The device retains all revision history while in an unclassified state.

---

## Creating Auto Discovery Jobs

Devices are associated with a Network through the Auto Discovery process. The Network Configuration Manager Auto Discovery mechanism offers three Auto Discovery options; Multi-Hop, Ping Sweep, and SNMP Sweep. Depending on the type of Auto Discovery selected, details must be entered into the four tabs.

Creating an Auto Discovery job is a multi-step process. Depending on the Auto Discovery type, you must provide details on the following tabs:

- Properties
- Seed Addresses
- Ranges
- Credentials (Common Strings, Accounts, and Privilege Passwords)

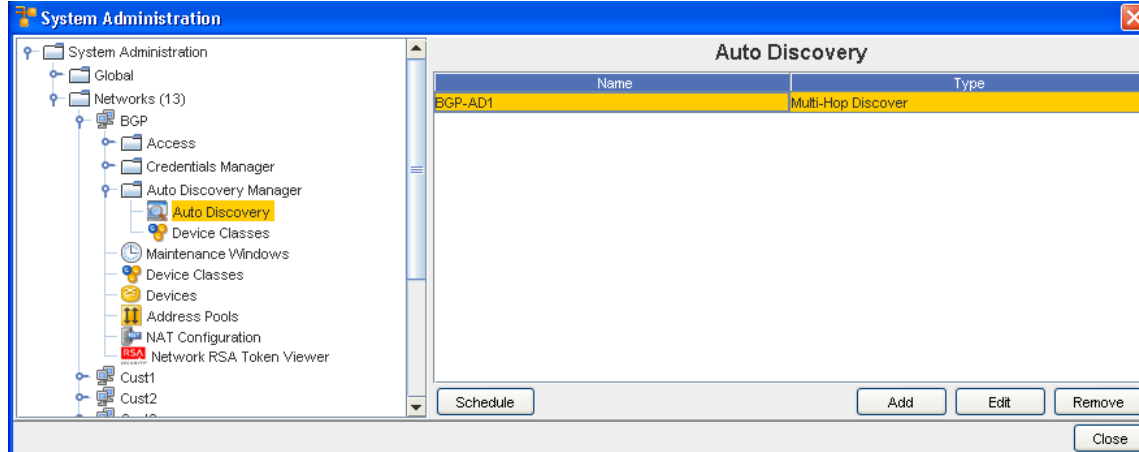
---

**Important** If insufficient details are entered on any tab, the Auto Discovery job may fail, or the job may not run completely.

---

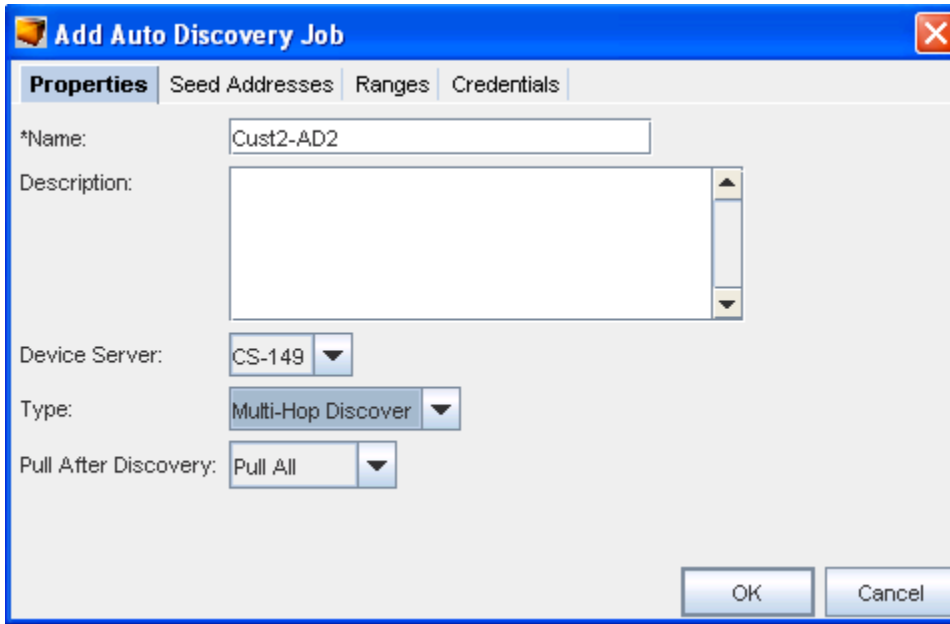
To create an Auto Discovery job,

- 1 From the menu bar, select **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Networks folder**.
- 3 Click **Auto Discovery**.



- The right pane populates with any Auto Discovery jobs that have already been setup.
- The Schedule, Add, Edit, and Remove buttons are all selectable in the window (when a device is selected, Prior to select the Add button is the only button selectable).
- Click **Add**. The Add Auto Discovery Job window opens.
- To define the Auto Discovery job, you must enter details in each of the following tabs:
  - Properties
  - Seed Addresses

- Ranges
- Credentials



Properties Tab

Seed Addresses Tab

Ranges Tab

Credentials Tab

Editing Auto Discovery Jobs

Removing Auto Discovery Jobs

### Properties Tab

The **Properties** tab in Auto Discovery is the first tab you must complete. The Properties tab contains the basic description and type of Auto Discovery being run. You can also select the Pull After Discovery action.

The following fields are available.

The screenshot shows a dialog box titled "Add Auto Discovery Job" with a close button (X) in the top right corner. The dialog has four tabs: "Properties", "Seed Addresses", "Ranges", and "Credentials". The "Properties" tab is selected and contains the following fields:

- \*Name: A text box containing "Cust2-AD2".
- Description: A large text area that is currently empty.
- Device Server: A drop-down menu showing "CS-149".
- Type: A drop-down menu showing "Multi-Hop Discover".
- Pull After Discovery: A drop-down menu showing "Pull All".

At the bottom right of the dialog are "OK" and "Cancel" buttons.

Field	Description
Name	This field populates with an auto-generated name that can be edited.
Description	Descriptive summary of the Auto Discovery
Device Server	Contains the name of the Device Server
Type	Options include: Ping Sweep, SNMP Sweep, Multi-Hop Discover.
Pull After Discovery	Options include: Do not Pull, Pull Configs, and Pull All.

- 1 Type in a **Name** for the Auto Discovery job.
- 2 Optionally, enter a **Description**.
- 3 Select a **Device Server** from the drop-down listing.
- 4 Select a **Type** from the drop-down listing.
- 5 Make a selection from the **Pull After Discovery** drop-down listing.
- 6 Proceed to the next tab, **Seed Addresses**, or **Ranges**.

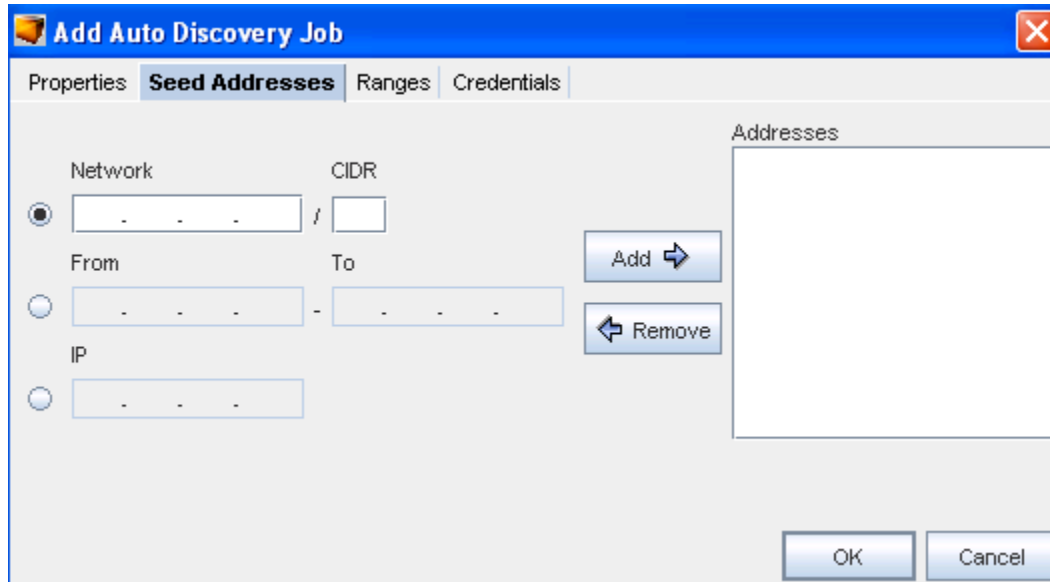
---

**Important** You can only continue on to the Seed Addresses if **Multi-hop** is selected in **Properties**. For all other selections, you do not have access to the Seed Addresses tab.

---

### Seed Addresses Tab

The **Seed Addresses** tab is only available when a **Multi-Hop Discover** job type is being completed. Seed Addresses are primer addresses to Network devices to be managed.



Seed addresses are portals to network devices that can be managed. This tab allows you to modify the seed addresses that are used during Auto Discovery.

The following fields are available:

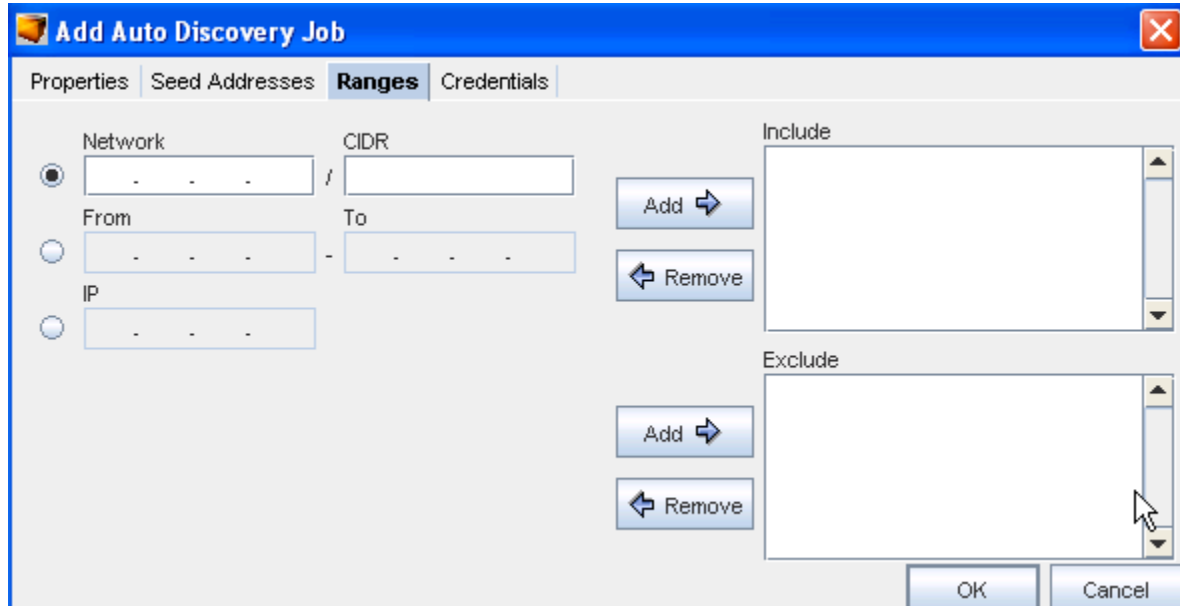
Field	Description
Network/CIDR	A single network subnet -default selection
From/To	Allows you to enter a span of addresses. You can then Add or Remove the content within the Addresses box.
IP	A single IP Address
Addresses	Contains all Seed Address types that have been entered. This list can be modified as needed, using the Add and Remove buttons.

- Complete **one or more** of the following:
- Enter a **Network/CIDR**. Note that, the CIDR number must be less than or equal to 32.
- Enter a **From/To IP address range**.
- **E nter a single IP Address**.
- Click **Add**. The addresses are now included in the Addresses box.
- Repeat the above steps until all the Seed Addresses are entered. Note that you can remove any exiting addresses using the **Remove** button, if needed.
- Proceed to the next tab. See **Ranges**.

### Ranges Tab

The **Ranges** tab allows you to enter ranges of IP addresses that are to **included** or **excluded** during Auto Discovery. IP addresses not included are ignored during Auto Discovery. IP Addresses located in the Excluded field are addresses within the included IP address ranges that should be ignored during Auto Discovery.

The Included and Excluded ranges can be modified as needed.



The following fields are available:

Field	Description
Network/CIDR	A single network subnet. Default selection
From/To	Allows you to enter a span of addresses
IP	A single IP address
Include	To include the first of IP Ranges that are included during the Auto Discovery
Exclude	To exclude the first of IP Ranges that are excluded during the Auto Discovery

To Include ranges,

- 1 Complete one or more of the following:
  - Enter a **Network/CIDR**
  - Enter a **From/To IP address range**
  - Enter a single **IP address**
- 2 Click **Add ->** in the **Include** section. The address are added to the Addresses column.
- 3 Repeat **steps 1 and 2** until all IP addresses needing to be included are added.

- 4 To remove included IP Addresses in the Include field, select the **IP Address**, then click **Remove**.

**Result:** The address is removed from the Include column. If the address need to be included in the future, it must be re-entered.

To Exclude ranges,

- 1 Complete one or more of the following:
  - Enter a Network/CIDR.
  - Enter a From/To IP address range.
  - Enter a single IP address .
- 2 Click **Add** -> in the Exclude section. The address are added to the Addresses column.
- 3 Repeat **steps 1 and 2** until all IP addresses that need to be excluded are added.
- 4 To remove excluded IP Addresses in the Exclude field, select the **IP Address**.
- 5 Click **Exclude**. The address is removed from the Exclude column.
- 6 Click **OK** when you have completed excluding ranges.
- 7 **Proceed to the next tab.**

[Auto Discovery Overview.](#)

[Seed Addresses Tab.](#)

## Credentials Tab

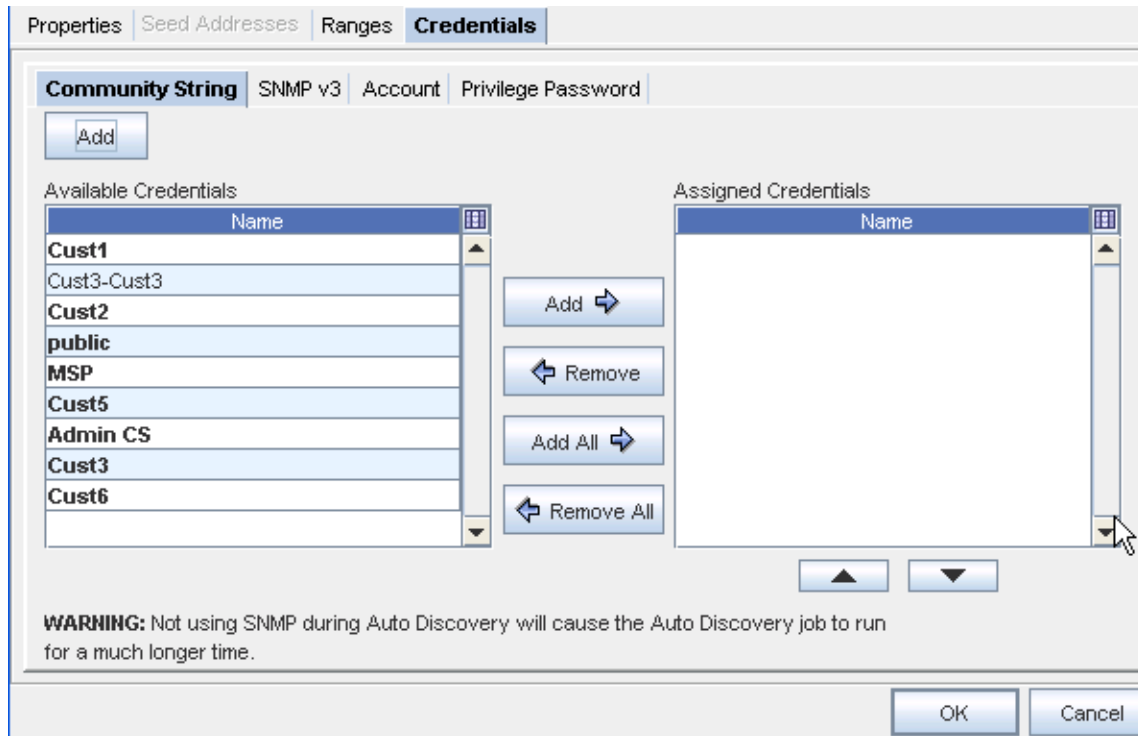
**Global credentials** appear in bold. Network credentials are plain text.

Auto Discovery uses your device class preferences to determine how to discover devices into your Network. Bulk Import utilities can also be used to trigger Auto Discovery or populate the device database.

Network Configuration Manager supports the use of standard R/O and RW Community strings, or the use of SNMPv3 credentials. SNMP strings are typically used for initial device discovery, and for pulling hardware information from the device MIB.


The Credentials tab contains four separate tabs.

- Community String
- SNMP v3
- Account
- Privilege Passwords



To work with the Community String window (in the Credentials tab),

- 1 From the **Available** Credentials listing, select a Credential, then click the **Add** button to move that credential into the Assigned Credentials list. You can also use the Add All arrow if needed.

 If you have added more than one credential into the Assigned column, you can use the up and down arrows to change the order of the list.

- 2 Click **Ok** to preserve the credentials within the list, and the order of the list.

To Add a Credential,

- 1 To add a new credential, click **Add**.
- 2 The **Add Credential** window displays.
- 3 Enter a **Credential Name**.



- 4 If this is a Voyence Unique Credential, select the **check box** , and then enter the exact length of the unique credential.

---

**Note**

- Community Strings are authorized credentials used by SNMP to communicate with devices.
- Multiple Read-Only (RO) or Read-Write (RW) Community Strings can be added to support network environments requiring unique Community Strings for different devices or device types. The sequence of each type of Community String can be adjusted using the up and down arrows.
- During Auto Discovery, when SNMP is enabled, each RO and RW Community String is tried until matches are found. The following fields are available:

---

**Add Credential**

\*Credential Name:

Credential Type: Account

Voyence Unique Credentials Length:

User Name:

Password:

Confirm Password:

This account is managed by an external authentication server.

Generate...

OK Cancel

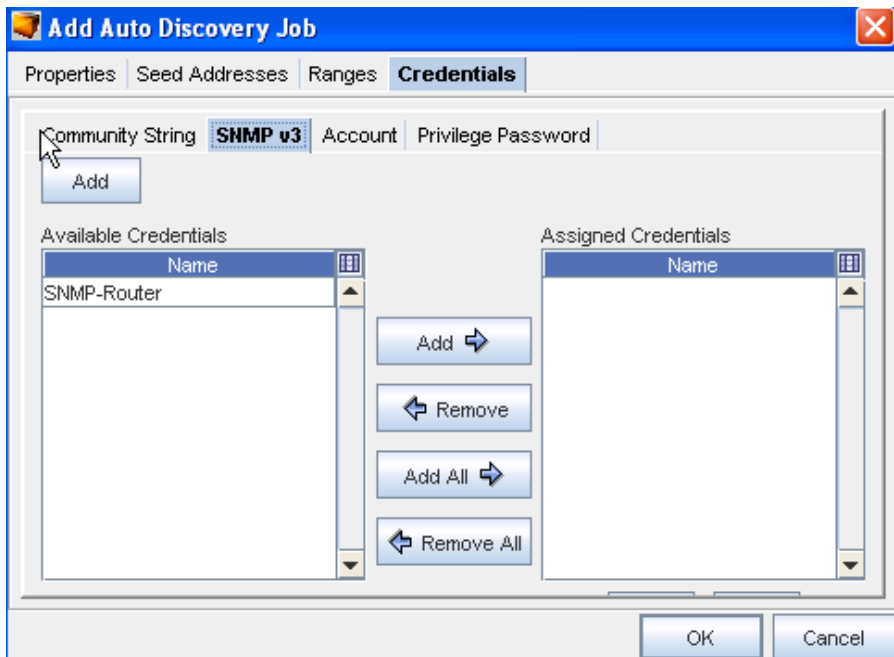
- 5 Enter the information needed for that window, and click **Ok** when you are finished.

Field	Description
Community String	Text field for entering community strings
Read-Write	Read-Writer community string list, which when discovered, can be updated with configs
Read-Only	Read-Only community strings list, which when discovered, cannot be written to or can a config be pulled from it

**Generate button** : Use the Generate button to have the system automatically generate Read Only and Read Write strings.

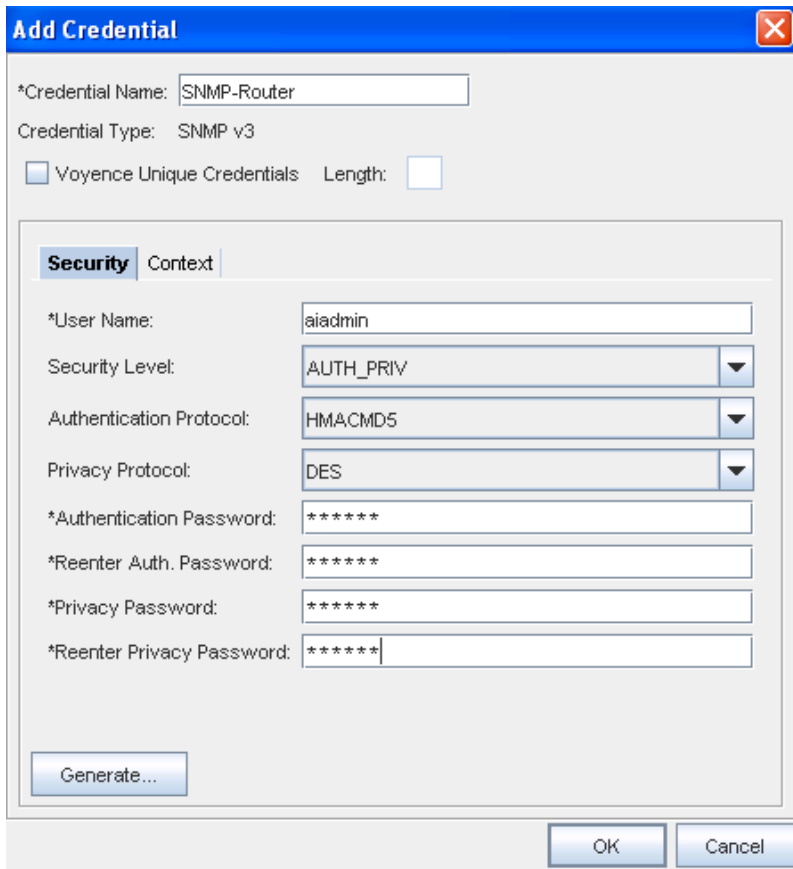
To work with the SNMP v3 window,

- 1 From the Available Credentials listing, select a Credential, then click the Add button to move that credential into the Assigned Credentials list. You can also use the Add All arrow if needed.



**i** If you have added more than one credential into the Assigned column, you can use the up and down arrows to change the order of the list.

- 2 To add a credential, click the **Add** button on the Add Auto Discovery Job windows (just above the Available Credentials pane).

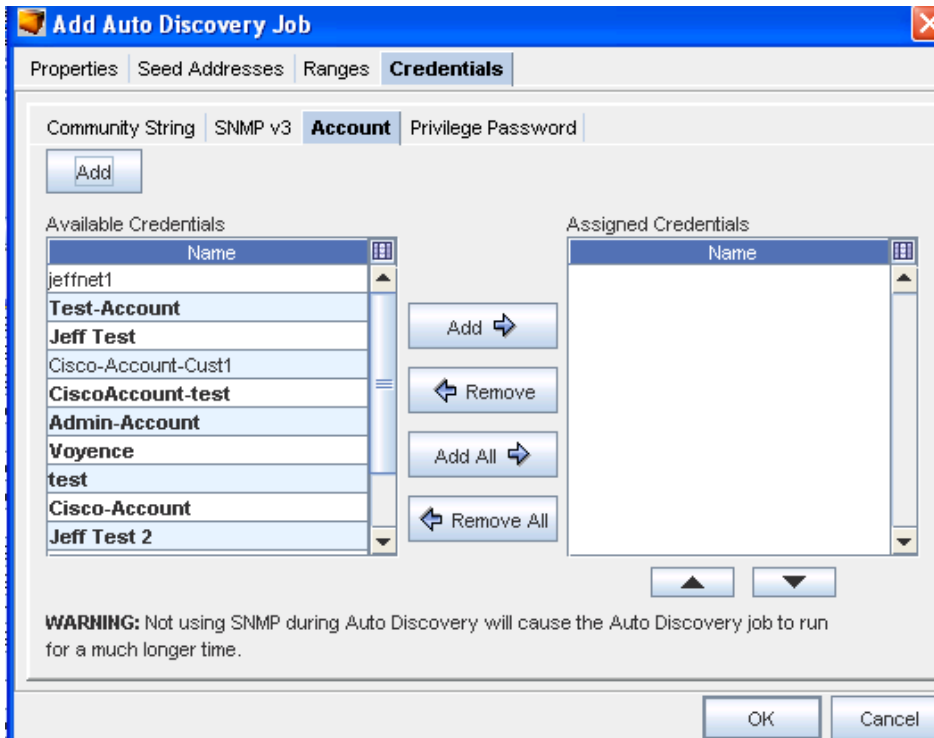


3 The **Add Credential** window displays.

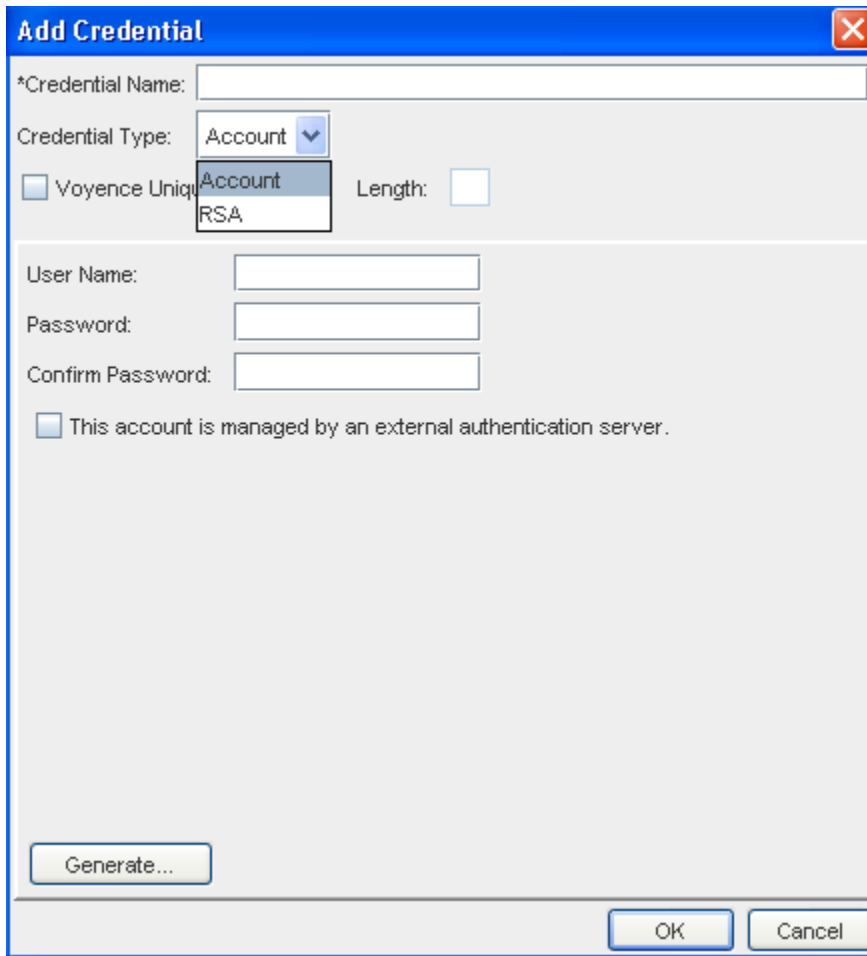
4 Enter the information needed for that window, and click Ok when you are finished.

To work with the Account window,

- 1 From the Available Credentials listing, select a Credential, then click the **Add** button to move that credential into the Assigned Credentials list. You can also use the **Add All** arrow if needed.



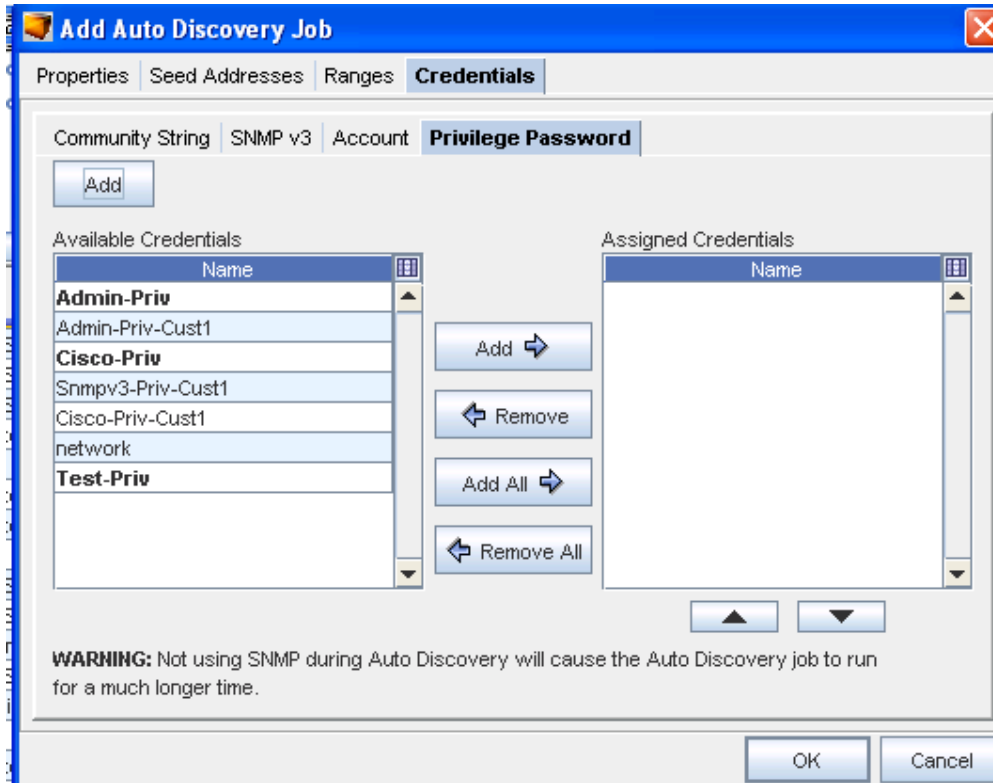
- 2 Click **Ok** to preserve the credentials within the list, and the order of the list.



- 3 To add a new credential, click **Add**.
- 4 The **Add Credential** window displays.
- 5 Enter the information needed for that window, and click **Ok** when you are finished.

To work with the Privilege Password tab,

- 1 From the **Available Credentials** listing, select a Credential, then click the **Add** button to move that credential into the **Assigned Credentials** list. You can also use the Select All arrow if needed.



- 2 To Add a new Credential, click **Add**.
- 3 The **Add Credential** window displays.
- 4 Enter the information needed for that window, and click **Ok** when you are finished.

**Add Credential**

\*Credential Name:

Credential Type:  ▾

Voyence Unique

\*Password:

\*Confirm Password:

Secure

[Properties Tab](#)

[Seed Addresses Tab](#)

[Ranges Tab](#)

[Editing Auto Discovery Jobs](#)

[Removing Auto Discovery Jobs](#)

[RSA](#)

[SNMP Enabled/Disabled](#)

[SNMP Enabled](#)

If SNMP is **enabled**, and SNMP credentials are supplied, the device server attempts to determine which SNMP credentials are valid for the device. The device server starts with SNMPv1, then SNMPv2c, and finally SNMPv3. This order is used for performance reasons. Once a valid SNMP credential is found, the device is queried for its SysObjectID. This allows the device server to know which device driver to use for the remainder of the process.

---

**Note** While the discovery process starts with SNMPv1, the order of assignment is actually reversed. For instance, if all three SNMP versions are valid for the discovered device, the SNMPv3 mechanism is set as the active version .

---

Depending on the settings for the discovered device class, the device server now attempts to determine credentials for SSH, Telnet, FTP, and/or SCP. The management mechanism is set for the device based on the discovered credentials and the ordering options set in the application.

### SNMP Disabled

If SNMP is **disabled**, the device server attempts first to SSH, and failing that, Telnet to each device and determine the proper login credentials. Once the proper credentials are determined, the device server traverses through the device drivers to determine what the device class is for the connected device.

This is attempted based on the order contained in the addev.order file on the device server. Once a device class is determined, the appropriate commands are sent to the device to determine it's model information, which is then cross referenced with Voyence's database to determine the SysObjectID for the device.

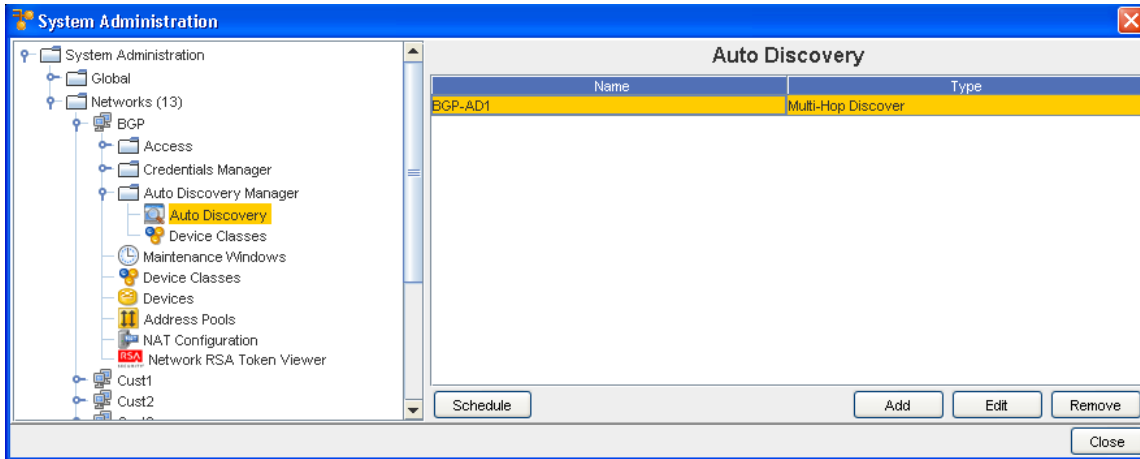
Depending on the settings for the discovered device class, the device server now attempts to determine if FTP and/or SCP are enabled. The management mechanism is set for the device, based on the discovered credentials and the ordering options set in the application.

### Assigning Privilege Passwords

You can also assign Privilege Passwords during an Auto Discovery job.

- 1 Select **Add** from the Auto Discovery window.

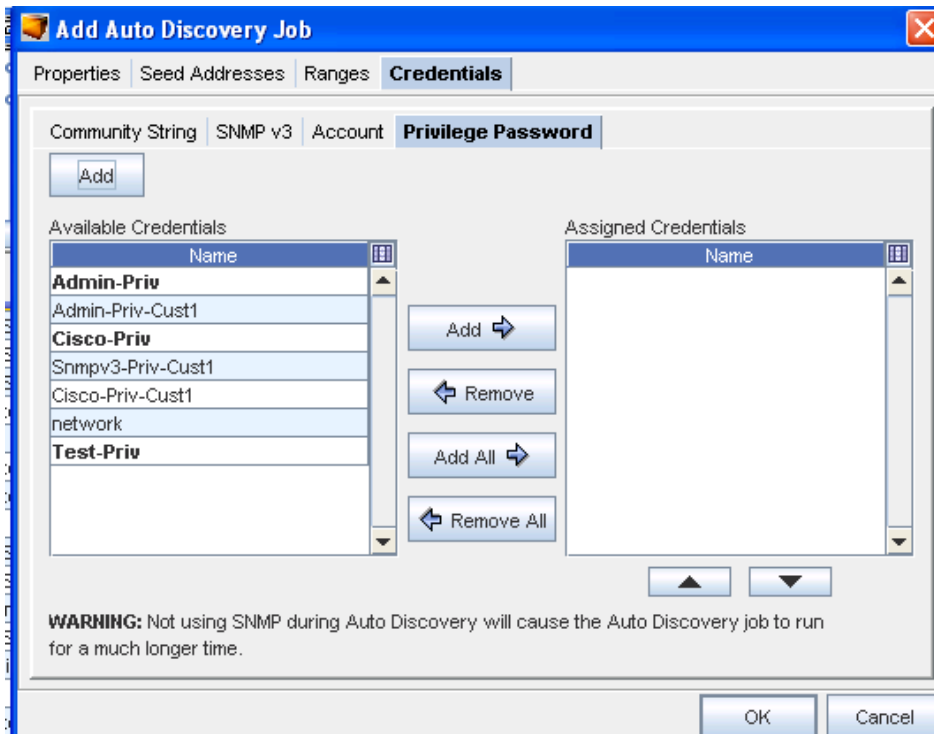




2 At the **Add Auto Discovery Job** window, click **Credentials**.

To work with the Privilege Password tab,

1 From the **Available Credentials** listing, select a **Credential**, then click the **Add** button to move that credential into the **Assigned Credentials** list. You can also use the **Select All** arrow if needed.



2 To Add a new Credential, click **Add**.

3 The **Add Credential** window displays.

4 Enter the information needed for that window, and click **Ok** when you are finished.

### Editing Auto Discovery Jobs

Editing an Auto Discovery job allows you to edit the details that have been previously set for a job. The tasks completed when editing are the same tasks you go through when the Auto Discovery job was first created.

When a job is edited, it does not have to be scheduled to run immediately. If it is on a recurring run cycle, the next time the run occurs, the changes are in effect.

For more information on the Auto Discovery tabs, see [Creating Auto Discovery Jobs](#).

Depending on the Auto Discovery type, details can be edited on the following tabs:

- Properties
- Seed Addresses
- Ranges
- Credentials

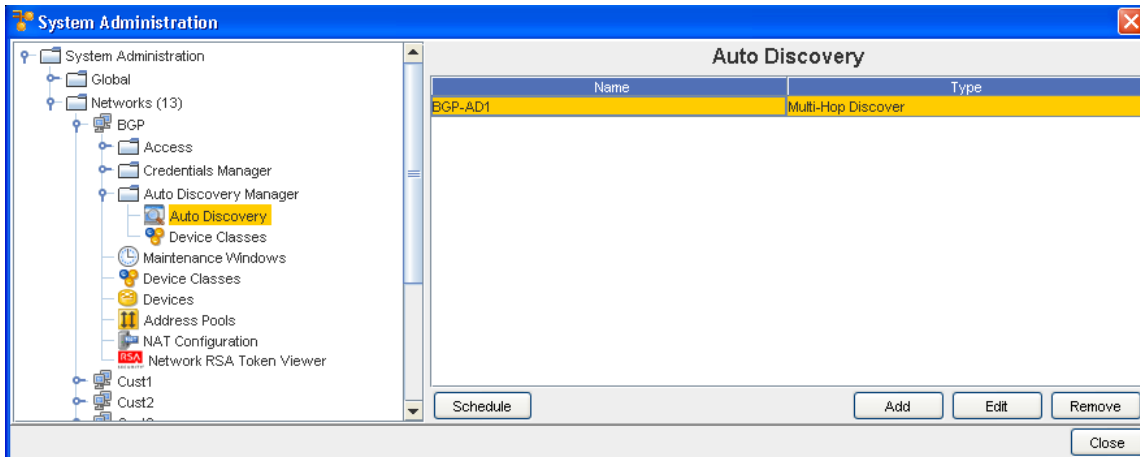
---

**Important** If insufficient details are entered on any tab, the Auto Discovery job may fail, or may not run completely.

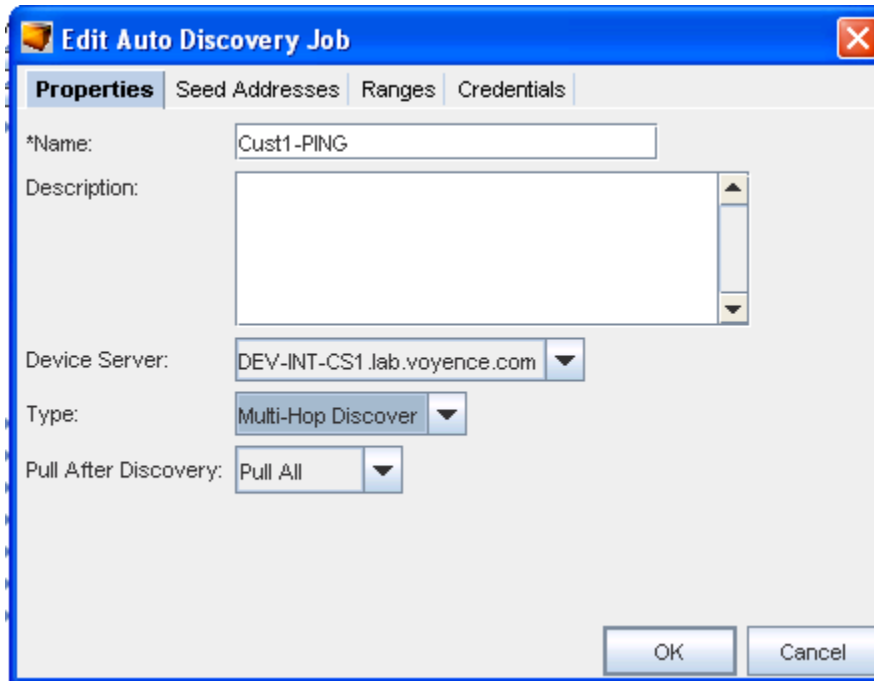
---

To edit an Auto Discovery job,

- 1 From the menu bar toolbar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Networks** folder.
- 3 Open the **Access** folder.
- 4 Click **Auto Discovery**.



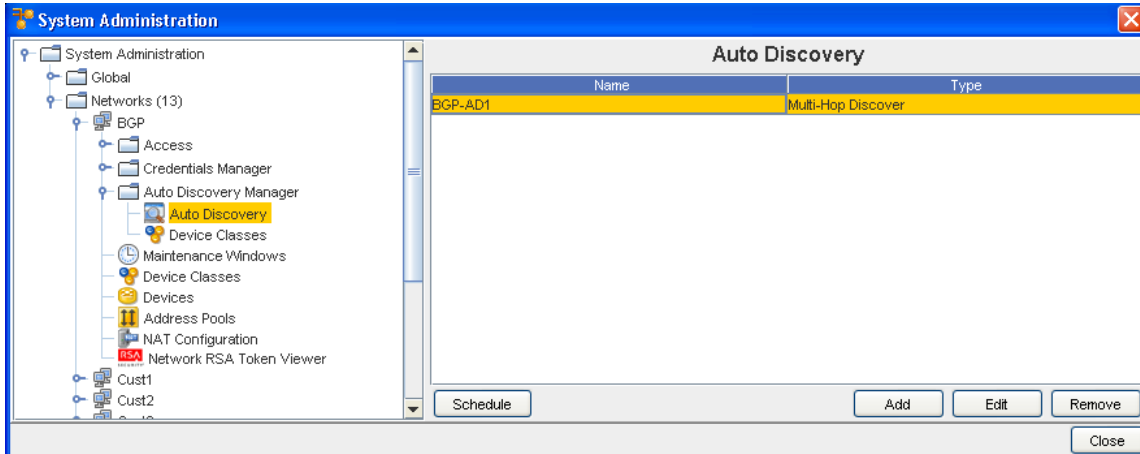
- 5 In the right pane, select the Auto Discovery **job** that you want to edit.
- 6 Click **Edit**. The Edit Auto Discovery Job window opens.



- 7 Make any needed changes to the existing information contained within each one of the tabs.
- 8 Click **Ok** when you have made your changes.

## Removing Auto Discovery Jobs

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Networks folder**.
- 3 Click **Auto Discovery** .
- 4 The right pane populates with any Auto Discovery jobs that have been created.
- 5 The Schedule, Add, Edit, and Remove buttons are displayed



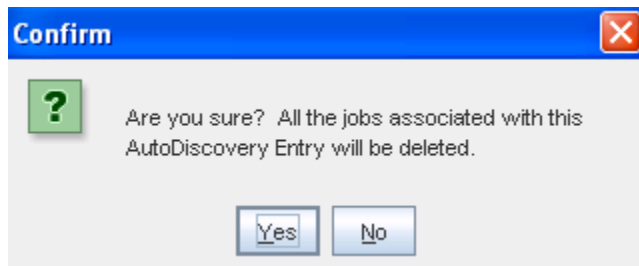
- 6 Select **one or more** Auto Discovery **jobs** to be deleted.
- 7 Click **Remove**. The Confirm window opens asking, "Are you sure?".

---

**Note** All associated jobs with the Auto Discovery entry will be deleted.

---

- 8 If okay, click **Yes**. The Confirm window closes.



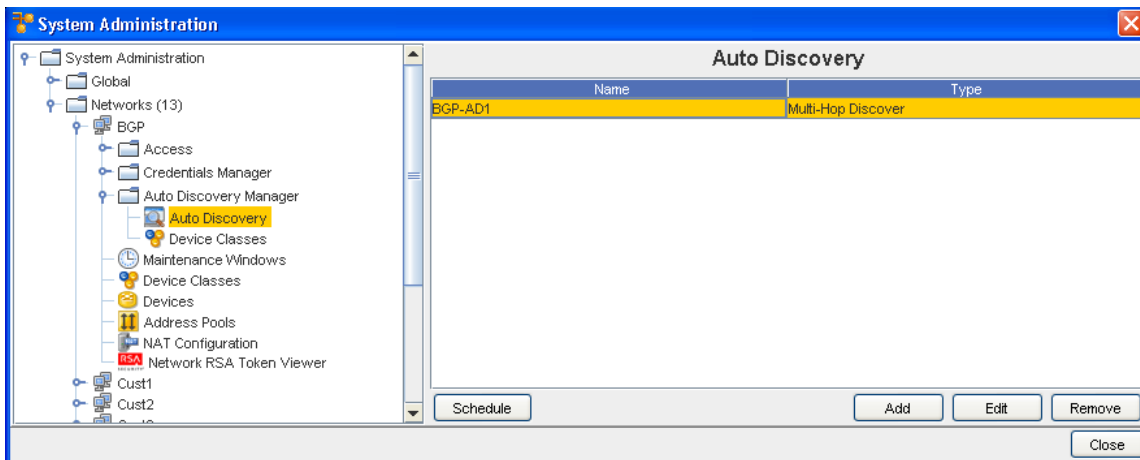
The System Administration window refreshes. The selected Auto Discovery job is removed from the right pane.

## Scheduling Auto Discovery Jobs

Auto Discovery jobs can be scheduled and then rescheduled. By storing all Auto Discovery jobs that have been created for each network, you are able to select and schedule any existing job. All settings for the stored jobs are saved, and can be edited. For more information, see [Editing Auto Discovery Jobs](#).

To schedule and submit an Auto Discovery job for approval,

- 1 From the menu bar toolbar, select **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Networks folder**.
- 3 Click **Auto Discovery**.



- 4 Click **Schedule**. The Schedule Auto Discovery Job window opens.

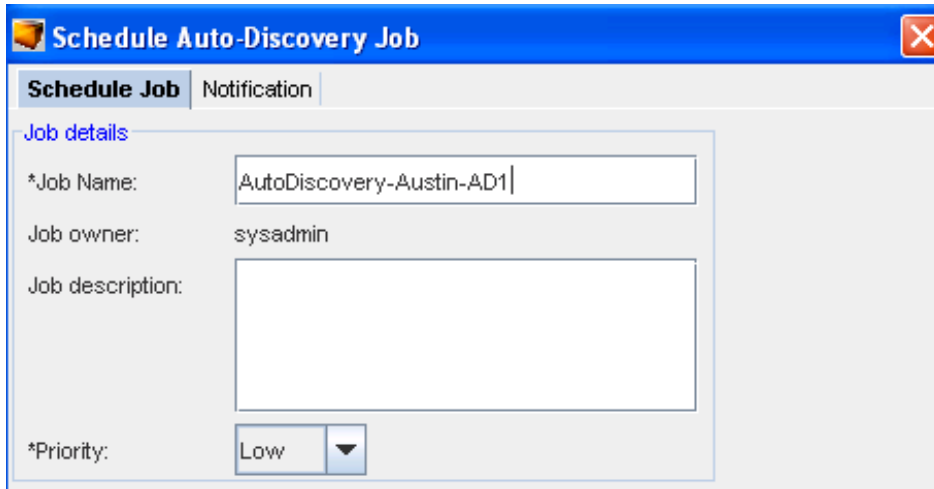
### The Schedule Job Tab

The Schedule Job tab is divided into two sections:

- Job Details
- Schedule Job

There are also two tabs, **Schedule Job** and **Notification**.

### Schedule Job - Job Details



The following fields are available when scheduling a job. The required fields are identified by an asterisk (\*).

Field	Description
Job Name	Required Field. The job name is how you refer to the job in the job history.
Job Owner	System generated, from the user creating the job
Job Description	Optional. Comment area for outlining job significance and other details that other users may find helpful during a review of the job history and tasks.
Priority Setting	Priority Setting priority allows the job to run ahead of other scheduled jobs, depending on the prioritized setting. Priority settings are: Low, Medium, and High. The default is Medium. If you are running a cut-through the priority must be High.

**Note** The priority setting affects the job execution between the device server and the network device.

### Schedule Job

**Note** When the **recurring schedule** is selected, the new time zone drop-down options are available. Make your selection from the drop-down options. The time zone you select must be the **client's time zone**. The new time zone field will be propagated with the client time zone automatically when creating a new Maintenance Window or recurring scheduled job.

The following fields are available when scheduling a job.

Field	Description
Run in next maintenance window	Setting allowing the job to run in the next maintenance window
Run upon approval	Setting allowing the job to run as soon as the job is approved. If you have job approval permissions, when you schedule the job you can also approve it to run immediately.
Run upon operator initiation	Will run when the operator designates the activity
Run at scheduled date/time	Used to set a specific date and time the job will run. This allows you to run jobs when best for your network, or based on planned network changes.
Run as recurring series	Used for pushing updates to the network automatically. Not only allowing you to set the start date, but also the end date for a limited time-span and frequency. If necessary, the update can be set to never end. This option allows the updates to continue, unless manually canceled in the Scheduler.
<b>Recurring Options:</b>	- Frequency (Hourly, Weekly, Monthly) - Start Time - End Time - Interval (Set by hours) The recurring updates do not change unless updated in the Scheduler.

The **Approve & Submit** button, located on the bottom of all tabs, can be used when adequate permissions have been granted. When clicked, the job is immediately sent to the scheduler, based on the defined settings.

- 1 Enter the information needed in the **Job Details** section.
- 2 Make your selections in the **Notifications** tab.
- 3 Make your selections in the **Schedule Job** section, then click the appropriate button ( **Approve & Submit** or **Submit**) at the bottom of the window.

## Device Types and Objects

Once auto discovery has located a device, the devices are made **available** to the networks.

Depending on the devices servers and the related devices, you might have the following devices types and objects that can be managed by your network:

- Routers
- Generic Switches
- Contivity
- Connectors
- Clouds
- Generic Devices
- VPN Concentrators
- ATM Switches
- Content Switch
- Firewalls
- layer and Switch
- Load Balancer
- Access Points
- Modems

After completing Auto Discovery to locate devices, you must [Managing Network Devices](#) to the appropriate networks. Devices can be assigned to multiple networks. When a device is assigned to a network or networks, the device is classified as *Managed*.

There are **two** ways that a device can be associated with a network:

- Automatically assigned during Auto Discovery
- Using the Mange Devices window

## Networks - Maintenance Windows



## Maintenance Window Overview

When there are large networks involved, downtime - due to changes to the network, can be costly. Network Configuration Manager allows you to set a window of time in which updates to your networks can be scheduled. This can be designated by time of day, days of the weeks, or scheduled to run on a regularly scheduled event until changed basis.

A maintenance schedule can be set for the entire network, or for separate networks that are managed by Network Configuration Manager.

Similar to the Schedule Manager window, the Maintenance window uses the One-time schedule, or a Recurring schedule, that allows you to determine not only when, but how often updates occur to the network.

It is not necessary to create Maintenance schedules for all networks. Networks inherit any System Maintenance window settings. If a System Maintenance is not set, then each network defaults to the individual scheduled times.

Maintenance windows can be overridden at the Network level. When set at the Network level, any Global Maintenance windows must be copied down to the Network. Windows can only be set at either the Global or Network level, but not both,

Maintenance windows can be set for the following:

- Pushes
- Pulls
- Auto-discovery
- Commands
- Quick commands
- Cut-throughs
- OS Updates
- Reports

If more than one of the following types is scheduled, the following priority sequence will be used.

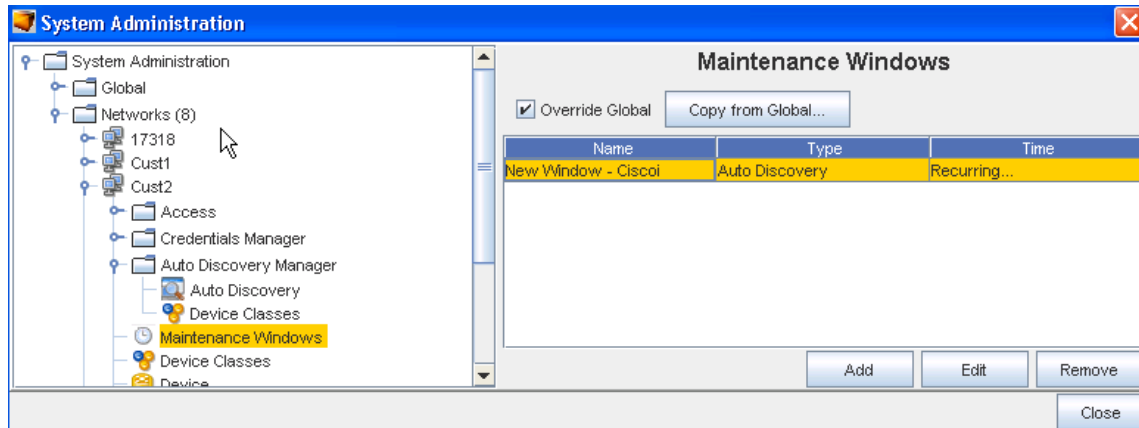
- OS Update
- Config/Configlet Push
- Saved Command
- Auto-Discovery
- Pulls

---

**Note** Quick Commands and Cut-throughs cannot be scheduled. Overlapping schedule times is not allowed.

---

As an added feature, a user with the **appropriate privileges can override a scheduled maintenance (at the Network level)** . This is allowed, for emergency changes to the network for which the schedule change is either unnecessary or harmful.



**Important** Note that you can select to Override Global settings, and then Copy from the Global Settings from this Network window. You must select Yes to continue the copy process.

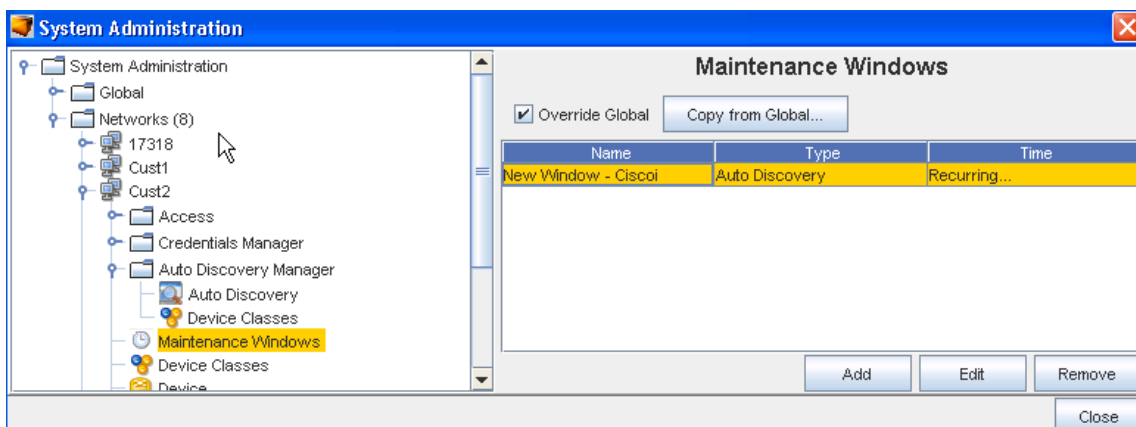
### Networks - Adding a Maintenance Window

A Maintenance window can be added at the System (Global) Level, or at the Network Level.

**Note** You can now define a window for each activity that can be completed against a device, thus ensuring that only those activities can only be completed during that designated window.

To add a scheduled maintenance window,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Networks -> Maintenance Window**.



- 3 Click **Add**.

The Maintenance window uses the same schedule window as the Schedule Manager.

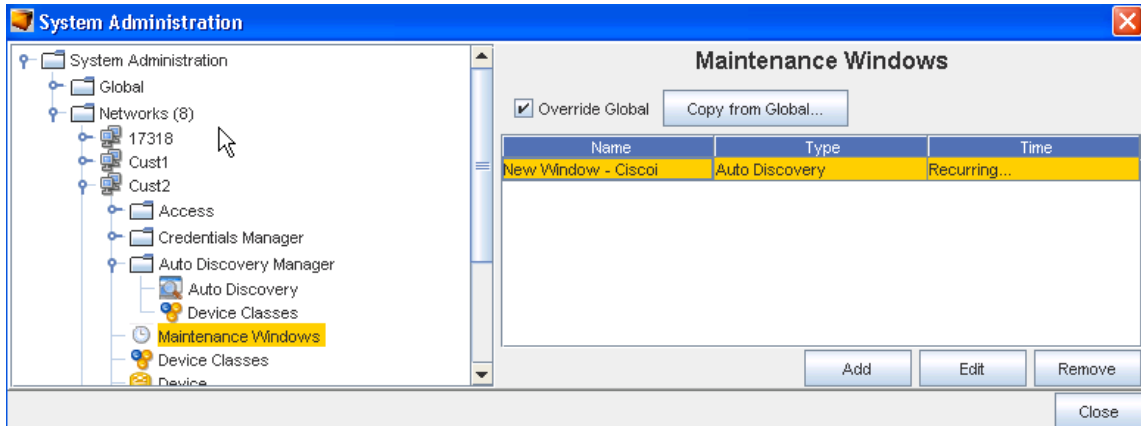
- Set the **exact date** and time for the run to occur.
  - Select a **recurring schedule** using the **Run As Recurring series** option. When the recurring schedule is selected, the new **time zone** drop-down options are available. Make your selection from the drop-down options. The time zone you select must be the **client's time zone** . The new time zone field will be propagated with the client time zone automatically when creating a new Maintenance Window or recurring scheduled job.
- 4 After making your schedule preferences, click **OK**. The maintenance window closes, and the information is now stored within the Maintenance Windows.
- Enter a **unique name** for the maintenance window.
  - From the drop down list, select a **Type**. Remember, you can now schedule a window for each activity.
  - From the next drop down ( **Window Duration**), select the time allocated updates.
  - Next, at the Schedule portion of the window:

### Networks - Editing a Maintenance Window

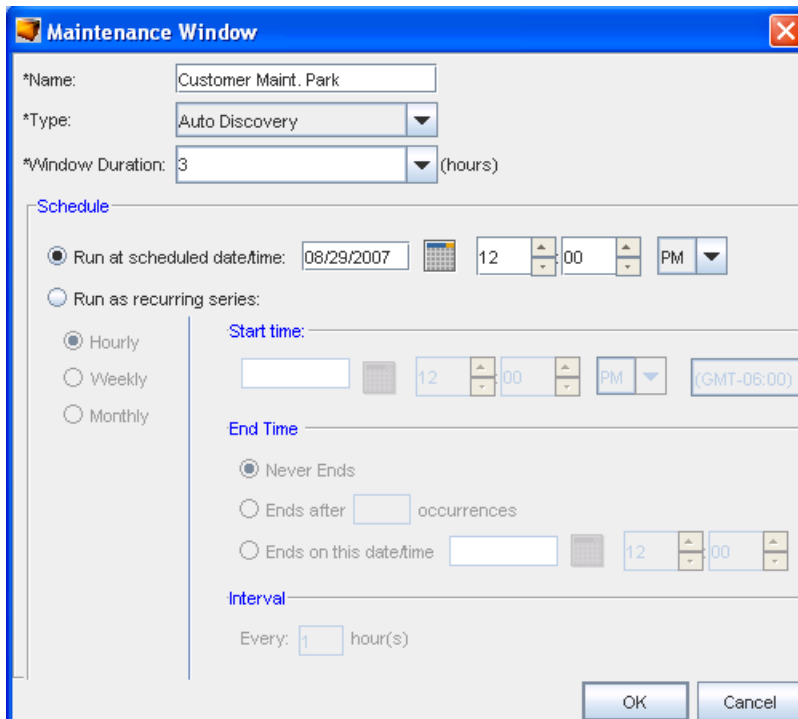
Maintenance windows can be added at the System (Global) Level, or at the Network Level. The date, time, or recurring sequence can be edited, based on the needs of your networks.

To edit a scheduled maintenance window,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Networks -> Maintenance Window**.
- 3 Select the **Schedule** from the list, then click **Edit**.



Or, select the schedule, then click **Edit**. The schedule opens. The current settings are available for edit.



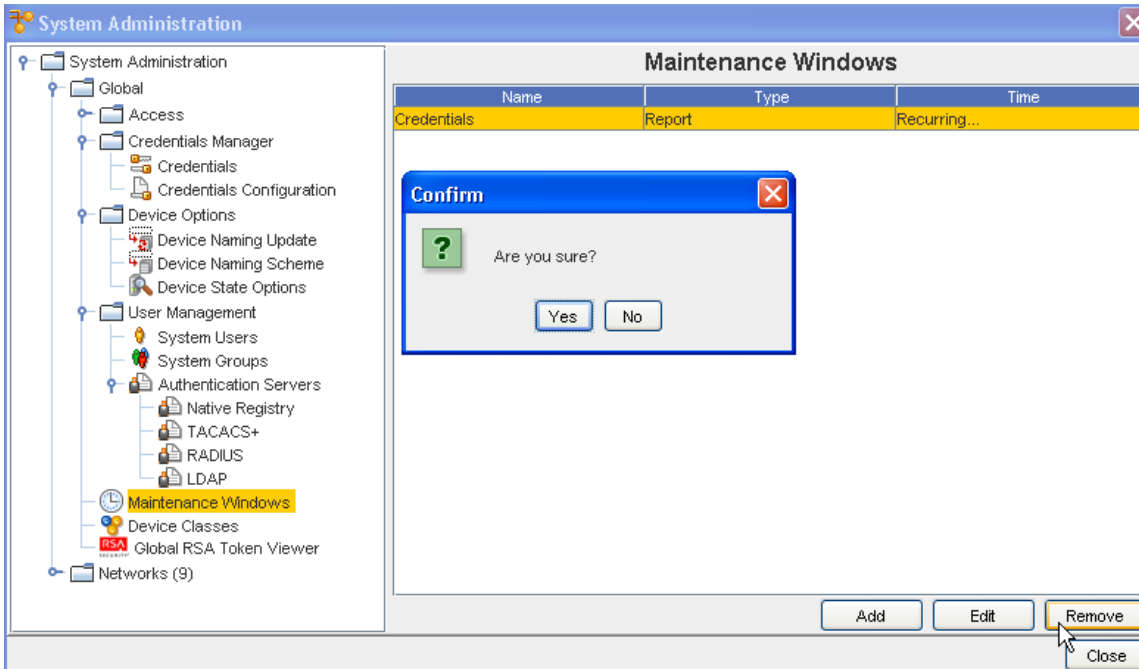
- 4 Make changes to the schedule as needed.
- 5 Click **OK**. The changes are saved and are in effect on the next schedule run. The Maintenance window closes.

### Networks- Removing a Maintenance Window

When a schedule is no longer needed for your networks it can be deleted from the list. By removing a maintenance schedule, any network with the associated schedule takes on the settings of the System (Global) maintenance schedule (if one has been previously set).

To remove a scheduled maintenance window,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Global -> Maintenance Windows**.
- 3 Select the schedule (maintenance window), then click **Remove**. The confirmation window displays.



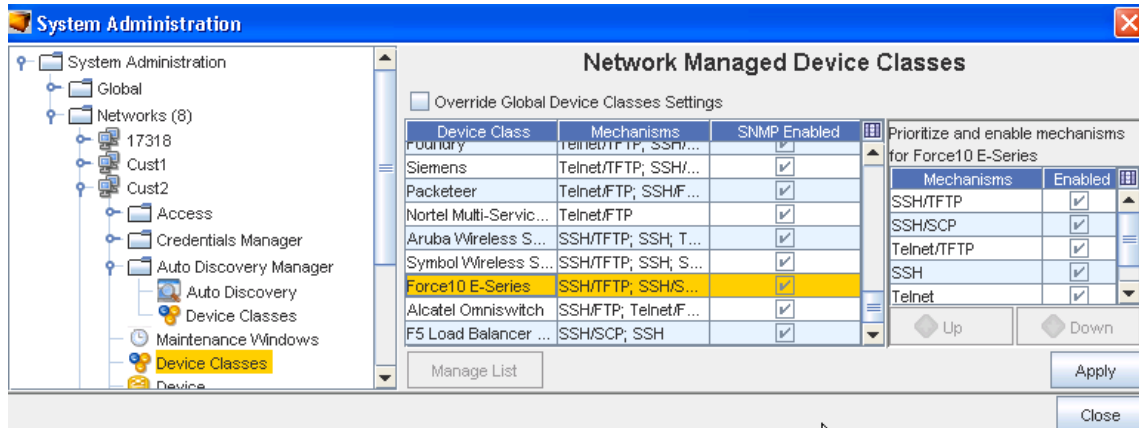
- 4 If okay, click **Yes**. Or, to cancel this action, click **No**.

The Maintenance Window updates with the selected item removed from the list.

## Networks - Device Classes

### Network - Device Classes Overview

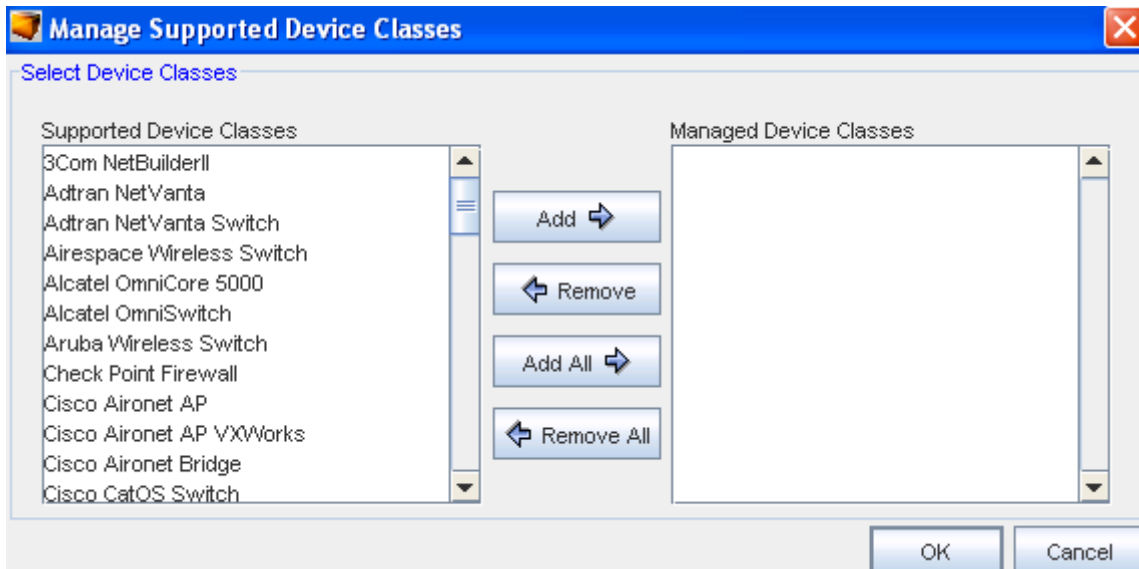
From the System Administration tool, you can access the Device Classes for the various Networks you have created.



From this Network Managed Device Classes window you can work with the Device Classes.

To Manage the Devices Classes list (and override Global Settings),

- 1 From the listing of Device Classes displayed in the Network Managed Device Classes window, select a **Device Class**, then click the **Override Global Settings** check box.
- 2 Next, select the **Managed List** button to view a listing of the Supported Device Classes shown in the Manage Supported Device Classes window.



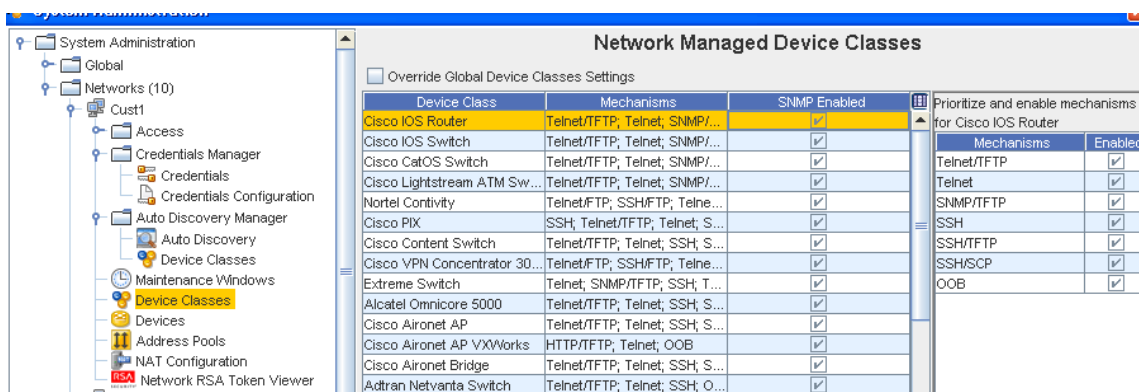
- 3 Make your selections from the **Supported Device Classes** pane, and move them into the **Managed Device Classes** pane using the **Add** or **Add All** buttons. Note that you can also remove any unneeded classes using the **Remove** or **Removal All** buttons.
- 4 Click **Ok** when you have made all your additions to the Managed Device Classes pane. The Device Classes you added are now in the listing shown in the Network Managed Device Classes window.

## Networks - Specifying Device Class Protocol

**Important** Your Networks may not be configured to handle certain protocols for supported devices. If you choose, you can enable or disable communications to your network devices using specific communication protocol methods.

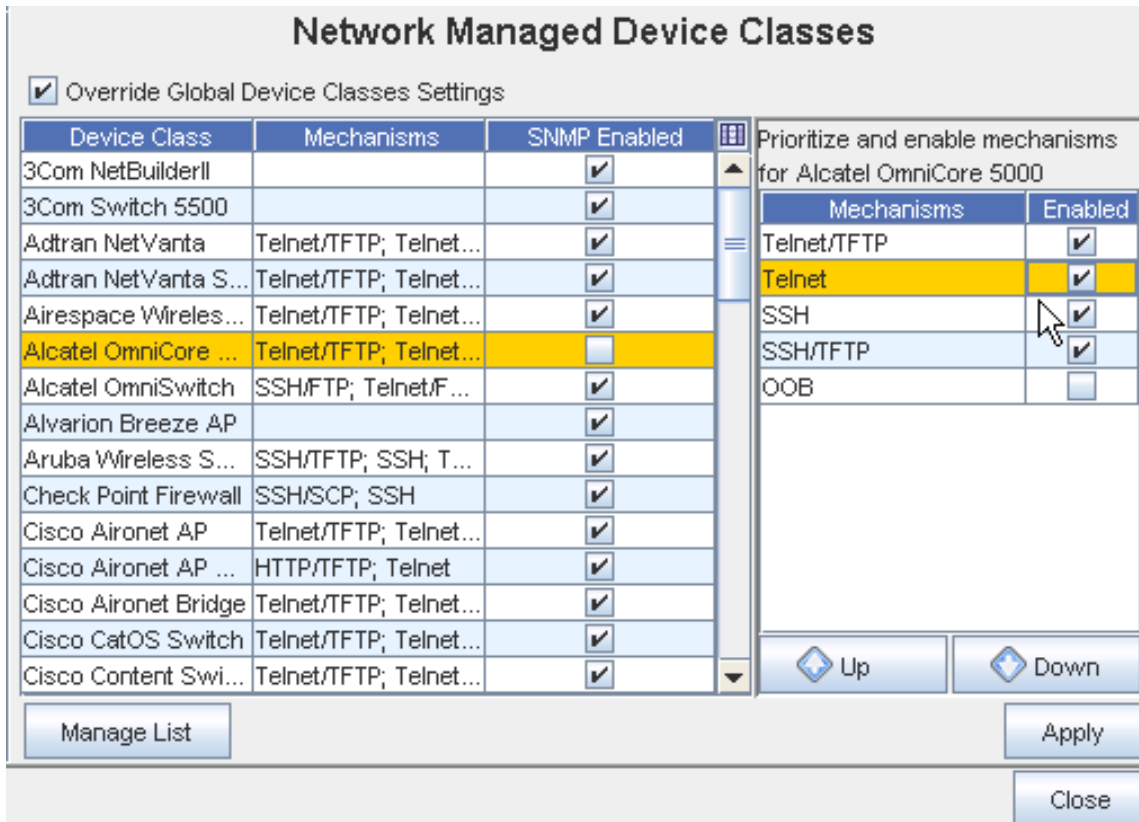
To adjust the device class protocols,

- 1 From the menu bar, select **Tools**.
- 2 From the menu options, select **System Administration**. The System Administration window opens.
- 3 On the tree menu, expand the **Networks -> Access** folders.
- 4 Select **Device Classes**. The Network Managed Device Classes configuration window populates the right pane.
- 5 Select a **row (listing the Device Class and the Primary Protocol)**. When highlighted, the Enable or Disable fields show any protocols that are active/deactivated for the device class.



**Note** By default the Use SNMP check box is selected. If you choose not to use SNMP, un-check this check box.

- 6 To make changes to the Protocols section, **disable** the device class by un-checking the check box, then select another **Mechanism** from the listing to the right.



- Adjust the priority of the protocols
- Enable or Disable protocols

7 Click **Apply** when you have select a Mechanism from the list.

- This window allows you to:

To change the priority of the listed protocols,

- 1 Select a **protocol** from the list. Based on its location in the list, the Up and Down arrows activate.
- 2 Using the Up/Down arrows move the selected protocol to the new location. The top-most protocol is used as the default.
- 3 If you are enabling or disabling protocols, proceed to the next step. Or, if no other changes are required, click **OK**. The Manage Devices - [Device Class Name] window closes.

To enable and disable device protocols,

- 1 If you are enabling a protocol, in the Enable column, check the boxes of the **approved protocols**.
- 2 If you are disabling a protocol, in the Enable column, de-select the check box.
- 3 If no other changes are required, click **OK**. The Manage Devices - [Device Class Name] window closes.

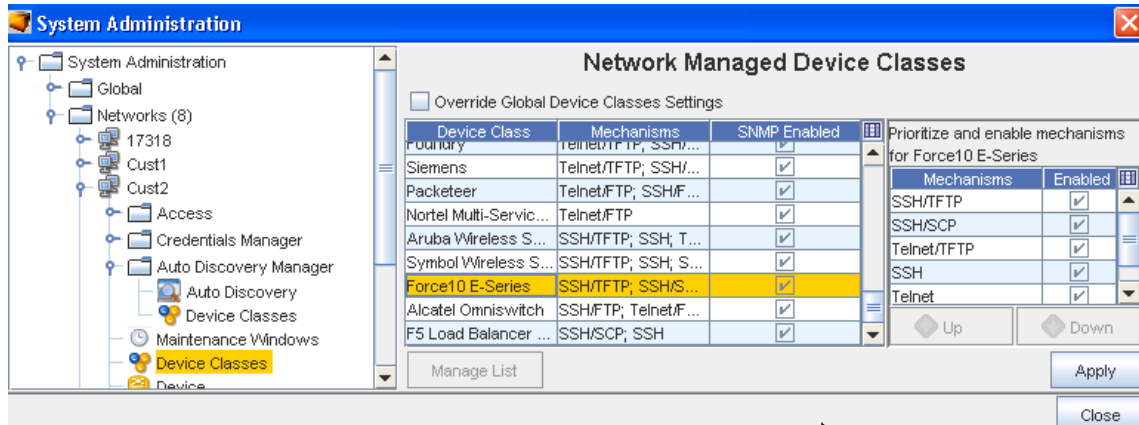


- When all changes have been completed on the Network Managed Device Classes window, click **Apply**.

## Override Global Settings

Device Classes and Communication mechanisms can be overridden at the Network level. To do this, the Override Global Settings check box must be selected.

This allows you to use SNMP/TFTP to manage Cisco routers in one Network, and to use Telnet for management in another Network.



## Networks - Devices

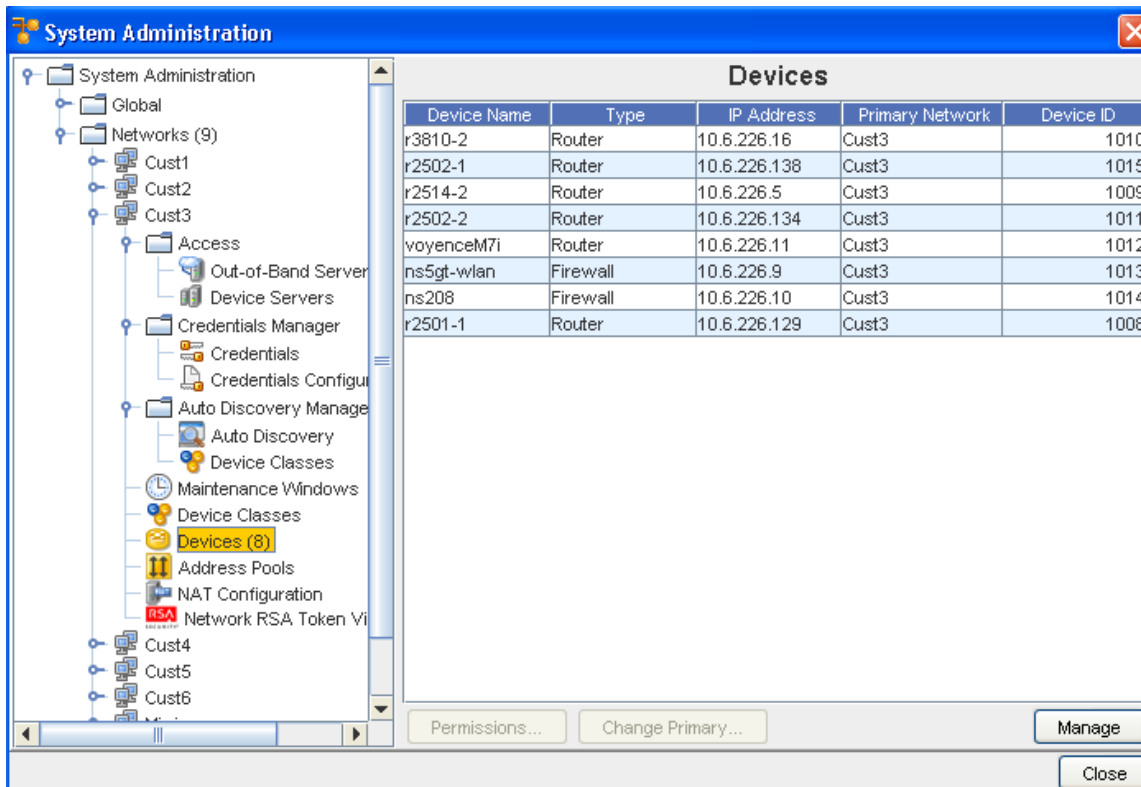
### Managing User and Group Device Permissions

The devices on the device server are edited in two ways:

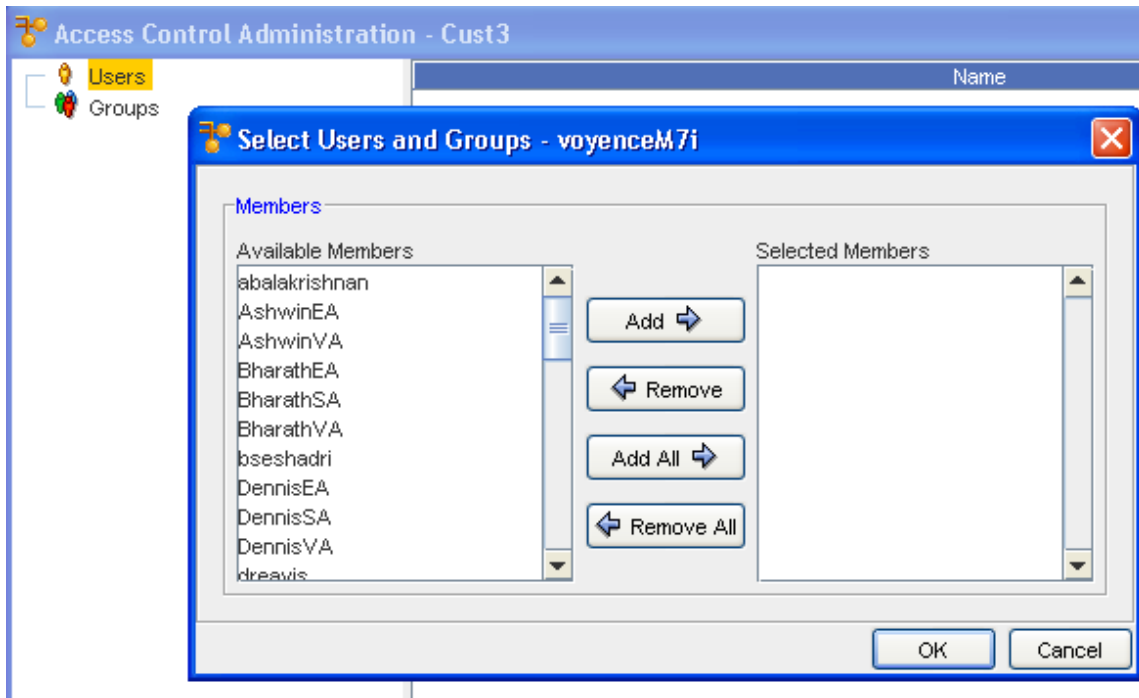
- Editing the device override default settings
- Defining devices level permissions

To designate users permissions at a device level,

- In the navigation pane, open the network where the device is located.
- Expand the **Network** folder, then select **Devices**.
- In the right pane, select one or more devices .



- 4 In the lower portion of the window click **Permissions**. The Access Control Administration window opens. There are two groups:
  - Users
  - Groups
- 5 Select an option, then at the bottom of the window, click **Manage**. The Select Users and Groups window opens.



- Users and groups that do not have permissions are listed in the Available Members column.
  - All users and groups with permissions are listed in the Selected Members column.
- 6 To give users or groups permissions to the workspace, click the **name of the user or group** in the Available Members column.

**Note** A string of users/groups can be selected by holding down the Shift-key while selecting users/groups. Or, select multiple, non-sequential users/groups can be selected by holding the Ctrl key while selecting users/groups.

- 7 Click **Add**. The selected users and groups are moved to the Selected Members column, and have permissions to the workspace. Or, to remove a user or groups permissions, in the Selected Members column, select the name or group.
- 8 Click **Remove**. The selected users and groups are moved to the Available Members column and no longer have permissions to the workspace.
- Clicking **Add All** moves all users and groups listed in the Available Members column to the Selected Members column.
  - Clicking **Remove All** moves all users and groups back to the Available Members. If you complete this action, remember to put your own user name back into the Selected Members column.
- 9 Once you have the needed users and groups to have access to the workspace, click **Ok**. The Select Users and Groups window closes.

The Access Control Administration window refreshes. All users and groups are re-categorized to reflect the changes that were made.

You are now able to set the [Setting User and Group Permissions](#) and Others. (Others are users that have limited access determined by the permission settings for selected devices only.)

### Changing the Device's Primary Network

Device Permissions, Device Status, and Primary Network are all set in the Network level devices area. Since a device can be shared by multiple Networks, and its credentials and communications are set from its Primary Network, the Primary Network name is available in this window.

You can change the Primary Network associations by clicking on Change Primary, and then re-selecting the Primary Network.

---

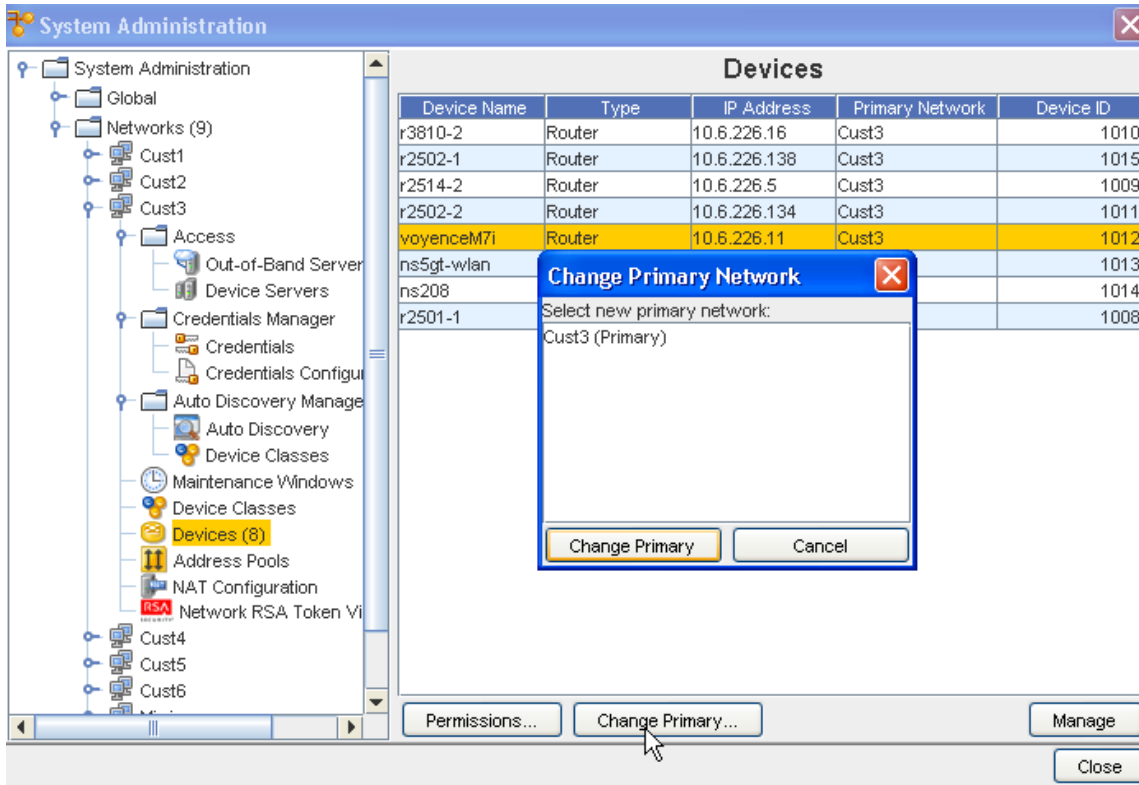
**Important** Primary Network does not appear by default in the Device table. To view the Primary Network, you must modify the table setting to include this field.

---

Network Configuration Manager allows devices to be managed by multiple networks . The first network that the device is associated with becomes its **primary** network.

To change the primary network of a device,

- 1 From the menu bar, select **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, click **Networks**.
- 3 Open the device's current primary network.
- 4 Expand the **Network** folder, then select **Devices**. The right pane populates with all devices currently residing in the network. If the network is the primary location of the device, they Primary Network column contains information.
- 5 In the right pane, select one or more devices. The selected devices are affected by the following steps.



- Click **Change Primary** . The Change Primary Network window opens.
- Select a name from the listing, then click **Change Primary** . The Primary Network you selected is now displayed in the Devices list.

## Networks - Address Pools

### Address Pool Overview

The Address pools allow you to setup flat address pools using Network Configuration Manager. You can define address pools for each Network within Network Configuration Manager.

**Note** This feature is also available using the API.

The IP Addressing feature uses a flat topology, but it contains multiple blocks. These flat pools are only seen in the network for which they are created. The pools are then used in the Workspace, Sites, and Views of the network.

There is no limit to the number of IP Addresses that can be set up in the pool. When needed, addresses can be excluded. When a device is pulled into the repository, the device's IP is authenticated to make sure it's IP is defined in the networks pool.

IP Addresses are blocked for each network. Each block can contain as many IP Address as needed for the block. Address blocks can be allocated from pools for use in assigning IP Addresses to new devices and interfaces. Addresses are assigned through the use of insert IPs and Insert Reference Variables within [Editors Overview](#)

When completing cleanup and maintenance on the IP Address blocks, you can [Removing an IP Address Pool](#) or only [Editing an IP Address Pool](#).

### Managing Address Pool Usage

The status of existing Address pools can be checked by clicking **Manage Usages**. Address blocks in each of the four status pools (Used, Ready, Held, and Excluded) can be checked.

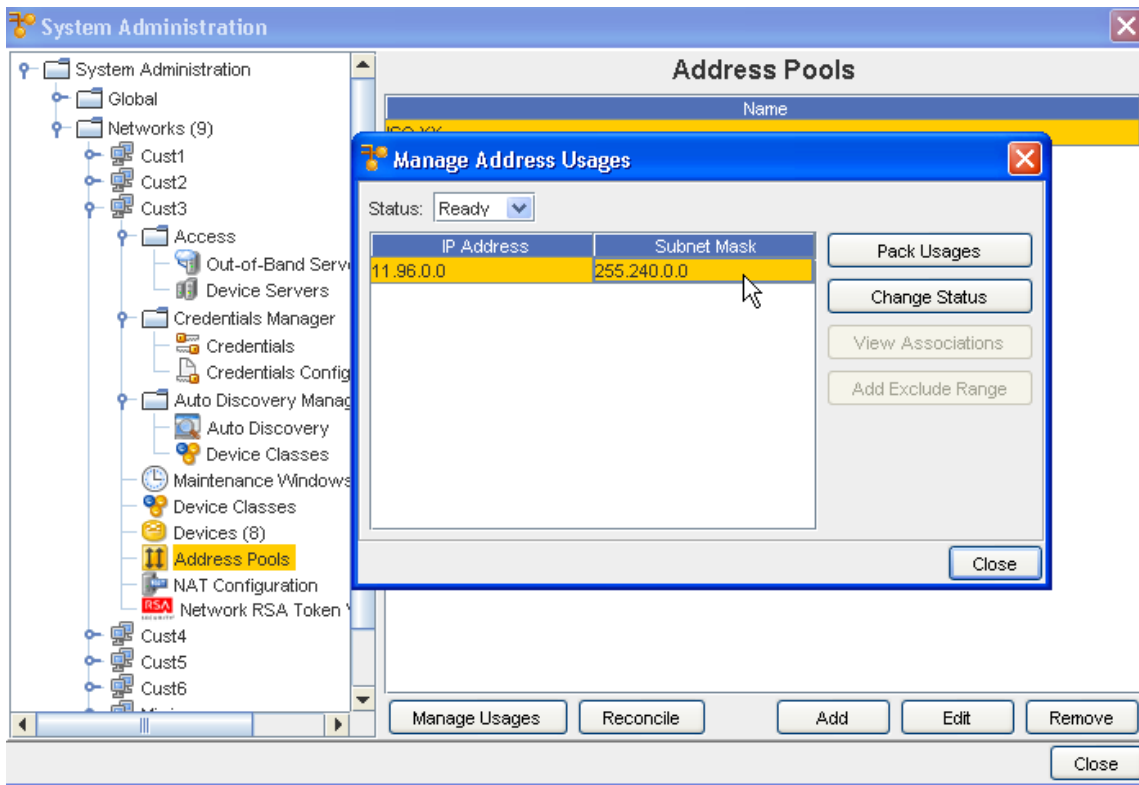
IP associations can be checked, and the status of currently used blocks can be managed.

The ability to manage the usage of IP Addresses has four options:

- Pack Usages
- Change IP Address Status
- View the Associates of the IP Address
- Add Exclude Range

To access the Manage Usage feature,

- 1 From the menu bar, select **Tools -> System Administration** .
- 2 Next, select **Network -> Address Pool**. The Address Pools List window opens. All existing IP Address Pools are listed.



- 3 Select an address pool, then click **Manage Usages**. The Manage Address Usages window opens.

You can view the **Status** of the range of IP addresses using the drop-down arrow, and making a selection from the list. You can view IP addresses in the Held, Used, Ready and Excluded status. Once you have made a Status selection, the IP addresses within that status are displayed.

The Manage Address Usages window allows to you see the following details about the selected address pool.

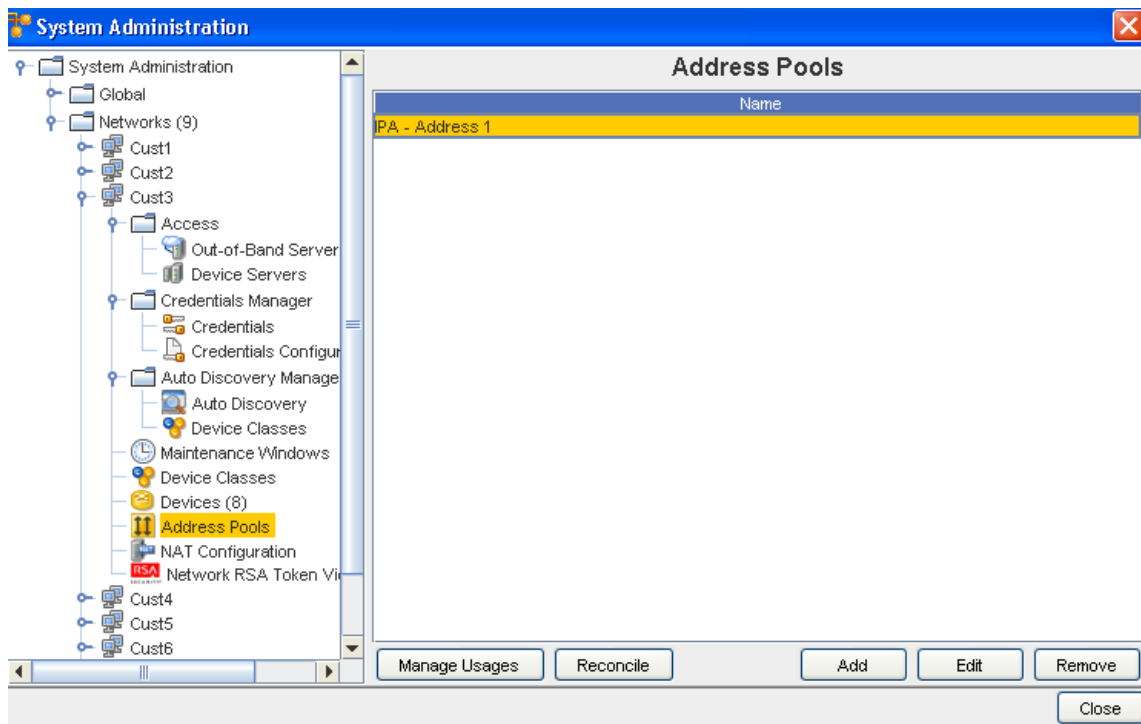
### View IP Address Pool Associates

The ability to manage the usage of IP Address has four options:

- Pack Usages
- Change IP Address Status
- View the Associates of the IP Address
- Add Exclude Tang

To view devices which currently use the selected IP Address,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Address Pool**. The Address Pools List window opens. All existing IP Address Pools are listed.



- 3 Select an Address pool, then click **Manage Usages**. The Manage Address Usages window opens.
- 4 Select the **IP Address row**. If there are devices associated with the IP Address, the View Associations button becomes active.

5 Click **View Associations** . You can now view the associations information.

### Change IP Address Pool Associates

The ability to manage the usage of IP Address has four options:

- Pack Usages
- Change IP Address Status
- View the Associates of the IP Address
- Add Exclude Range

The Change Status features allows you to modify the status of an IP address range without deleting the range.

---

**Note** Changing the status only affects the status for the specified range, not the entire address pool.

---

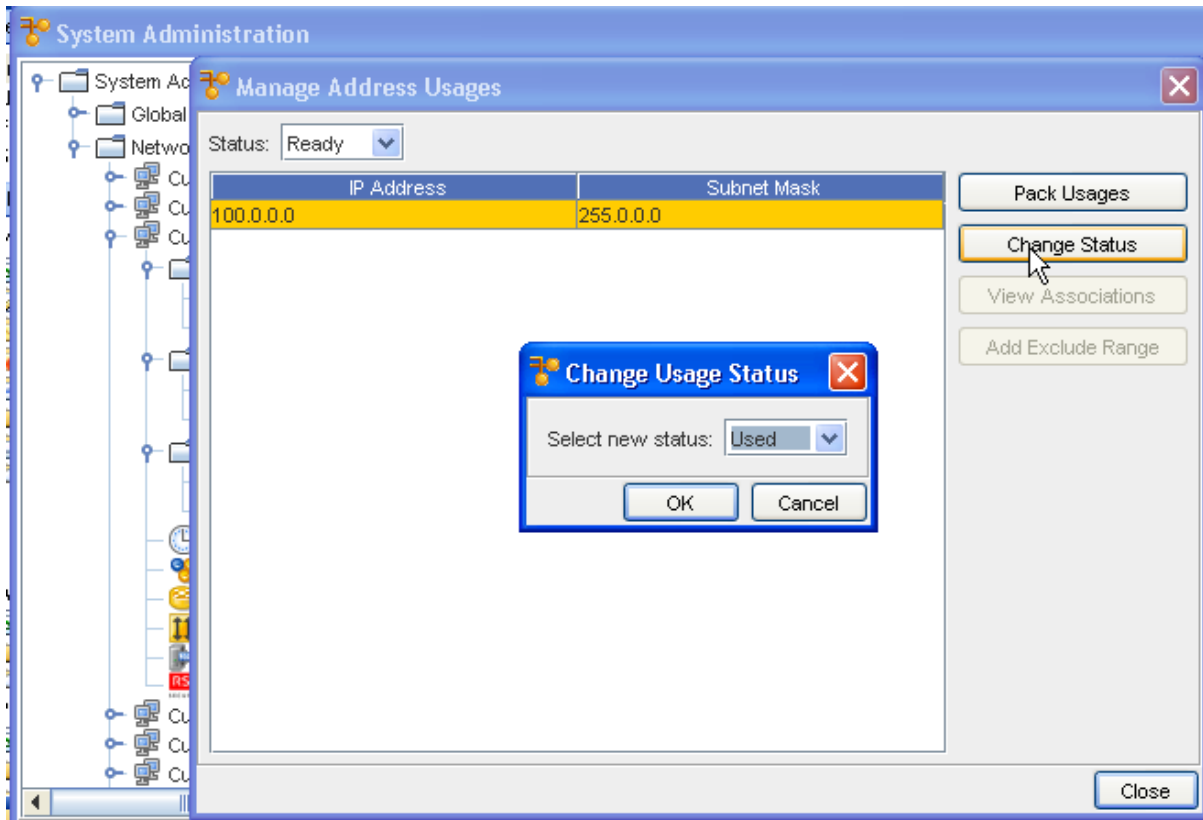
The current status options are:

- **Ready** - Identifies the IP address ranges that can be used for device IP address comparison or inserted in an editor
- **Used** - Identifies the IP address ranges that are currently being utilized
- **Held** - Identifies IP address ranges that have been assigned by Network Configuration Manager -- but not yet deployed to a device
- **Excluded** - Identifies address ranges that are currently excluded from use in Network Configuration Manager.

To change the status of an IP Address range,

- 1 From the menu bar, select **Tools -> System Administration** .
- 2 Next, select **Network -> Address Pool**. The Address Pools List window opens. All existing IP Address Pools are listed.
- 3 Select an Address pool, then click **Manage Usages**. The Manage Address Usages window opens.





- 4 Select the **IP address row**, then click **Change Status**. The Change Usage Status window opens.
- 5 From the drop-down list, select the new status for the IP Address.
- 6 Click **OK**. The Change Usage Status window closes, and the Manage Address Usages window updates.

### Reconcile Address Pools

IP Address pools may need to be **reconciled** if there have been changes made to the pools that are no longer in-sync. Reconciling IP Address pools permits you to see those address ranges within your pool already allocated to devices within the Network.

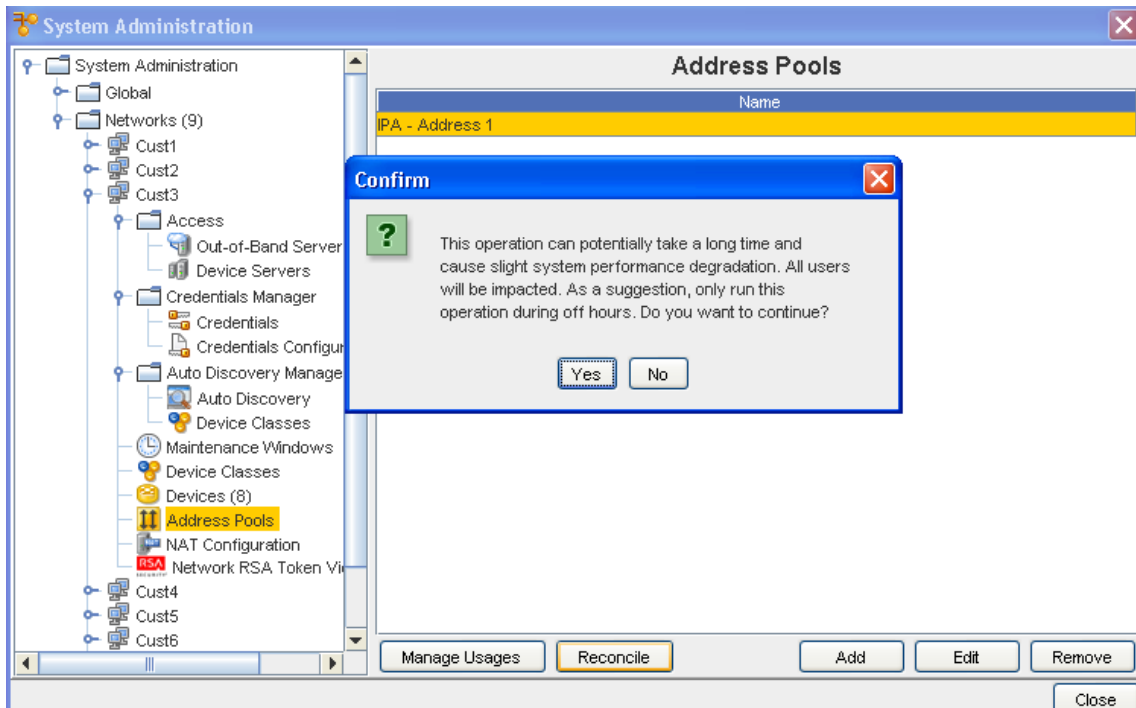
---

**Important** Take care in using Reconcile, as it is an application-intensive process.

---

To reconcile an out-of-sync IP Address pool,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Address Pools**. The Address Pools List window opens. All existing IP Address Pools are displayed.
- 3 Select the Address Pool that is out-of-sync, then click **Reconcile**.



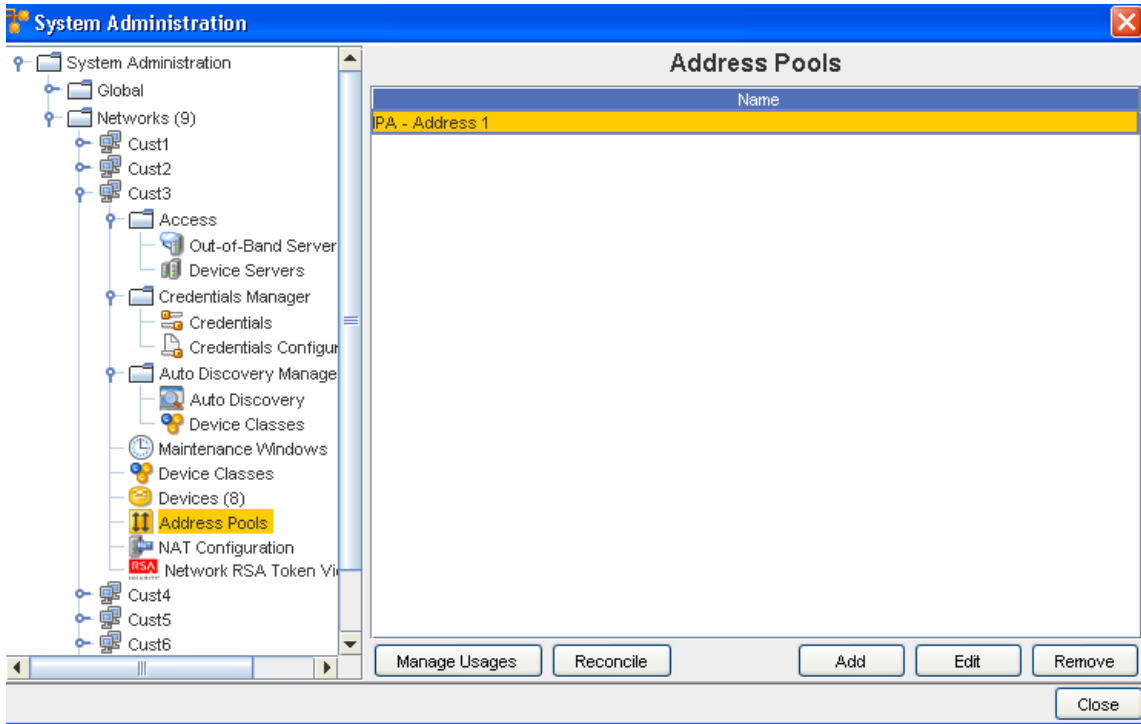
- Carefully read the Confirm message, then select **Yes** to complete the task, having been made aware of the effects, or select **No** to end this activity.

### Adding an IP Address Pool

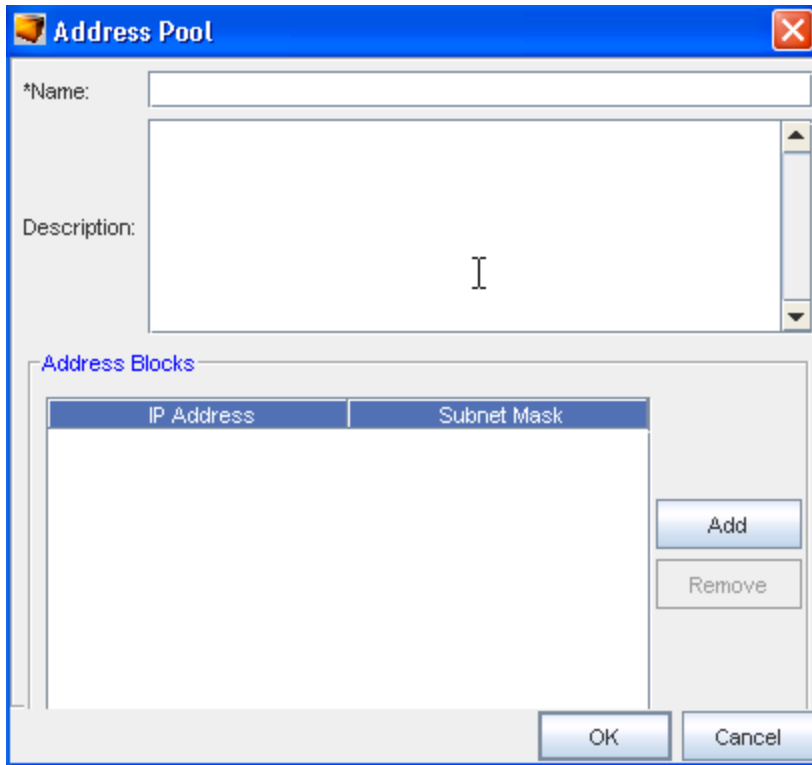
IP Address pools are added in a flat topology, and can only be used with the network in which it is created. Voyence does not allow you to create an overlapping IP Address block.

To add an IP Address to the network pool,

- From the menu bar, select **Tools -> System Administration**.
- Next, select **Network -> Address Pools**. The Address Pools List window opens. All existing IP Address Pools are displayed.

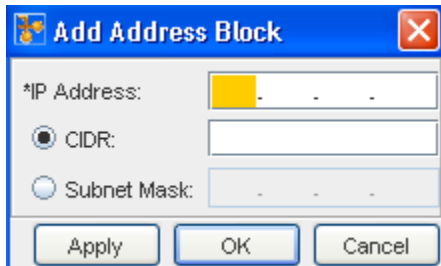


3 At the bottom of the window, click **Add**. The Address Pool window opens.



4 At a minimum, you must enter a **name for the pool**. Once the IP Address Pool has been named, the name cannot be modified.

- To define the IP addresses, click **Add**. The Add Address Block window opens. At a minimum, the **IP Address** must be defined in this Add Address Block window. A **CIDR or Subnet** for the IP Address must also be entered.




---

**Note** When the CIDR and Subnets are defined, and when the IP Address matching is queried, the specified details must also match.

---

- If you are entering more than one IP Address pool, click **Apply**. Both the IP Address List and Add Address Block window refreshes. Or, if you are entering a single block, click **OK**.

The Add Address Block window closes, and the IP Address is added to the IP Address List window.

### Editing an IP Address Pool

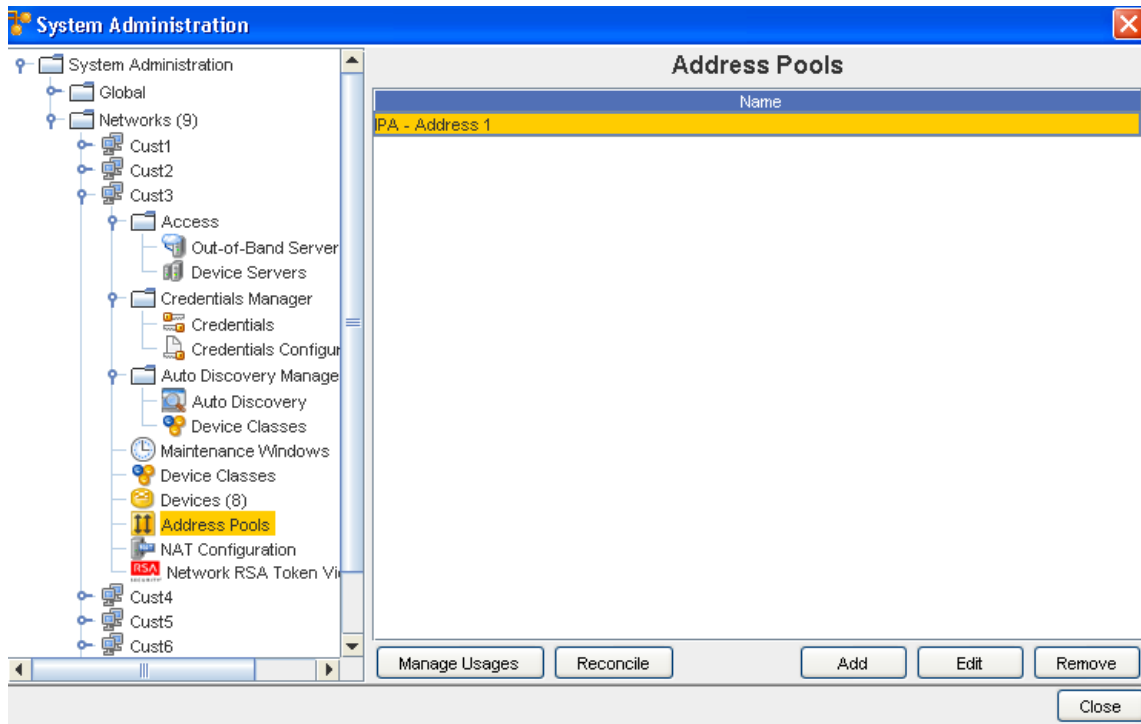
With the current design of IP Address Pools, you can:

- Add IP Addresses to a block
- Insert a description of the pool
- Delete an existing IP Address from the block

The ability to add an IP Address to an existing block uses the same instructions as provided in the [Adding an IP Address Pool](#) topic.

To edit the IP Address Pool description,

- From the menu bar, select **Tools -> System Administration**.
- Next, select **Network -> Address Pools**. The Address Pools List window opens. All existing IP Address Pools are listed.
- At the bottom of the window, click **Edit**.



The Address Pool window opens.

- 4 Make any changes needed, then click **OK**.

To remove an IP Address Pool from a block,

- 1 Open the Network IP Address Pool list.
- 2 At the bottom of the window, click **Edit**. The Address Pool window opens.
- 3 From the list of IP Address within the pool, select the **pool** you want deleted.
- 4 Click **Remove**. The window updates.
- 5 When finished, click **OK**. The Address Pool window closes.

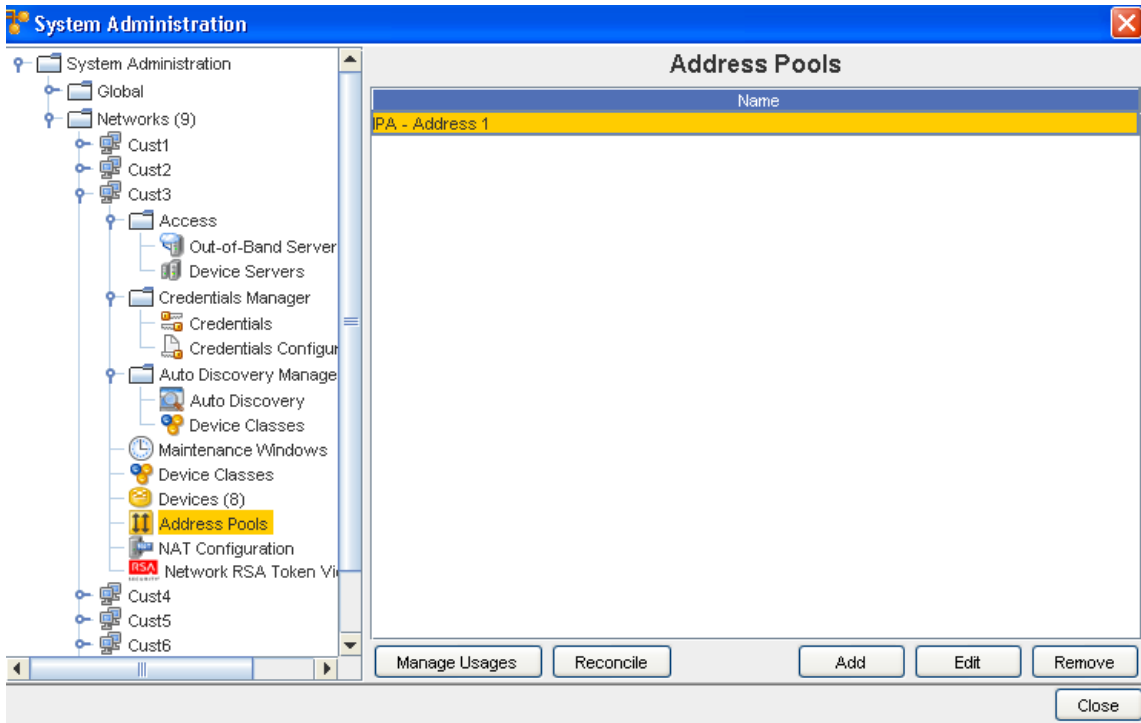
### Excluding IP Addresses

The ability to manage the usage of IP Address has four options:

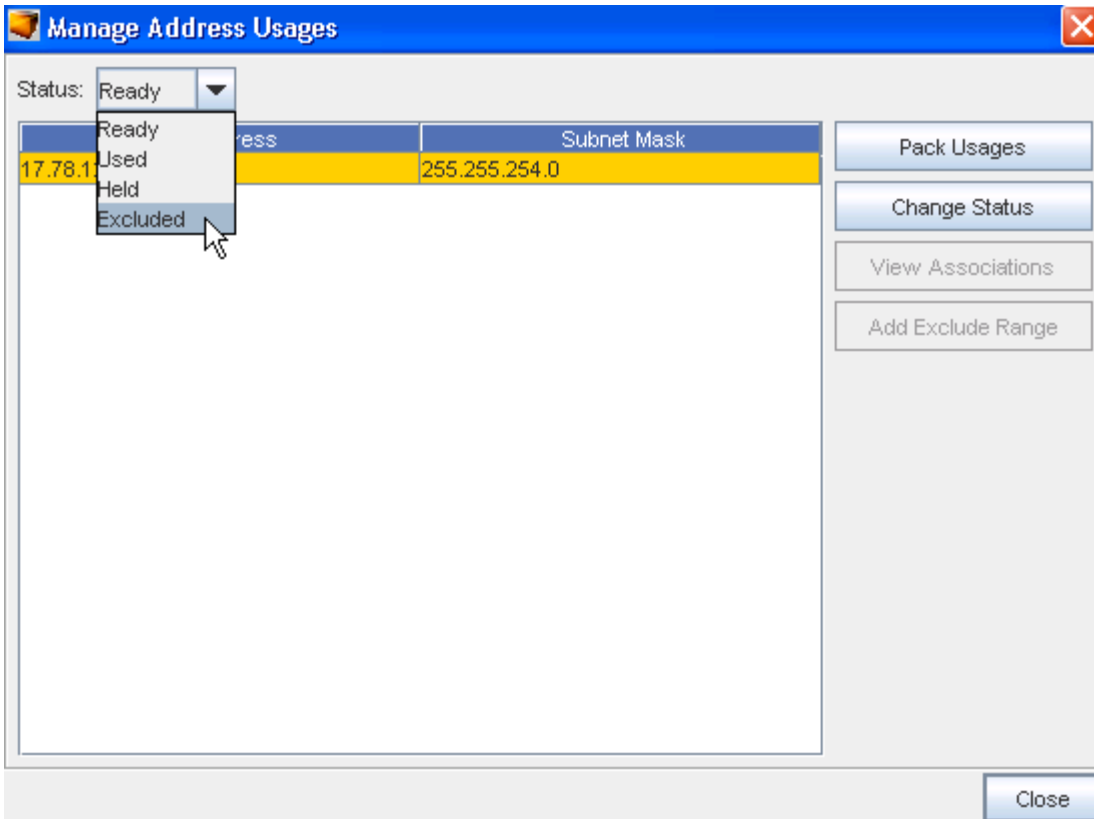
- Pack Usages
- Change IP Address Status
- View the Associates of the IP Address
- Add Exclude Range

To excluded ranges within an IP Address range,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Address Pool**. The Address Pools List window opens. All existing IP Address Pools are listed.



- 3 Select an Address pool, then click **Manage Usages**. The Manage Address Usages window opens.



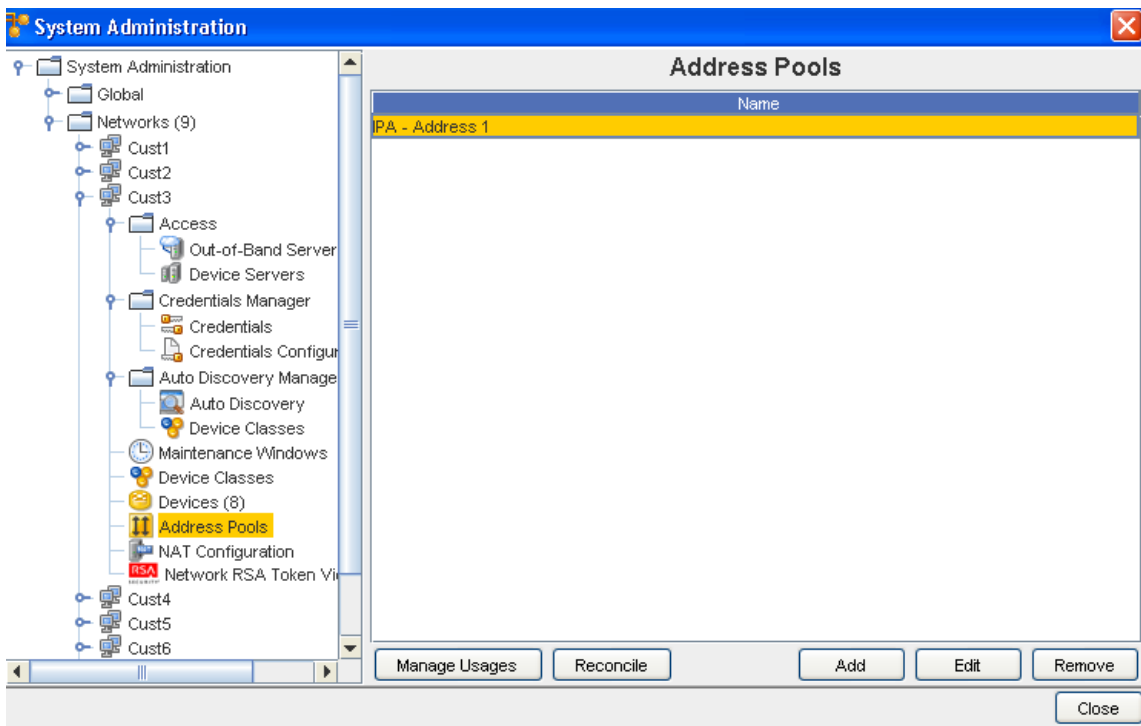
- 4 From the Status drop-down select **Excluded**. The Add Exclude Range window opens.
- 5 From the drop-down list, select an **Address Block**.
- 6 In the IP Address field, enter the **IP** that will be excluded.
- 7 Enter the **CIDR**.
- 8 Optionally, enter a **Subnet** if needed.
- 9 When finished, click **OK**. The Add Exclude Range window closes. The Manage Address Usages window updates.

### Pack IP Address Pool Usage

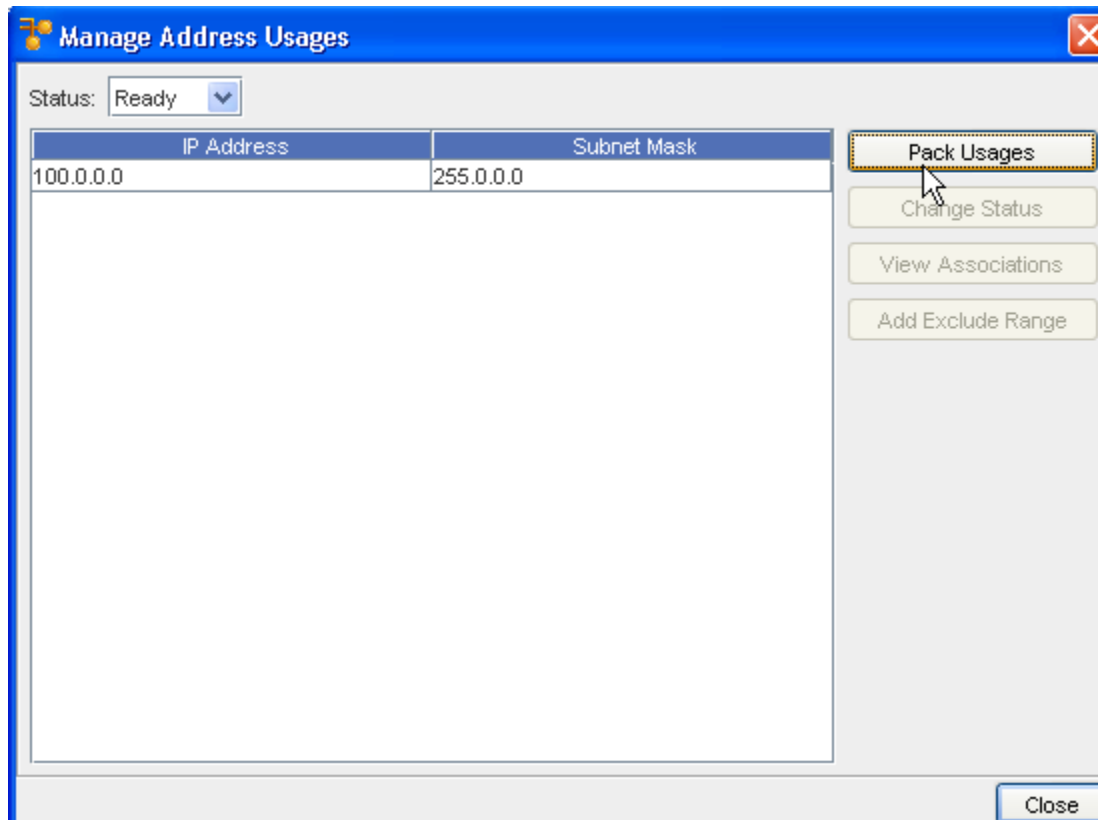
The Pack Usages feature activates a system review of devices to summarize the use of the IP address. Once summarized, the other options are updated with current IP address details on each device.

To access and use the Pack IP Address Pool Usage,

- 1 From the menu bar, select **Tools -> System Administration** .
- 2 Next, select **Network -> Address Pool**. The Address Pools List window opens. All existing IP Address Pools are listed.



- 3 Next, click **Manage Usages**.
- 4 Click **Pack Usages** . From here, you can then use the Pack feature to allocate, or re-allocate IP addresses as requested.



### Removing an IP Address Pool

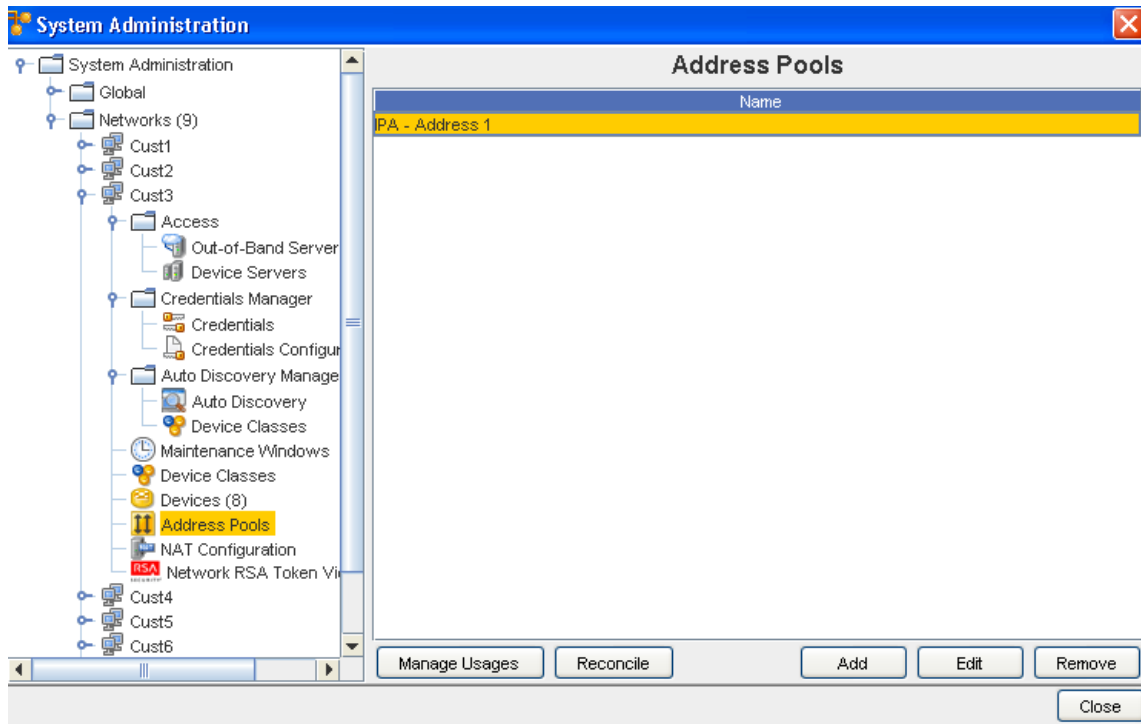
**Note** This feature is also available using the API.

IP address blocks can be deleted when they are no longer useful to the network. When deleting address blocks, all IP addresses defined for the block are also deleted.

To delete Address blocks defined for a network,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Address Pools**. The Address Pools List window opens. All existing IP Address Pools are listed.
- 3 Select the IP Address block that needs to be removed.





**Note** For added integrity, address blocks can only be deleted one at a time.

- 4 Click **Remove**.
- 5 At the Confirm message, click **Yes** to continue and remove this Address Pool. Note the information within the confirmation message. Click **No** to cancel this removal action.

## Networks - NAT Configuration

### NAT Configuration - Overriding Device Server IPs

Network Address Translation (NAT) configuration allows both the System Administrator and the Network Administrator to define an IP address for each Device Server to **override** the existing IP address of that Device Server.

- 1 From the menu tool bar, select **Tools**, then **System Administration**.
- 2 Expand the **Network** section, and go to **NAT Configuration**.

### Network-Specific NAT Setup

Administrators can define an IP address for each Device Server within a network that will then be the **Device Server IP Address** for that network.

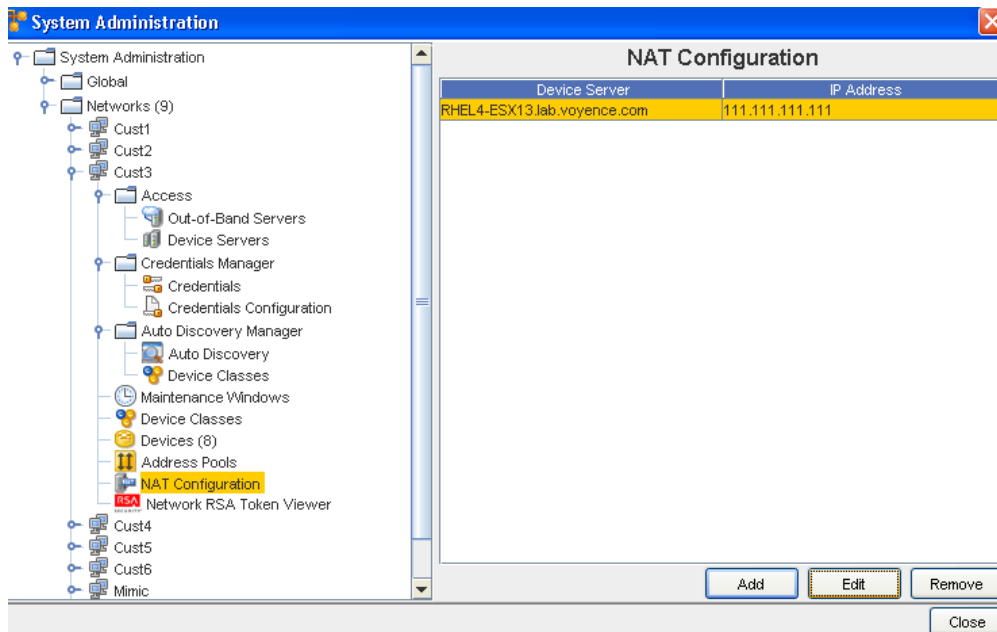
**Note** Only One IP Address is allowed for each Network-Device Server combination.

The new IP Address then affects all devices that consider that network to be the "primary" network. The new IP Address will be the address the Server uses to communicate to the devices.

For example, in a Telnet/TFTP managed device, when the Network Configuration Manager Device Server telnets to the device, it sends the configured NAT IP address needed for the device to TFTP to its configuration. This is used for any communication originating from the device back to the Device Server, including event-based pulls (which is also cached on the device server).

To add a NAT IP Address,

- 1 From the NAT Configuration window, select a **Device Server** from the listing, then click **Add**.
- 2 At the Add NAT IP window, select a **Device Server** from the options shown in the drop-down arrow.
- 3 Enter the **NAT IP Address** you want to use to for the selected Device Server.
- 4 Click **Ok** when you have entered the IP Address. You can also use Cancel to leave this window without saving any new text.



### Additional Tasks - Editing and Removing NAT IPs

- You can Select to **Edit** any existing Device Servers in the NAT Configuration window by first selecting the Device Server from the list, clicking **Edit**, then making the needed IP Address changes. Once your changes are make, click **Ok**.
- To **remove** (delete) existing Device Servers from the list in the NAT Configuration widow, first select the Device Server, then click **Remove**. At the confirmation window, select **Yes**.

## Device-Specific NAT Setup

A Network Administrator can **override** the Device Server IP Address for a specific device. This can be completed using two Quick Commands.

- **View NAT Setup** : View NAT Setup shows only device-specific Device Server NAT IP, and not the network-wide NAT setting.
- **Setup NAT** : If there is no IP Address provided at the time of Setup, the existing setup is to be cleaned. This is provided as a method of re-setting a previous configuration (if any exists). If the device override is set, then that server address is used, regardless of any other configuration setting.

To setup a Device-Specific NAT - from the Devices View,

- 1 From the **Devices View**, select a device with an existing Device Server IP Address that you want to override.

State	Device Name	IP	Device Class
	Switch	172.22.2.73	Cisco IOS Switch
	Nortel-450	172.22.2.80	Nortel Baystack
	<b>VPN-3000-2</b>		<b>Cisco VPN Con...</b>
	Cat190		Cisco CatOS S...
	lansw	Compliance Audit...	Alcatel OmniSw...
	netvar	Enforce Policy	Adtran NetVanta
	Lab-4	Cut-Through ▶	Nortel BoSS Sw...
	Tasma	Editor ▶	Tasman Router
	Adtran	Edit Device ▶	Adtran NetVant...
	LAB-4	Pull ▶	Nortel Baystack
	ASN-1	Quick Commands ▶	Nortel Router
	netvar	Saved Commands	Test Credentials
	350t	Save To...	Setup NAT
	Passp	Update OS Image	View NAT Setup
	Nortel-	Wizards ▶	OSUpgrade
	NetVa	Navigations ▶	Clear Cache
	Tasma	Compare Configs	Cisco PIX
	pix1	Properties	Nortel BoSS Sw...
	bps20		Cisco VPN Con...
	Cisco3		Cisco IOS Router
	r1841-		Tasman Router

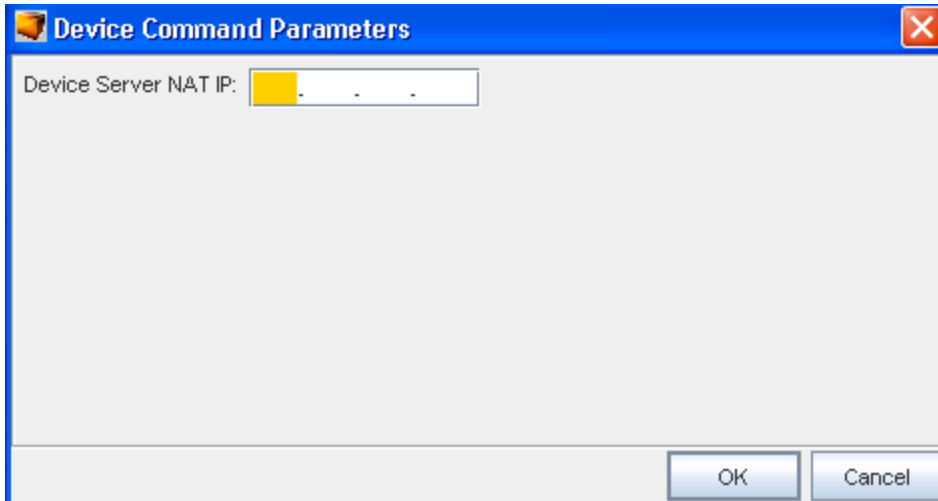
- 2 **Right-click** on the selected device to view the right-click options, then select **Quick Commands** from the list. Now, select **Setup NAT** from the Quick Commands list.

---

**Note** You can also select **View NAT Setup** from this Quick Commands option.

---

The Device Command Parameters window now displays.

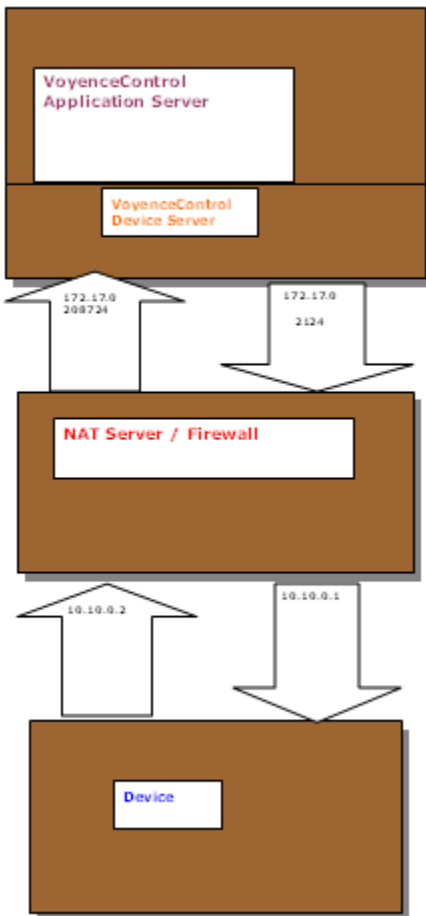


3 Enter the **Device Server NAT IP Address** into the field provided, then click **OK**.

Review the [NAT Setup - Example](#).

### NAT Setup - Example

Following is an example of a Network Address Translation (NAT) setup.



## Network - RSA Token Viewer

### RSA Tokens Overview

RSA tokens provide a means to allow users **two-factor authentication** access to the Network Configuration Manager application. RSA SecurID<sup>®</sup> two-factor authentication is based on something you know (a password or PIN), and something you have (an authenticator), providing a much more reliable level of user authentication than reusable passwords.

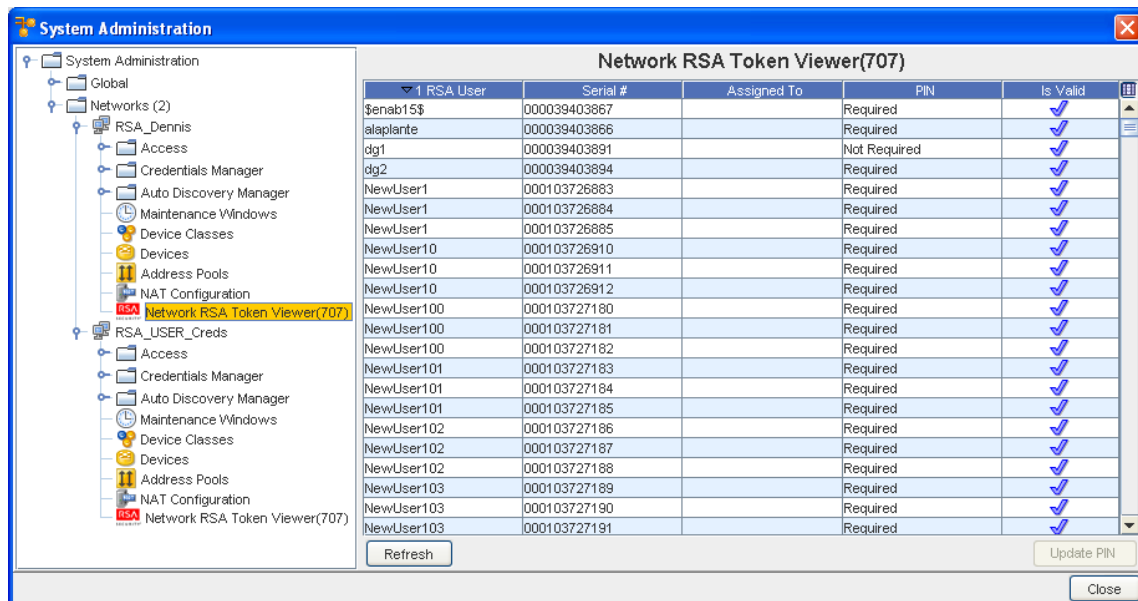
In addition, for additional user security, a lock out feature is available. To limit the number of attempts a user can try to access Network Configuration Manager, you can use this feature. For more information, see [User Lock Out Security](#)

### Network RSA Token Viewer

The Network RSA Token Viewer window allows organizations to view associated devices for an RSA Token and reset the PIN associated with an RSA token.

Using the Network RSA Token Viewer Window

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Networks**.
- 3 Select an available network.
- 4 Select **Network RSA Token Viewer**.



Updating the PIN for an RSA Token from the Network RSA Token Viewer Window:

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Networks**.
- 3 Select an available network.
- 4 Select **Network RSA Token Viewer**.
- 5 At the bottom of the Network RSA Token Viewer pane, select **Reset PIN**.
- 6 A confirmation box opens. Click **Yes** to confirm the PIN reset.

## Working with Networks

### Networks Overview

Network configuration is the "backbone" of the tool. A properly configured network speeds productivity when sending changes to multiple devices on the network.

Networks are completely configurable by adding and removing devices. Regardless of the size of a network, the focus is on *ease of management*. Management of large networks is aided by the use of **Sites** and **Views**. Using these two features allows you to either create a hierarchical site construct, or to create user-defined views of specific devices.

By taking advantage of the access controls, you are able to dictate who and how networks are accessed. While the access to networks is provided by assigning users or groups to networks, further enhancements allow you to provide security at not only the network level, but the device level as well.

Network level permissions are setup in the **Access Control Administration** window. When users are created, they can be provided permissions to networks individually, where permissions are defined specific to the user, or assigned to a group, where the same permissions are granted for each user within the group.

When creating networks, you may want to use the following steps (in sequence):

- 1 Associate Device Servers
- 2 Schedule and Run Auto Discovery
- 3 Create Users and Groups
- 4 Set User/Group Permissions
- 5 Assign Users and Groups to Network
- 6 After Auto Discovery, Manage Devices to Networks
- 7 Set Network Credentials

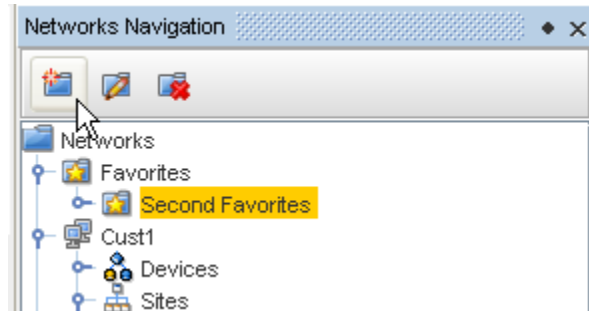
Once you have completed these steps (in sequence), the network can be accessed by other users or groups.

The **Network area** is where you:

- Manage networks
- Create auto discovery jobs
- Manage device level credentials and communications

### Managing Network Folders

From the Network Navigation view, you can use the icons to Add a New Folder to the Network, Edit an existing Folder Name, or Delete a Folder from the Network.

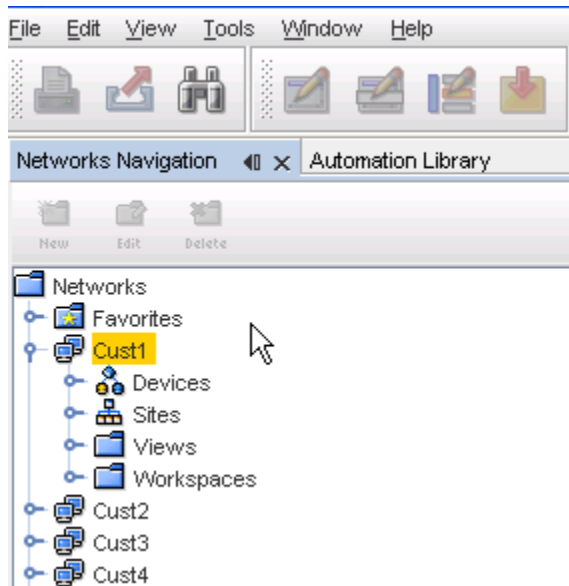


- [Working with Networks](#)
- [Creating Networks](#)
- [About Network Properties](#)
- [The Dashboard](#)
- [Assigning Device Servers](#)
- [Scheduling Auto Discovery Jobs](#)
- [Creating Users](#)
- [Setting Network Level Permissions](#)
- [Auto Discovery Overview](#)
- [Setting Network Level Credentials](#)

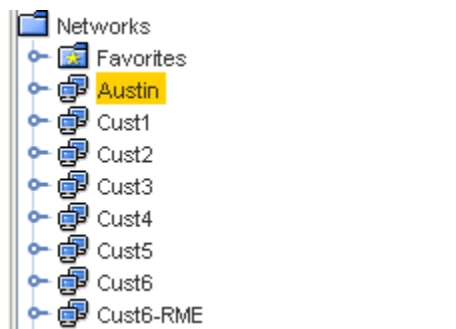
## Working with Networks

To work with Networks, you must first select **Networks Navigation** from **Tools** on the menu bar.

Once Networks Navigation is selected, your existing Networks are listed. For example, the Networks Cust1, Cust2, Cust3, and Cust4 are listed. Notice also that the Devices, Sites, Views, and Workspaces are also displayed. These options are offered for each Network.



Within Network Configuration Manager, a **Network** is defined as a logical partitioning of the devices that are in a physical network. A network is also often times referred to as a "container".



- Networks can be created to best model your business environment. For example, networks can be created and defined by customer, region, subsidiary, or responsibility; for example, corporate vs. division.
- Within networks, devices can be further organized logically and physically. In addition, you can design and stage modifications to the devices in user-defined workspaces.
- Networks, when created, contain basic information about the network (name, description and domain).
- The content of a network is determined by selecting devices that are housed on the devices servers. Once selected, these devices make up a network.
- Depending on the size of the network, Network Configuration Manager has included two interfaces for viewing a network; Table and Diagram layout.

A network is a container that groups the following:

Feature	Description
Devices	A specialized view that contains all network devices



<b>Sites</b>	A hierarchical structure that allows physical segmentation of devices. Sites are viewed and updated in the Site view of a network by authorized users only. Sites uses locations to reference the devices network organization. For example, geography, building, and rooms.
<b>Views</b>	A folder containing user-defined views. Views contain user-defined groupings of operational network devices
<b>Workspaces</b>	A folder containing user-defined workspaces. Workspaces are "sandboxes" for storing and staging device configuration changes, and can be used for design and complex changes

Extremely large networks, even when arranged in manageable sites, can become unmanageable. With this in mind, there are several filtering options that have been included that allow you to filter what is seen in the interface you are using and segmenting options (views and sites).

For information on creating new networks, see [Creating Networks](#).

**Note** Networks can only be created by users who have adequate permissions. If you are unable to create a network, contact your System Administrator.

- [About Network Properties](#)
- [Workspaces Overview](#)
- [How Sites and Views Work](#)
- [Favorites Overview](#)

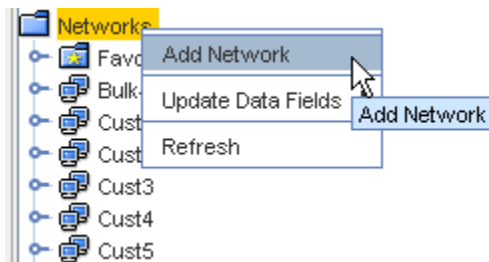
## Creating a New Network

Networks are created to hold devices. A network can contain a single Site, with an unlimited number of Views and Workspaces with any configuration.

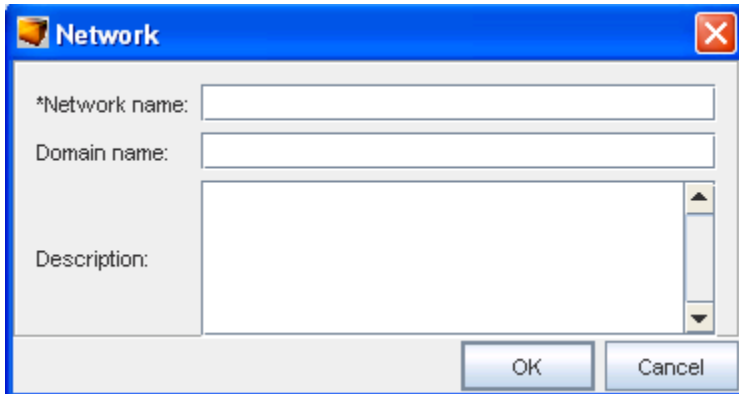
**Note** Sites, Views, and Workspaces are not required for your network, but are added to allow you to segment your network into manageable portions.

To create a Network,

- 1 At the navigation pane, right-click the **Networks** folder.
- 2 Select **Add Network** from the options .



The network window opens.



3 In the Network window, enter the following:

- Network Name
- Domain Name (optional)
- Description (optional)

4 Click **Ok**. Now, notice the new Network is now listed under Networks in the navigation pane.

Now that the Network is created, you can complete the following tasks:

- [Creating the Site Hierarchy](#)
- [Creating Views](#)
- [Creating Workspaces](#)

---

**Important** Use the **Refresh** option to refresh the network information when you have created or added information to the network.

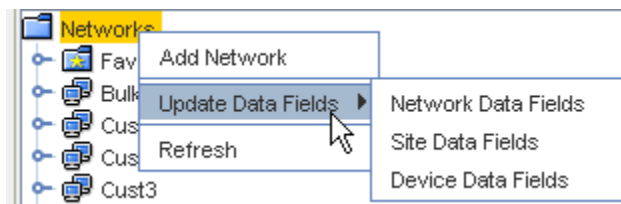
---

## Update Data Fields

From the Networks right-click options, you can select Update Data Fields to update the Network, Site or Device existing Data Fields.

**Note** Data Fields are used to create attributes, and to assign values to devices. You must **first** have added data fields to a Network, Site or Device before you can update them. For information on adding Data Fields, click [Adding a Data Field](#)

---



From this option, you can select to update the following:

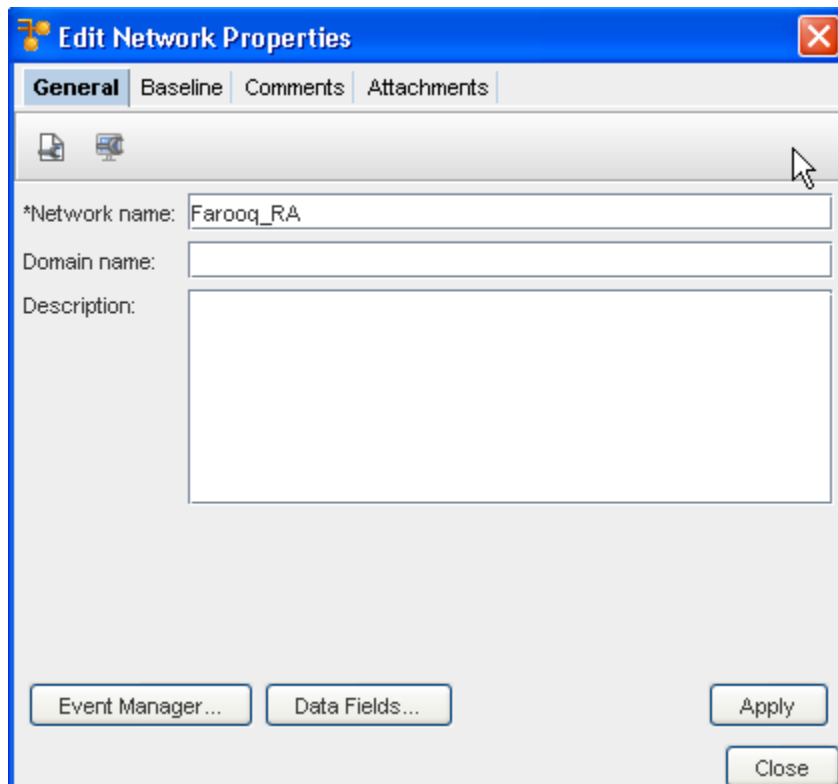
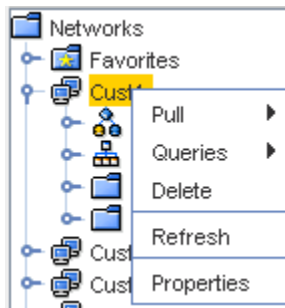
- Network Data Fields

- Site Data Fields
- Device Data Fields

## About Network Properties

When networks are created, basic information about the network is entered. After creation, additional information can be entered.

- 1 View this information by selecting a **Network** from the Networks Navigation Pane.
- 2 Next, right-click on the Network name, and select **Properties**.



There are four tabs of information that can be entered regarding network **Properties**:

- The General Tab
- The Baseline Tab

- [The Comments Tab](#)
- [The Attachments Tab](#)

Additional options on the Edit Network **Properties General tab** include:

- **Event Manager** - when selected it takes you to the Event Manager feature
- **Data Fields** - click this to get the latest view including any recent changes
- **Apply** - click this to apply and save all your edit changes.

---

**Note** Clicking **Close** at the bottom of each window (while in any tab) closes the Edit Network Properties window. If you have information to be entered on more than one tab, click each tab and save according to the provided instructions.

---



## The General Tab

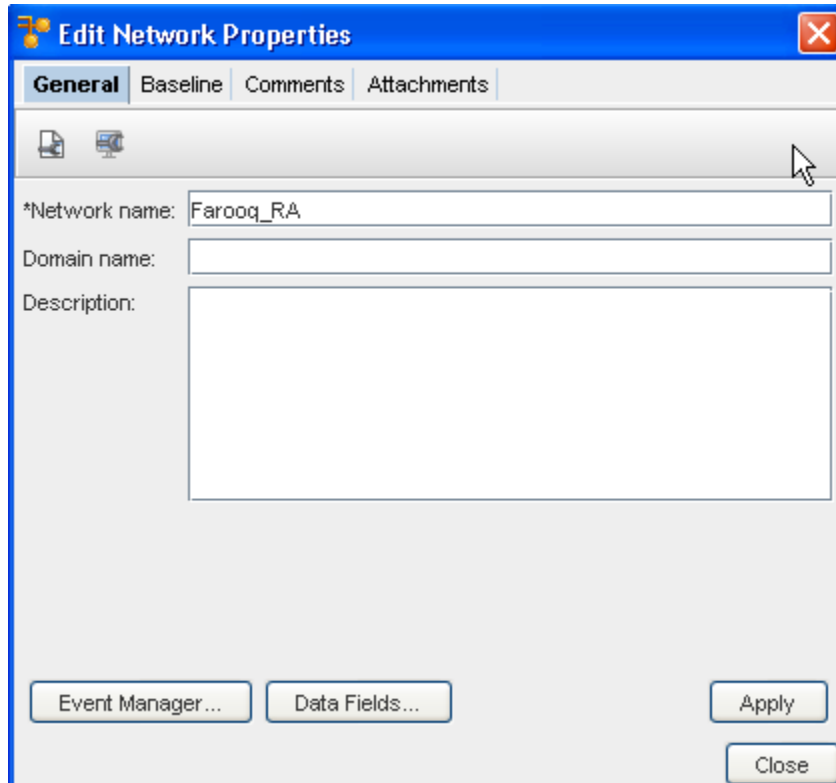
The **General** Tab contains the basic information that was initially entered when the network was created.

- Network Name - Name the network is referred to in Network Configuration Manager
- Domain Name - For example: customer.com
- Description - Information about the network and it's devices

All fields on the General tab can be edited. Only the Network name is required. The Network name is used to identify the network in the Networks Navigation pane.

The General tab also provides access to the following:

-  [Scheduling Network Level Config and Hardware Spec Pull Jobs](#)
-  [Scheduling Network Level Config and Hardware Spec Pull Jobs](#)



To edit or change information in this tab if needed,

- 1 Change the existing **Network Name**.
- 2 Change the **Domain Name**.
- 3 Change the **Description**, then click **Apply** and **Close**.

---

**Note** You can access the [Event Manager Overview](#) as well as Data Fields from the General tab.

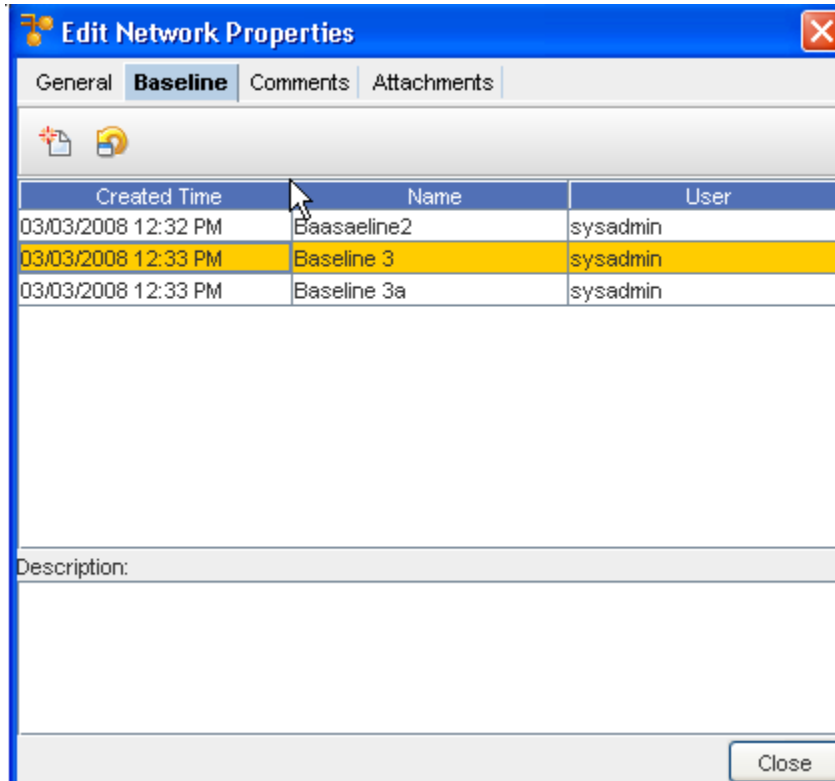
---

## The Baseline Tab

The Network **Baseline** tab allows you to tag all current configuration revisions for the network devices as a **baseline** for future comparisons. Baselines are helpful when you would like to maintain a consistent production collection of configs for your network devices.

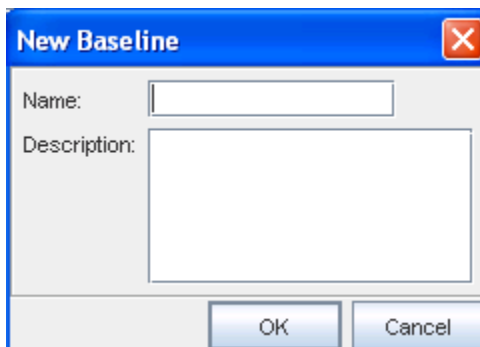
Once set at the Network level, a baseline can be reviewed by device, and a configuration rollback scheduled, if a change occurs on a device.

A baseline snapshot can be updated at any time. To review a device baseline, see the section on the [Baseline Tab Overview](#).



To create a baseline,

- 1 On the Baseline tab, click the **New**  icon. The New Baseline dialog window opens.

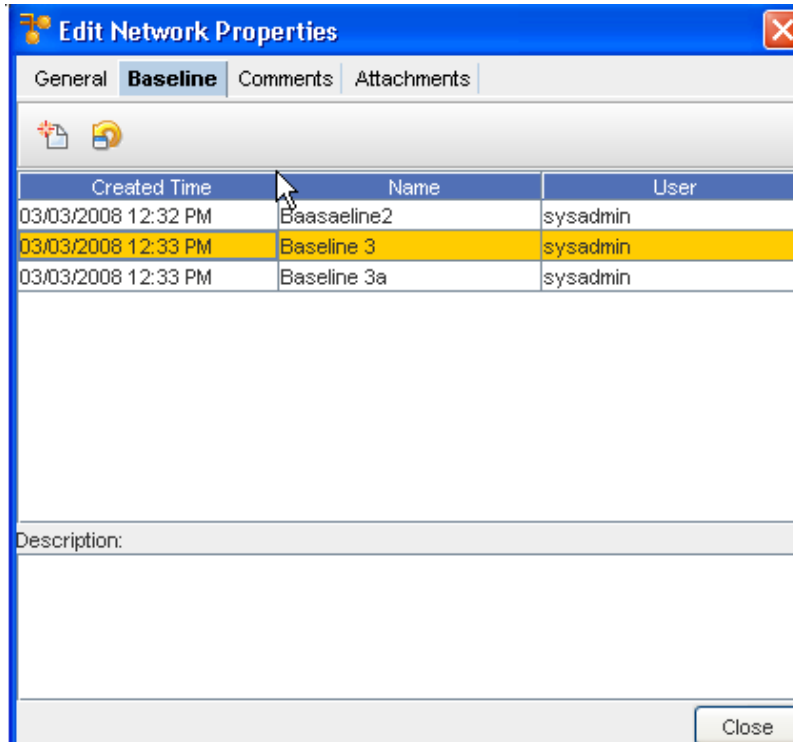


- 2 Enter a **Name** for the baseline. The name of the baseline should be reflective of the network configuration.
- 3 If the baseline name does not convey intuitive information about the network, enter a **Description**.
- 4 Click **OK**. The New Baseline window closes. The baseline is added to the Network Properties window. At this point, all device configurations are marked as part of the baseline configs.

To Rollback to the Baseline,

**Important** You can now **rollback any/all devices** that have a new and different configuration revision than the configuration revision that previously existed at the baseline. You can access this feature using the **Rollback icon**.

From this window, you can roll back to the baseline - back to the beginning.



- 1 Select the Baseline, then click the **Roll Back** icon to display the Schedule Rollback Job window.

- 2 Complete the information needed in the **Job Details** section of this window, including selecting a **priority** from the drop-down arrow.
- 3 Next, schedule a time in the **Schedule Job** portion of the window.
- 4 Schedule the users you want notification of this job to go to accessing the **Notification tab**.

---

**Important** For more information, go to [Using the Scheduler](#).

---

- 5 After making your revisions, or adding additional information, click **Submit**. This starts your job in the process, with the revisions.
- 6 You can now **Close** the Edit Network Properties window.

---

**Note** You can click **Approve & Submit** if you have the appropriate permissions.

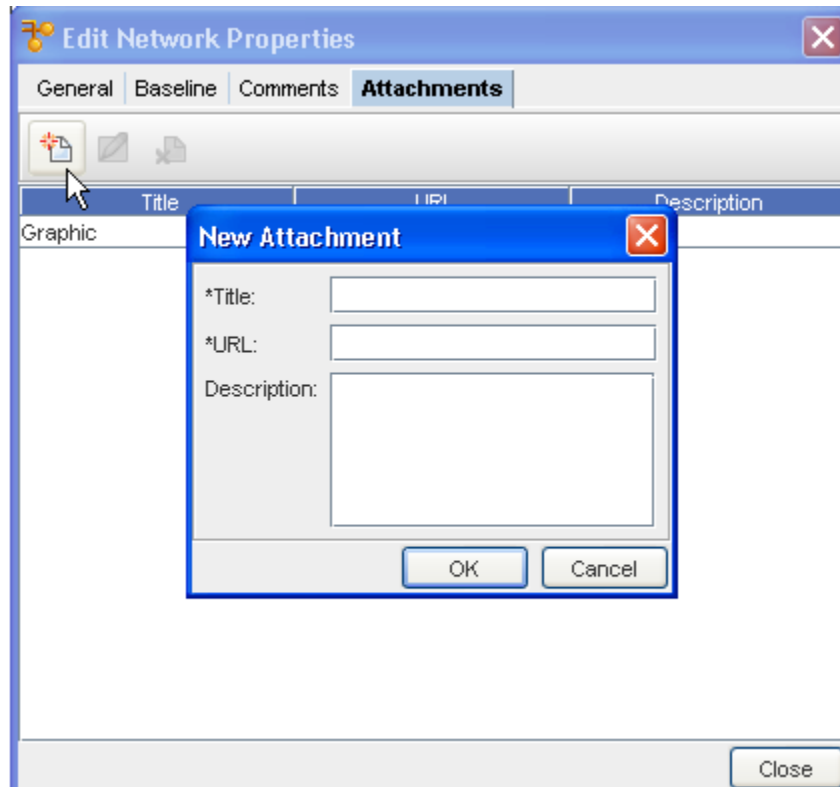
---


## The Comments Tab

The **Comments** tab contains a running list of comments, related to the Network, its devices, or other components. The comments are logged as they are entered. Each comment includes a header with the author's name, and the date the comment was created. Comments are separated by a series of dashed lines.

To create a comment,

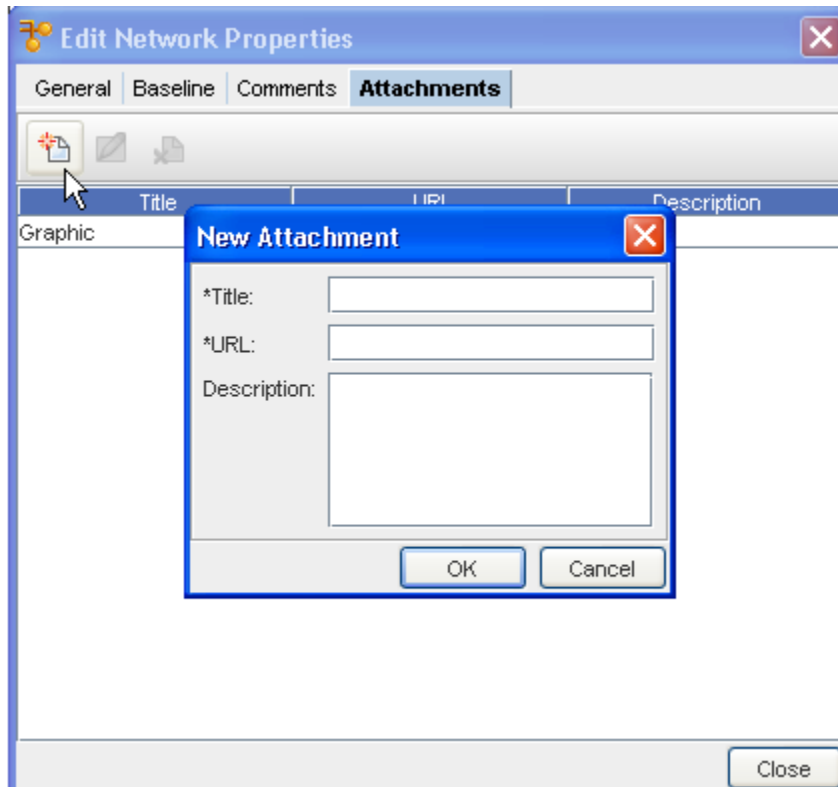




- 1 On the Comments tab, click the **New**  icon. The New Comment dialog window opens.
- 2 Enter **comments**. The Enter key can be used to create paragraph breaks while you are entering your comments.
- 3 Click **OK**. The New Comments window closes. Each new comment is added at the top.
- 4 For each additional comment, repeat **steps 1-3**.
- 5 Click **Close** when you are finished entering comments.

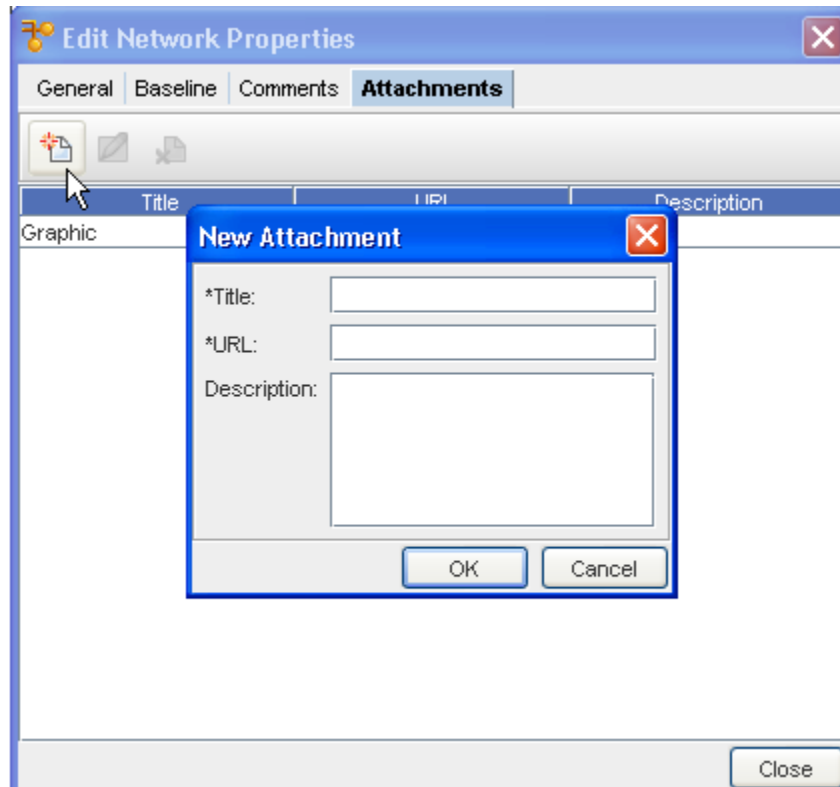
## The Attachments Tab

The **Attachments** tab allows you to associate an **external file to the site** . This can include worksheets, documents, or .html files. Any document that can be opened in a web browser can be mapped as an attachment. Multiple attachments can be added to each site.



- 1 Click the **New** icon, and then enter as **many attachments** as needed.
- 2 Click **Close** when you are finished adding attachments.

## Adding an Attachment



To add an attachment,

- 1 On the **Attachments** tab, click the **New icon**. The New Attachments dialog window opens.
- 2 Enter a title **for the attachment** .
- 3 Enter a **URL**. Remember, the document must be saved in a format that will open in a browser.
- 4 If needed, enter a **description**.
- 5 Click **OK**. The New Attachments window closes.
- 6 For each new attachment, repeat **steps 1-5**.
- 7 Click **Close** when you are finished adding attachments.

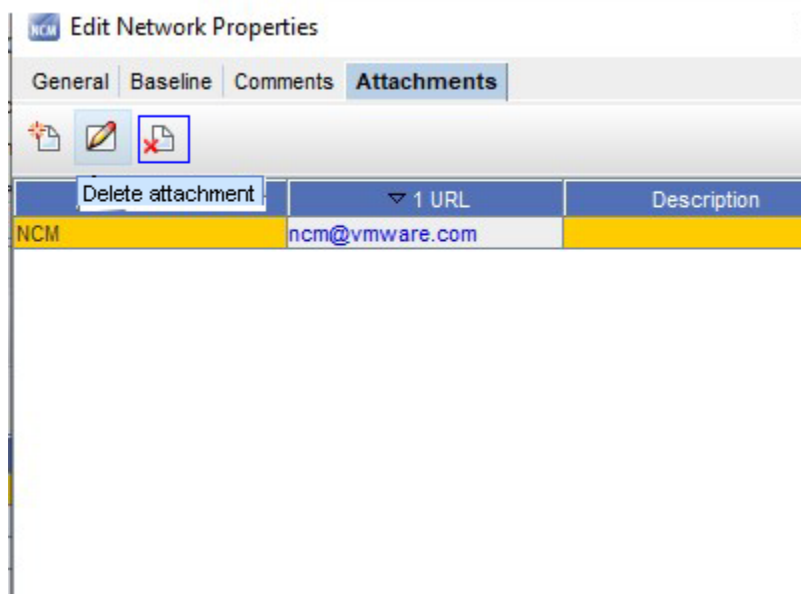
---

**Note** The Edit and Delete icons are only active when one or more attachments have previously been created.

---

## Deleting an Attachment

When deleting an attachment, the actual document that you are referring to is **not** deleted. You are removing its linked reference from Network Configuration Manager.





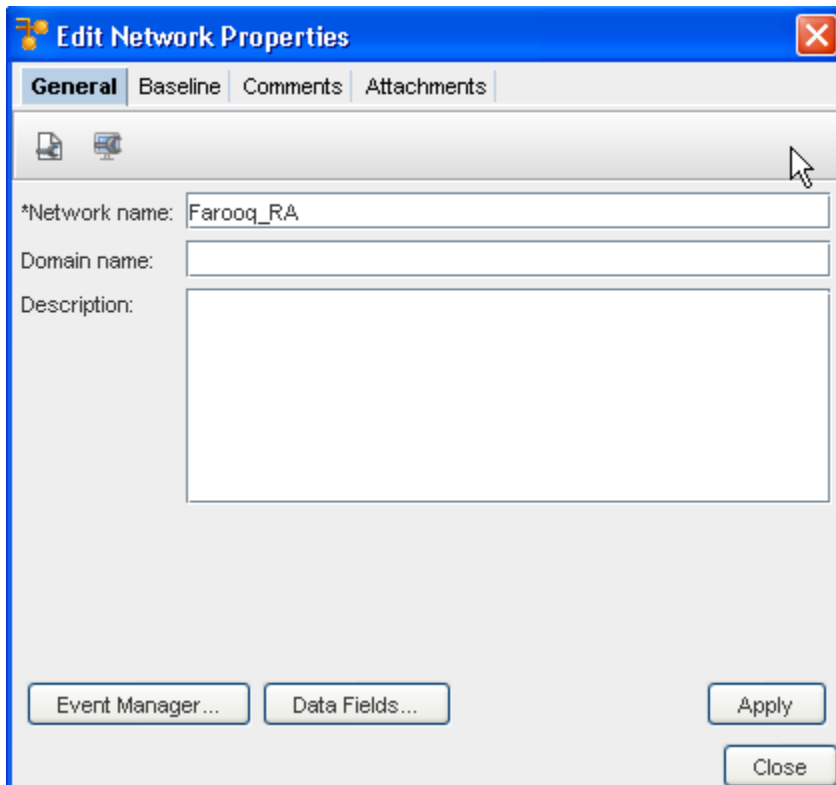
- 1 First, select an attachment from the list of attachments.
- 2 On the Attachments tab, click the **Delete** icon. The Confirm dialog window opens asking, "Are you sure?".
- 3 To delete, click **Yes**.
- 4 Click **OK**. The Confirm window closes. The Attachment tab refreshes.
- 5 Click **Close** when you are finished deleting attachments from the list.

## Scheduling Network Level Config and Hardware Spec Pull Jobs

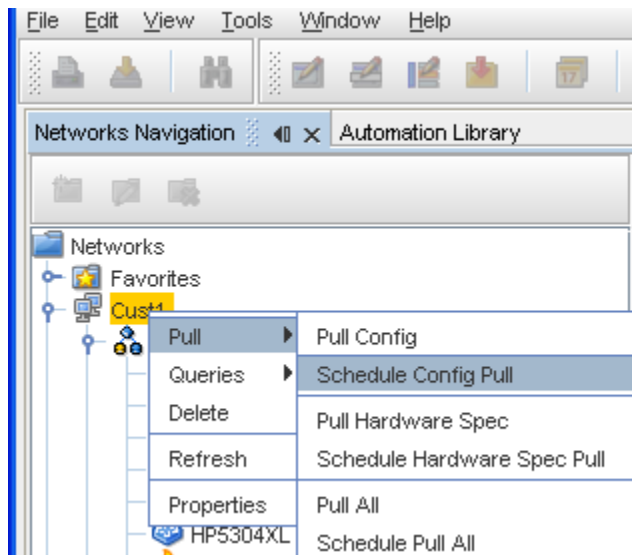
- Pulling of **Network and Hardware configurations** in this manner is typically completed when you do not have SNMP trap or syslogging enabled for devices.
- A Network level config pull job pulls all devices and updates your current Network configuration with any changes that have occurred since the last pull.
- A Network level hardware pull job polls each device and updates all hardware details. Hardware information is also revisioned.
- Both types of pull jobs use the Schedule Job window, and allow you to send email updates to other users (external and internal) who need to be notified on the status of the pull jobs (through the Notification tab)

There are two ways to access this feature:

- 1 On the **Network Properties** window, click the **Config**  or **Hardware**  Polling Jobs icons.



- 2 In the Networks Navigation Pane, right-click on the **N e twork** name, select **Pull**, then select **Schedule Config Pull** .



The pulling of network and hardware configurations is typically used when a customer *does not* have SNMP trap or syslog capabilities. Setting up a **recurring pulling** of the network allows you to have the most current network information on a set schedule.

- A **Network Level Config Pull Job** polls all network devices, and updates your current network configuration with any changes that have occurred.

- A **Network Level Hardware Pull Job** polls all network devices, and updates all hardware details.

**Important** For more information scheduling jobs, see [Using the Scheduler](#).

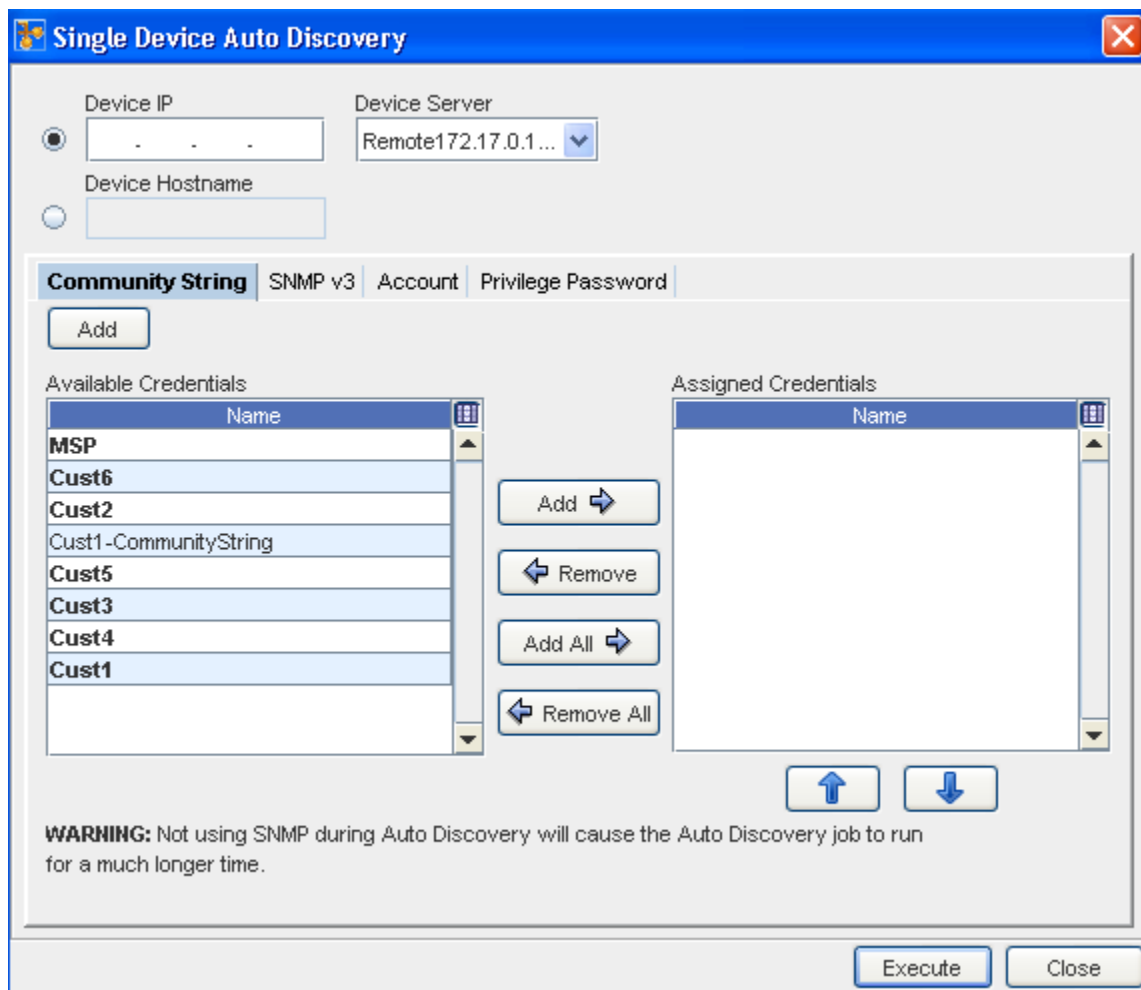
## Single Device Auto Discovery

Single Device Auto Discovery provides you with the ability to discover a single device from the Edit menu within a Network. This eliminates the need to access System Administration to manage newly deployed devices. You only have to enter the Management IP Address of the device to be discovered, complete the remaining options in the window and tabs, then Execute. The Scheduler Job window is bypassed for a Single Auto Discovery task.

While in the Devices view, you can select **Edit** from the menu bar, and then go to the **Single Device Auto Discovery**, to run an Auto Discovery job on a single Device.

- 1 From the menu bar, select **Edit** -> **Single Device Auto Discovery**.

The Single Device Auto Discovery window opens.



**Single Device Auto Discovery**

Device IP:  . . .

Device Hostname:

Device Server: Remote172.17.0.1...

Community String | SNMP v3 | Account | Privilege Password

Add

Available Credentials

Name
MSP
Cust6
Cust2
Cust1-CommunityString
Cust5
Cust3
Cust4
Cust1

Assigned Credentials

Name
------

Add →

← Remove

Add All →

← Remove All

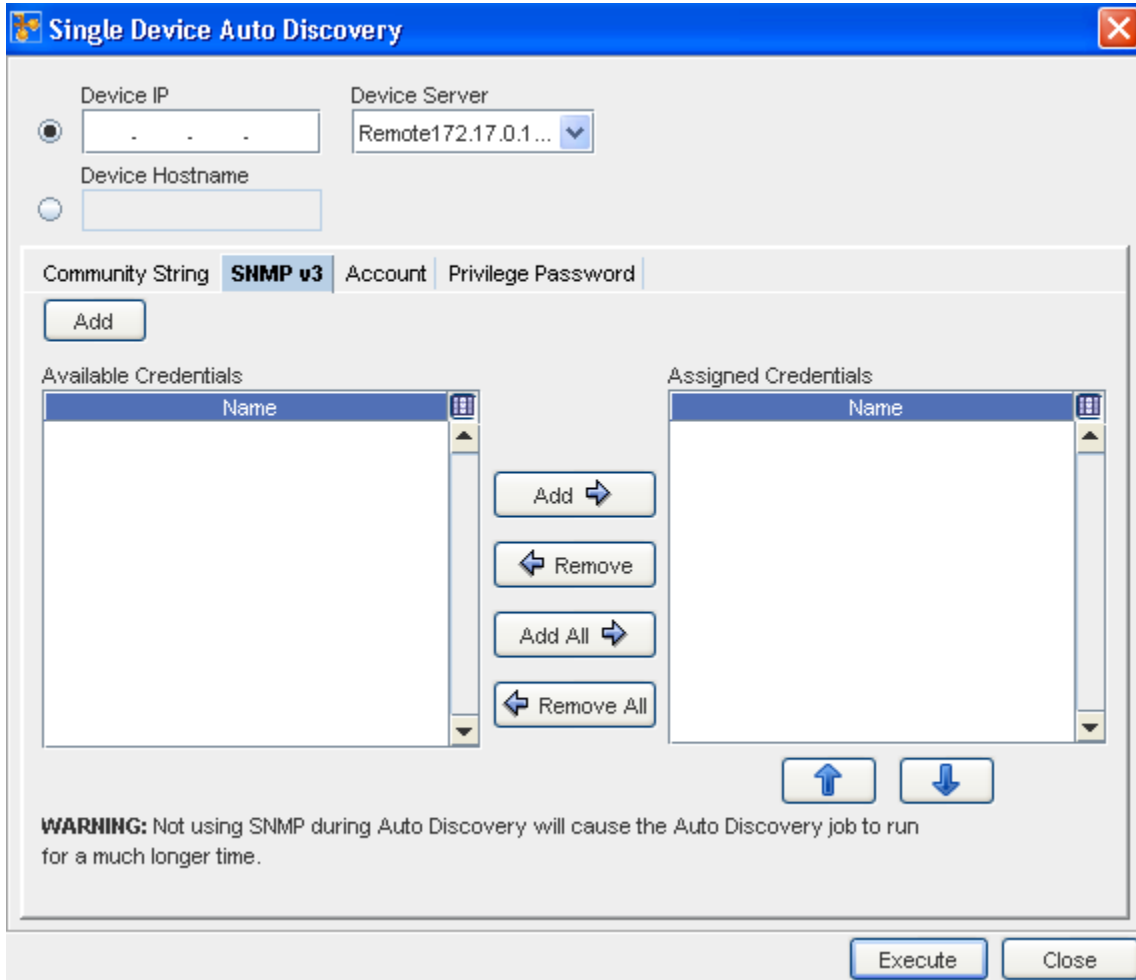
↑ ↓

**WARNING:** Not using SNMP during Auto Discovery will cause the Auto Discovery job to run for a much longer time.

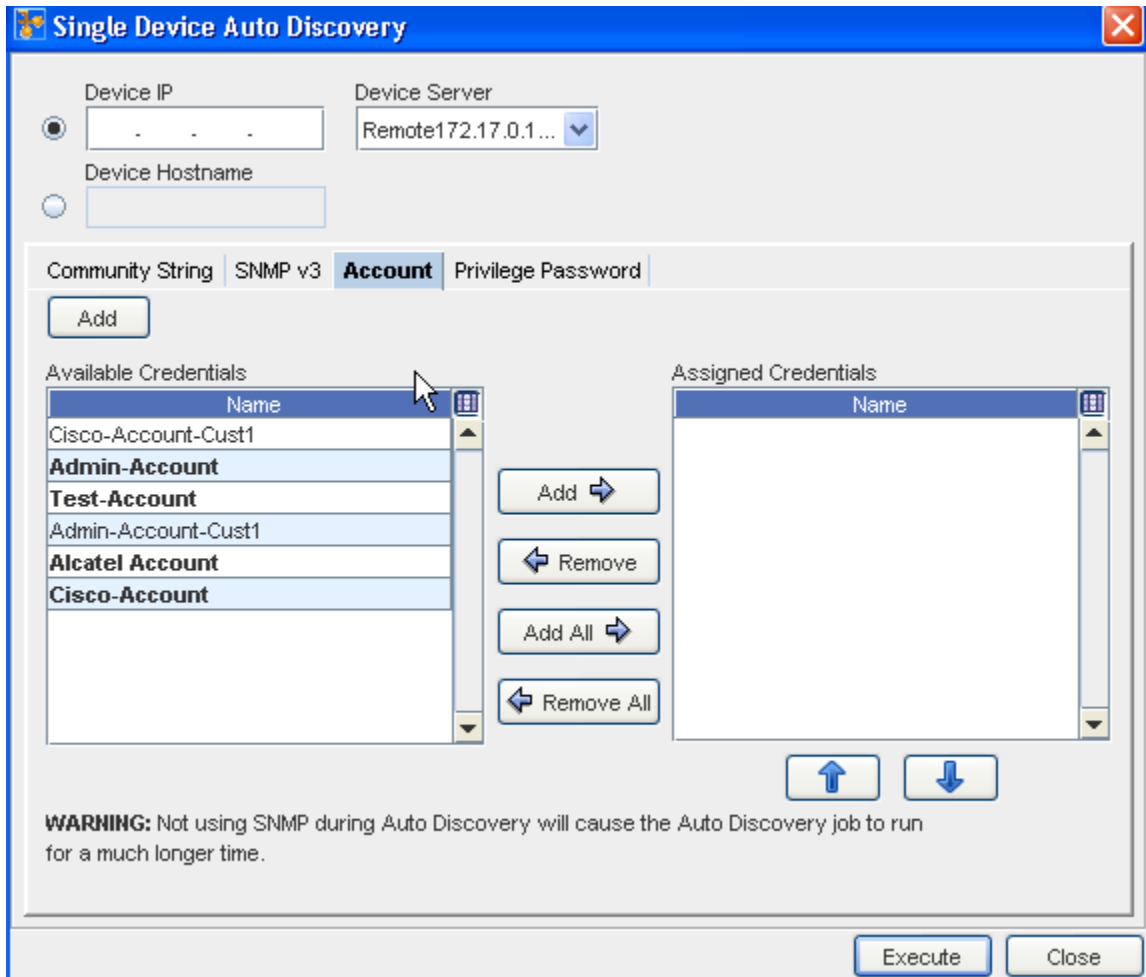
Execute Close

- 2 Enter the **Device IP Address** into the field.

- 3 Enter the **Device HostName**.
- 4 Click the **Device Server** drop-down arrow, and make a selection from the Device Server List.
- 5 In the **Community String** tab , click the **Add** button to Add a Credential, or from the list of Credentials, **Add Available Credentials** or **Remove Assigned Credentials**. As appropriate using the right arrow (->) to add Available Credentials, or use the left arrow (<-) to remove previously Assigned Credentials.
- 6 Go to the **SNMP v3** tab and make any needed additions or changes. From this tab, you can also Add or Remove credentials using the appropriate arrows.



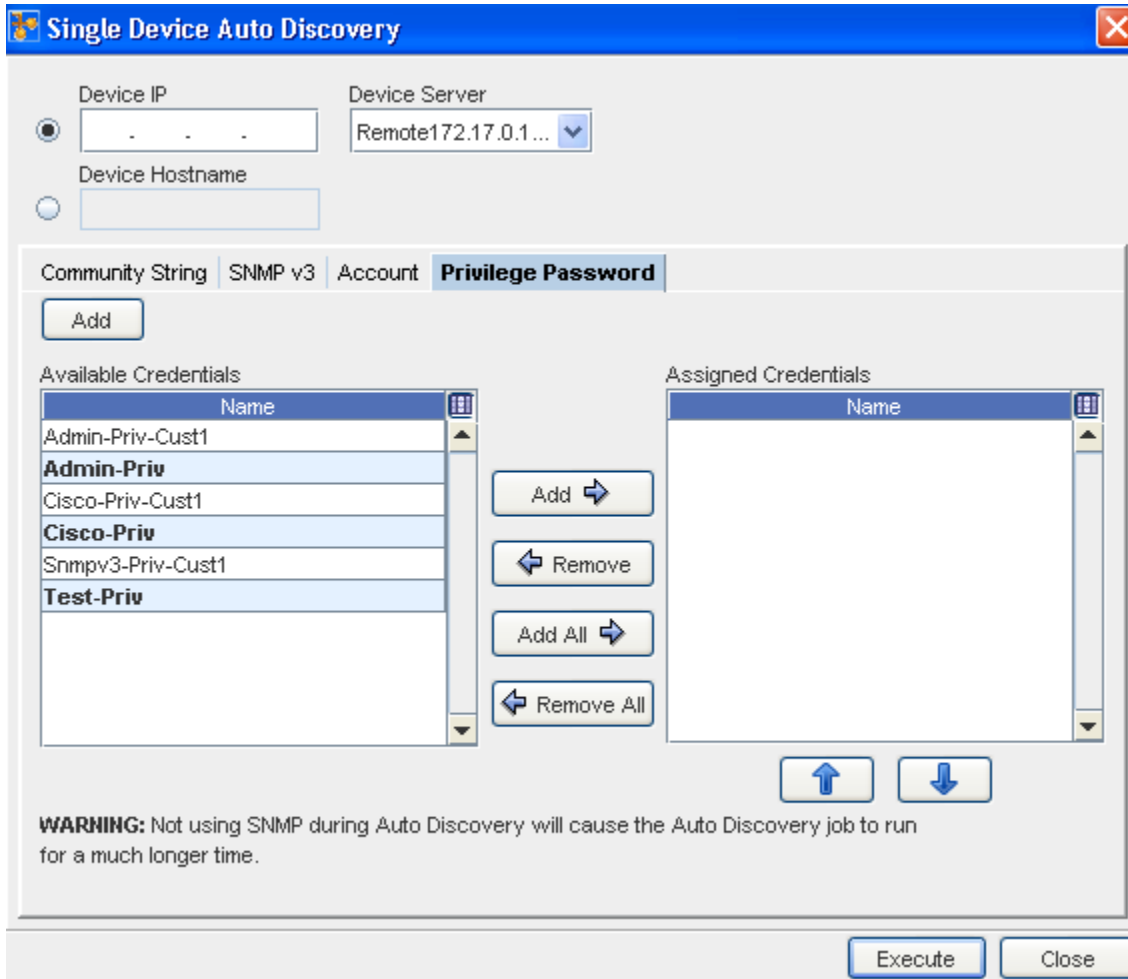
- 7 Go to the **Account** tab and make any needed additions or changes. From this tab you can also Add or Remove credentials using the arrows.



**Important** Make note of the Warning before executing the job.

- 8 Click **Execute** to run Auto Discovery on this single device. The results of the Auto Discovery are displayed.
- 9 Go to the **Privilege Password** tab and make any needed additions or changes to the credentials in the Available or Assigned panes.





10 Click **Execute** to begin the config pull.

## Scheduling Run Times

Regardless of how the Schedule Job window is accessed, the method for scheduling jobs is the same.

- All the required fields must be populated.
- Any required fields not filled generate errors until they are filled correctly.

For more information on the various settings, see [Scheduling Auto Discovery Jobs](#).

In the Schedule Job window (Job Details section),

- 1 Enter the **Job Name** .
- 2 Enter a **Description** (this is optional).

The screenshot shows the 'Schedule Job' window with a blue header. Below the header are three tabs: 'Schedule Job', 'Tasks', and 'Notification'. The 'Schedule Job' tab is active. Underneath, there is a section titled 'Job details'. It contains the following fields: 'Job Name:' with an empty text box; 'Job owner:' with the value 'sysadmin'; 'Job description:' with a large empty text area; and '\*Priority:' with a dropdown menu currently set to 'Medium'.

3 From the drop-down list, select a **Priority level**.

The screenshot shows the 'Schedule job' window. It features several radio button options: 'Run in next maintenance window', 'Run upon approval', 'Run upon operator initiation', 'Run at scheduled date/time:', and 'Run as recurring series:'. The 'Run as recurring series:' option is selected. Under this option, there are three sub-options: 'Hourly', 'Weekly', and 'Monthly', with 'Hourly' selected. The 'Start time:' field is set to 12:00 PM in the (GMT-06:00) America/Chicago time zone. The 'End Time' section has 'Never Ends' selected. The 'Interval' field is set to 'Every: 1 hour(s)'. At the bottom right, there are three buttons: 'Approve & Submit', 'Submit', and 'Cancel'.

4 At the Schedule job section, by default, all jobs are scheduled to **Run upon approval** .

**Important** All selections (in the example shown here) are displayed as being active in the schedule for viewing purposes only. All selections may not always be active. With adequate permission, you can click the Submit button located at the bottom of the window.

5 Note that you can select to have the job **Run in next maintenance** window.

6 If you select the **Run upon operator initiation** option, and Submit for approval, this keeps the job in a pending state after approval. After this, any user with Schedule permissions, can then execute this job.

- 7 To set a specific time, select **Run at scheduled date/time** . The related date and time fields activate.
- 8 Enter a **date**. For assistance, use the Calendar icon to open a monthly calendar. Select the time. The hour, minute and AM/PM setting must be designated. If this option is okay, click **Submit**.
- 9 To set a recurring schedule, select **Run as recurring series** . The recurring setting options activate.

---

**Important** When the recurring schedule is selected, the new **time zone** drop-down options are available. Make your selection from the drop-down options. The time zone you select must be the **client's time zone** . The new time zone field will be propagated with the client time zone automatically when creating a new Maintenance Window or recurring scheduled job.

---

- 10 Set the recurring options: Frequency, Start and End Times, and Time Interval. If this option is okay, click **Submit**. The job is sent to the Schedule Manager and the Schedule Job window closes.








In the Schedule Job section of the window,

The **Cancel** button takes you out of this window, and back to the previous window you opened. The job is sent to the Schedule Manager, and the Schedule Job window closes.

- To review the process of a job, see the [Schedule Manager Overview](#) .
- Once scheduling for the run is completed, go to the [Using the Notification Tab to Send an Email](#) to send email.

## Sending Email Notifications

The available states for Email notifications are:

Notification	Description
	<b>Pending Approval</b> - the scheduled job is waiting to be approved by a user with the appropriate permissions
	<b>Approved</b> - notifies the recipient when the scheduled job has been approved
	<b>Rejected</b> - notifies the recipient that the job has been rejected
	<b>Running</b> - notifies the recipient that the job is currently running
	<b>Completed</b> - notifies the recipient that the scheduled job was pushed successfully, and is completed
	<b>Completed with Warning</b> - successful push with a warning to the recipient
	<b>Partial Completion</b> - notifies the recipient that the push was only partially completed



**Failed** - notifies the recipient that the push failed without making the changes contained in the file



**Expired** - notifies the recipient that the time for the push has expired



**Hold** - notifies the recipient that the scheduled job has been placed on hold



**Deleted** - notifies the recipient that the scheduled job has been deleted

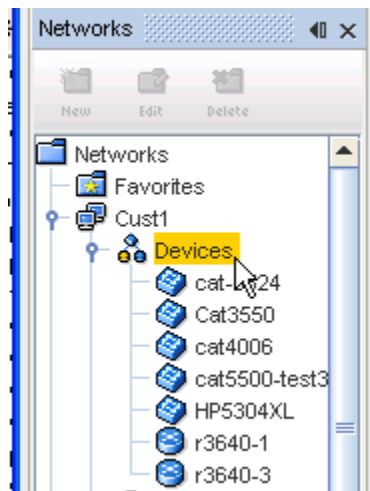
See: [Using the Notification Tab to Send an Email notifications](#) for more information.

## Working with Devices (Devices View)

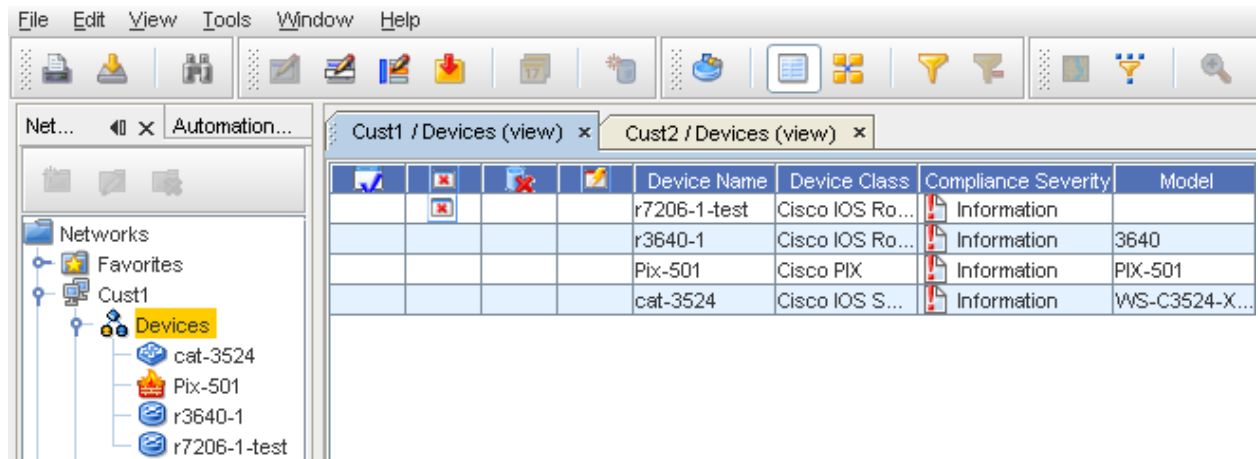
### Devices Window Overview


A **Device** can be a piece of equipment, and can also be routers, switches, firewalls, VPN concentrators, and OS images.

Access the Devices Window by selecting **Devices** from a specific Network listed in the Networks Navigation tree. The devices are displayed in the right pane. For example, the Devices within the **Cust1 network** are shown in a list.

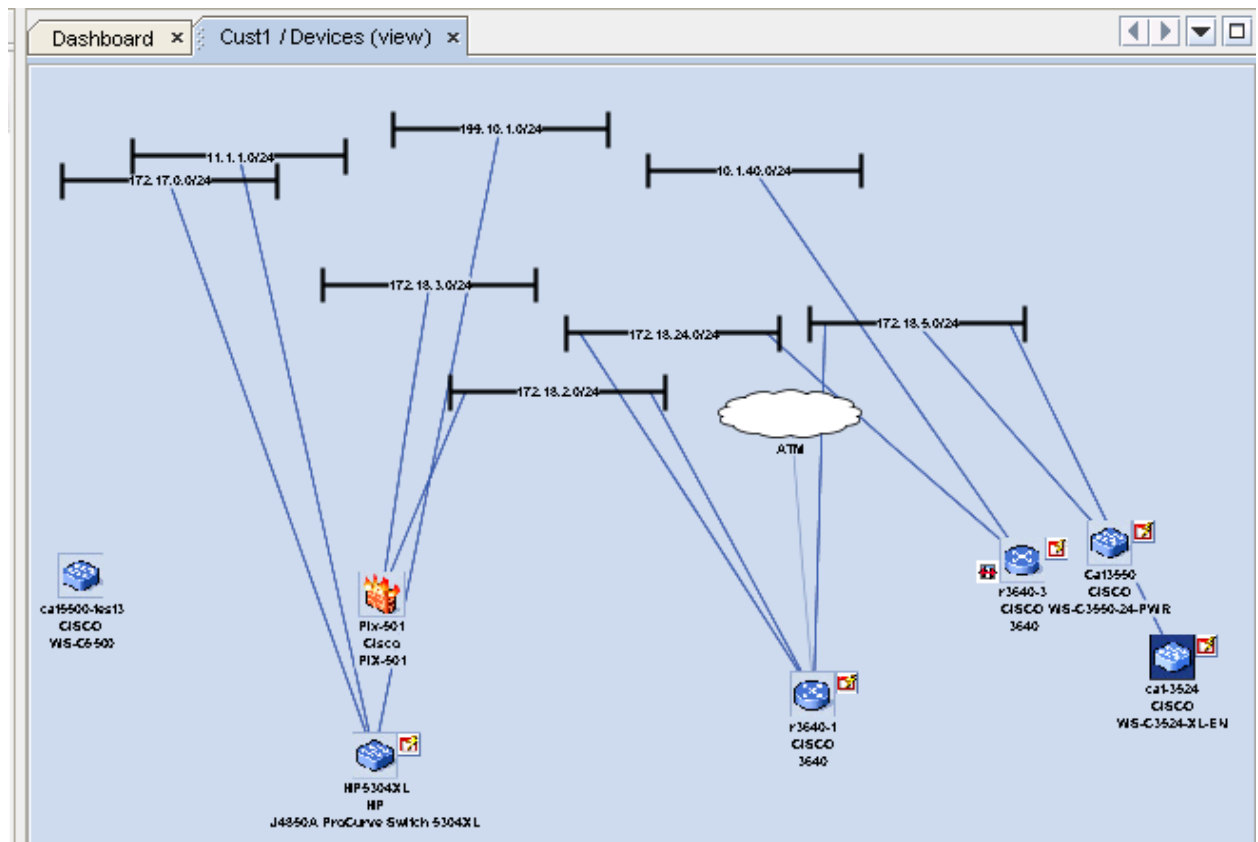


The Devices window has two interfaces you can use to monitor your networks. Each of these views is accessed by using the icons in the Devices tool menu bar. You can switch between the views.




- Table view** -  A display of all the devices in a network shown in **table format**. The table icon selection in the tool bar is used to display the devices in the table view.

**Note** Due to the large size that networks can become, when opened most Devices views default to a table view.

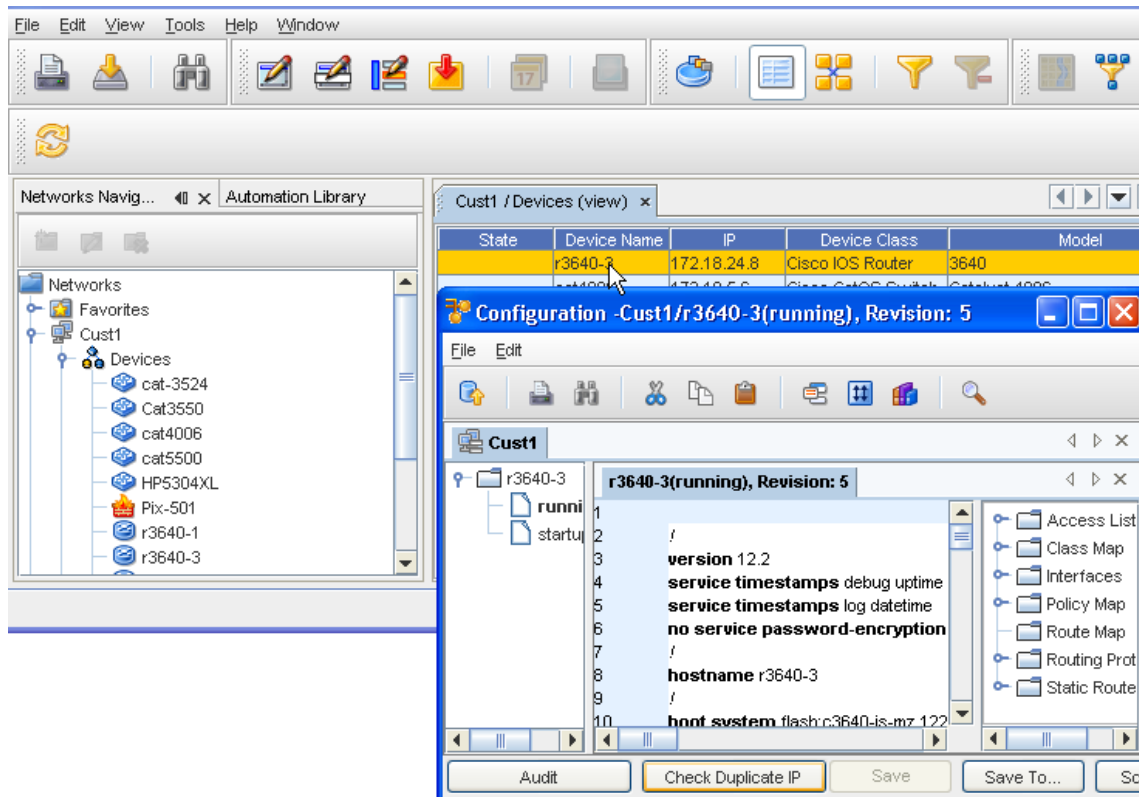


The graphical diagram for a Site, View or Workspace show the devices and their connections. Connections can be filtered by technology type, or presented as logical layer (layer 3) connections.

- 
**Diagram view** - A graphical representation of the **interconnections** of all the devices in a network. The diagram view icon selection is used to display the devices in the diagram view.

## Additional information

While viewing the devices listing in the Devices view, you can double-click the Device name, and view the **running Configuration** . For example, when the 23640-2 Device Name is double-clicked, the running Configuration for that device is displayed.





















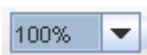


## Options on the Device View Tool Bar

Here are the options located on the **tool bar** when Devices are displayed.





The options include the following:

Icon	Icon Meaning	Action
	Print	Takes you your browser's print facility, where you can print the current view
	Export	Takes you to the Save window where you can select the location to save this view, and in what format you want to save
	Device Search	Takes you to the Device Search window where you can enter information to search on a specific device
	Config Editor	Takes you to the Config Editor. This editor is designed for editing a single, full running configuration file that affects one or more devices
	Configlet Editor	Takes you to the Configlet Editor. This editor is used to edit whole or partial configurations that are Pushed to the network.
	Interface Editor	Takes you to the Interface Editor. This editor is used to <b>make changes to multiple interfaces on multiple devices</b> - Global area
	Command Editor	Takes you to the Command Editor. The intent of the Command is not to change or update a device's configuration, although a Command can be used for this purpose. The intent is to provide access to device-level information for completing actions.
	Schedule	<b>Note</b> This feature is only available for Workspaces.
	New Virtual Device	Only available in the <b>Workspace</b> view. This allows you to create a device that can be added to a workspace for testing or creating "possible" networks.
	Properties	When accessed, the Device Properties tabs are displayed
	Table View	Displays the list of devices in a table format

Icon	Icon Meaning	Action
	Diagram View	Displays the list of devices in a diagram format. When accessed, you can switch between Diagram and Table format
	Apply Filter	Use this to access the Device Display Filter window, and select other filter criteria
	Cancel Filter	Use this to cancel a filter you have just selected, or to cancel a pre-existing filter or set of filters
	Birds-Eye View	Displays a birds-eye view of the network only in Diagram view
	Connection	Displays the Network connections
	Zoom In	Allows you to zoom in on the Diagram view
	Zoom Out	Allows you to zoom out on the Diagram view
	Enlarge/Reduce	Only available in the Diagram view. This can be used to enlarge or reduce the sign of the viewing window.
	Align	<ul style="list-style-type: none"> <li>■ Bottom aligns all devices along the bottom of the window</li> <li>■ <b>Horizontal</b> aligns all devices horizontally in the window</li> <li>■ <b>Left</b> aligns all devices to the left of the window</li> <li>■ <b>Right</b> aligns all devices to the right of the window</li> <li>■ <b>Top</b> aligns all devices along the top of the window</li> <li>■ <b>Vertical</b> Aligns all devices vertically in the window</li> <li>■ <b>Horizontal</b> aligns all devices horizontally in the window</li> <li>■ <b>Around</b> not active in this layout.</li> </ul>
	Rearrange Connections	<p>Rearranges the current view of the connections. Including:</p> <ul style="list-style-type: none"> <li>■ Around</li> <li>■ 90 degrees</li> <li>■ Stagger</li> <li>■ Top/Left</li> <li>■ Bottom/Right</li> <li>■ Arrange Connections</li> </ul>

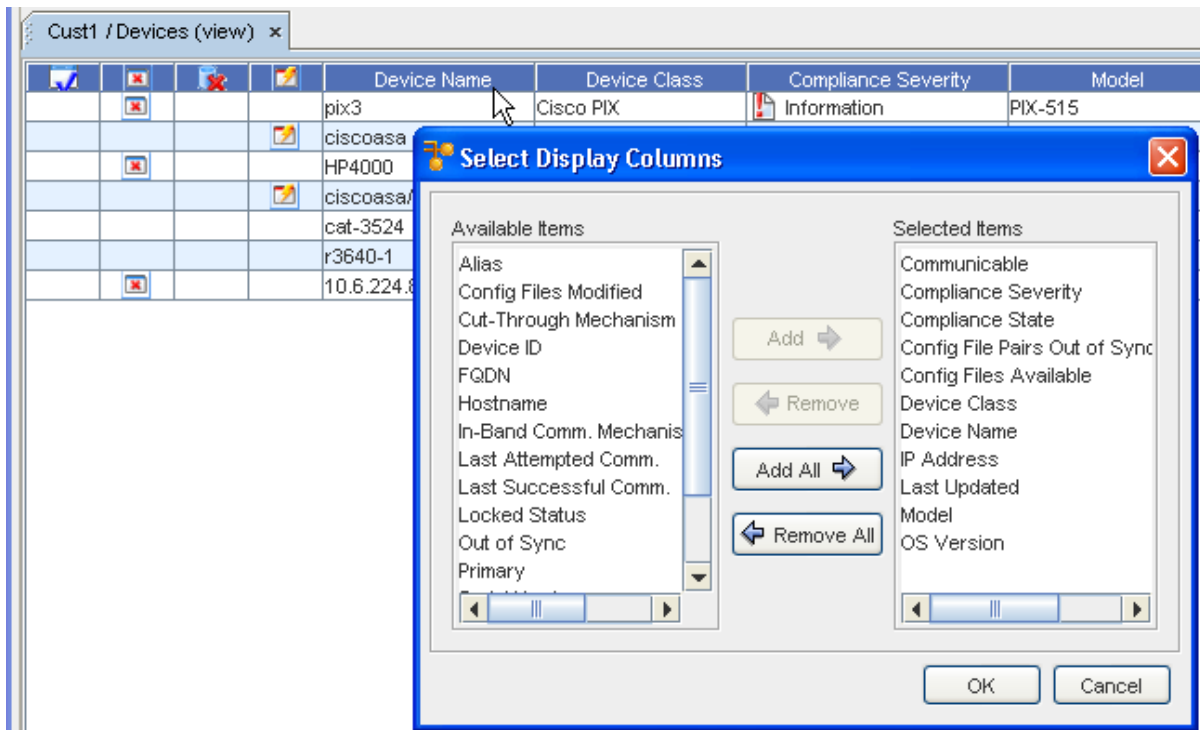


Icon	Icon Meaning	Action
	Legend	Takes you to the legend list. This list contains all the symbols used for the various device states, devices, and connections.
	Refresh	After making changes, use the Refresh icon to refresh your current view

## Displaying Column Headings in the Devices View

Table columns (and the information they contain) can be added or removed to customize your display.

- 1 With the Devices View displayed (shown here as Network **Cust1/Devices (view)**), right-click within any column heading to view the **Select Display Columns** window.




- 2 From here, determine **which of the column headings** you want displayed.
- 3 Make your selections by highlighting the columns you want displayed from the **Available Columns** pane, then use the **Add** or **Add All** arrows to move the headings you chose into the **Selected Columns** pane.
- 4 To hide column headings (and the information within that column) highlight the column heading in the Selected Columns pane, and using the **Remove** or **Remove All** arrows, move the headings you select back into the **Available Columns** pane.

- Click **Ok** to keep your final selections.

Only those column headings within the Selected Columns pane display on the Devices View in a table layout.

Once you have determined the column headings you want to display, you can then change the size of each column to view all the information that column holds by dragging the column table lines to the right or left to enlarge any specific column.

State	D...	Ali...	FQDN	Device ID	Hostn...
	ca...		cat-3...	1003	cat-35...
	Ca...		Cat3...	1001	CAgg...
	ca...		cat4...	1004	CatOS...
	ca...			1007	cat55...
	HP...		HP53...	1005	HP-53...
	r3...			1002	r3640...
	r3...			1006	r3640-3


Using the right and left arrows  you can increase or decrease the size of each column to view more or less column information. Within Network Configuration Manager, you can change the size or location of any column that is displayed within a table in the application. You can also move the columns horizontally (by dragging and dropping) to place a column anywhere within the table.

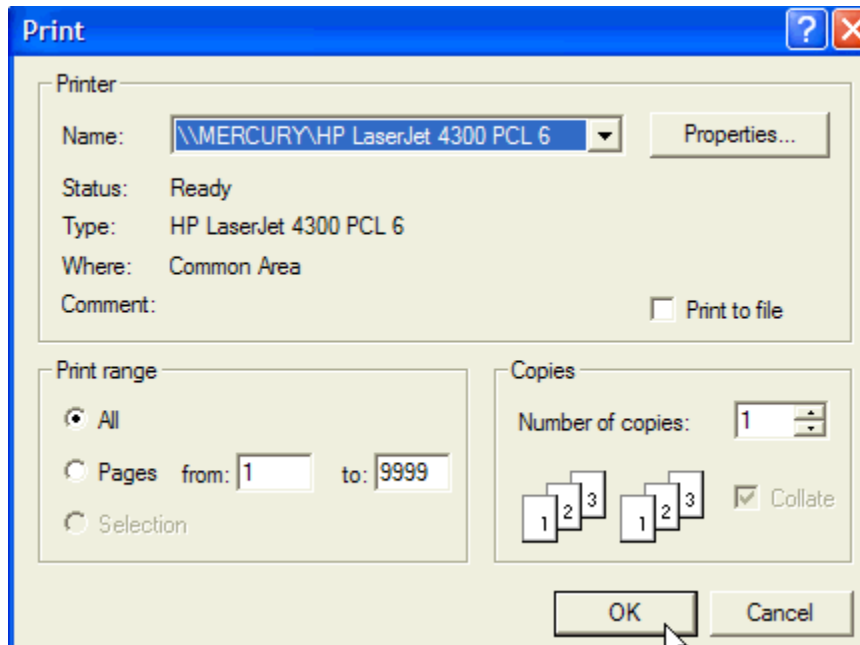
Following are the various states the devices can currently be classified in. Run your cursor over each icon to view the status.



## Printing the Devices View

While viewing information within the Devices View, you can print the screen using the print icon.

- From the Devices View menu bar, select the **Print**  icon.
- A print browser window opens, where you can include the appropriate printing information. Click **Ok** when you have made your print selections.



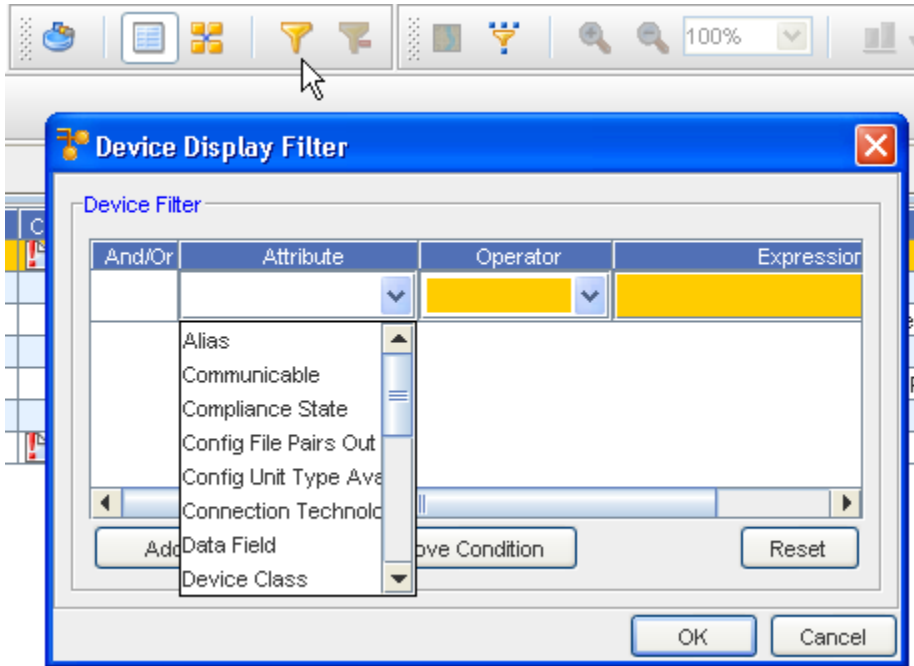
## Filtering Devices

Network devices can be filtered in any Site, View, or Workspace, so only those devices applicable to your tasks are displayed. Each attribute has its own set of application operations. Device filtering allows you to manage a select set of devices, based on a selected criteria.

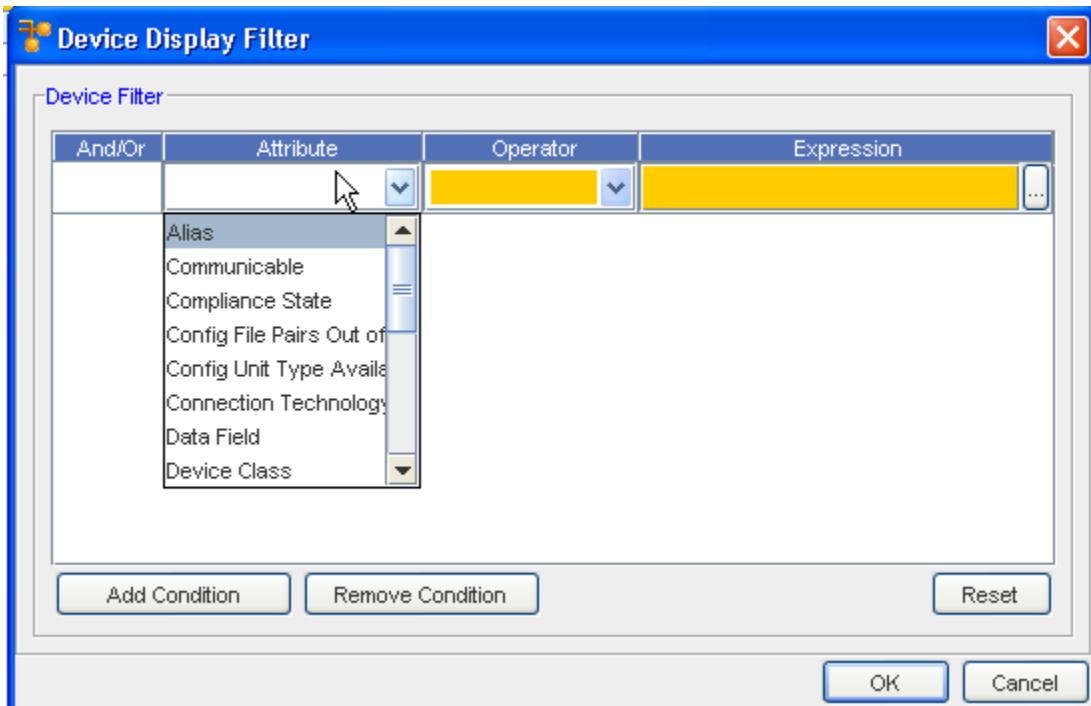
There are four ways you can create filters for devices:

- And/Or
- Selecting the Attribute
- Defining the Operator
- Entering an Expression

- 1 To Filter devices, select the filter icon ( **Apply**) on the tool bar. The Device Display Filter window opens.

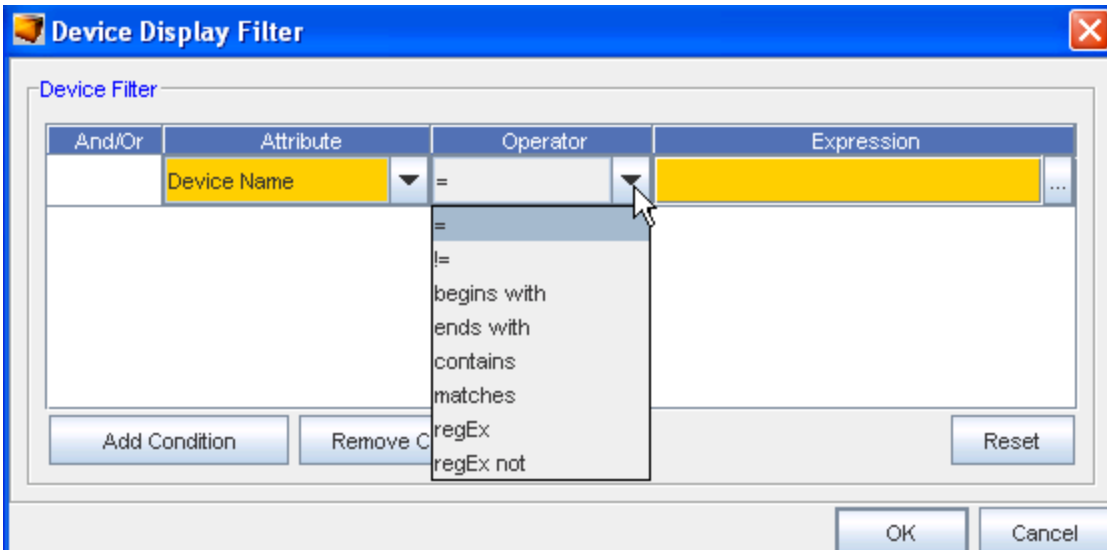


- 2 Select **Add Condition**, then select **And/Or** to allow your filters to be as specific as needed.
- 3 Although you may want to design a workspace with a large number of devices, you may also want to view specific devices based on certain criteria. These criteria are called Attributes. This is the lowest common denominator and cannot be a single filter setting. When an Attribute type is selected, you can enter either an **Operator** and/or an **Expression**. The Attribute options are similar to the following:



**Note** Additional filter attributes have been added that allow the user to create views, based on the Communication State (Communicable), Compliance State, Config File Pairs Out of Sync, and Config Unit Type Availability.

Note that you can select, and then **Remove** an existing condition. You can also select **Reset** to reset all condition selections.

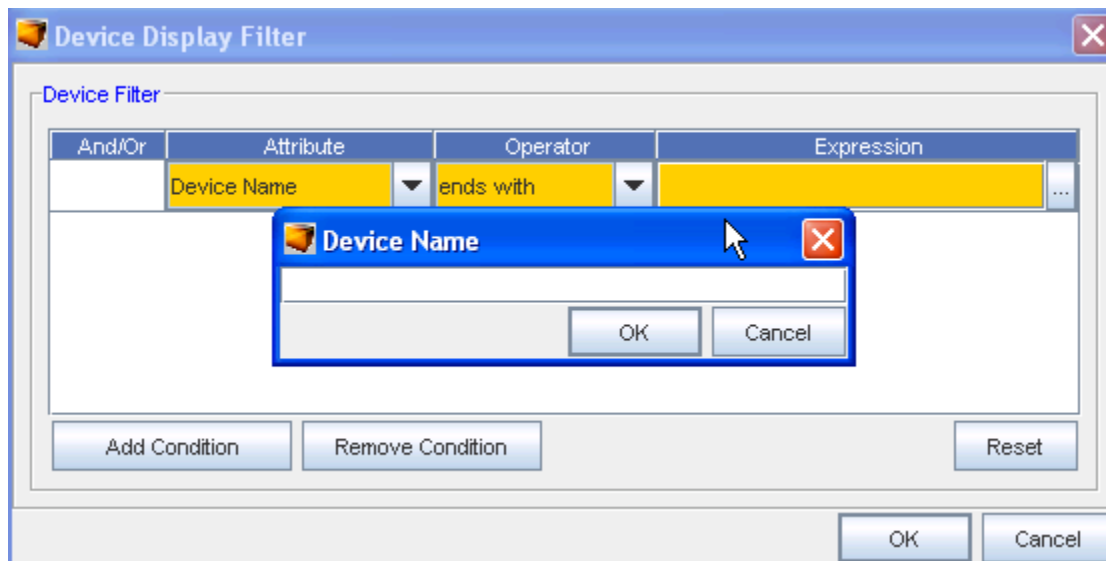


- 4 When configuring attributes, you can use one several options to specify what criteria is generated. For example, you can use one of the following:
  - = refers to the same or equal.

- **begins with** means the attribute begins with the defined expression.
- **ends with** means the attribute ends with the defined expression.
- **contains** means the attribute is include in the defined expression.
- **matches** indicates that your filter should match exactly those attributes you have selected.

**Note** The selections offered in the Operator drop-down depend on what is selected from the Attribute drop-down.

- 5 When the attributes Device Type or Connection Technology is selected, a list of selectable expressions are displayed. You can select either single-select or multi-select these options. The items that you multi-select are OR'ed together in the Expression field.




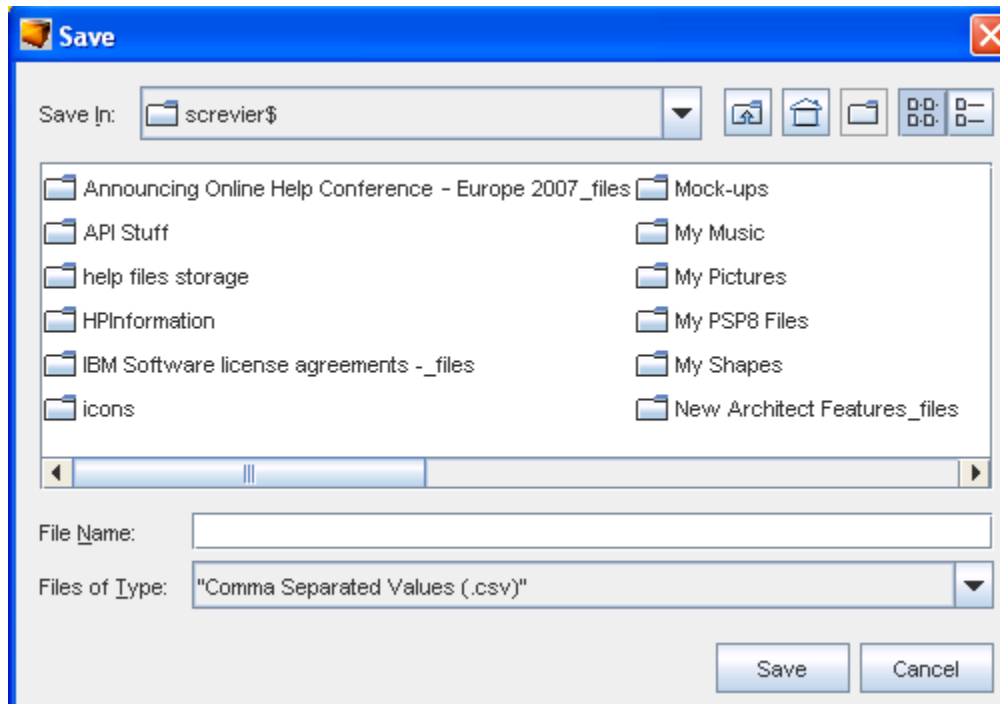
For all other Attributes, the Expressions field is an editable text field, where you specifically define the criteria. Using the filter settings as described above, allows you to filter the devices that display in the window work area.

- 6 Click **Ok** when you have added your expression.

**Important** Use the **Cancel** Button to close this window.

## Exporting the Devices View


- 1 From the Devices View menu bar, select the **Export**  icon.
- 2 A Save window opens. From here, determine where you want to save this Devices view. Include a **File Name**, as well as the **File Type** selection.
- 3 Click **Save** when you have made your export selections.

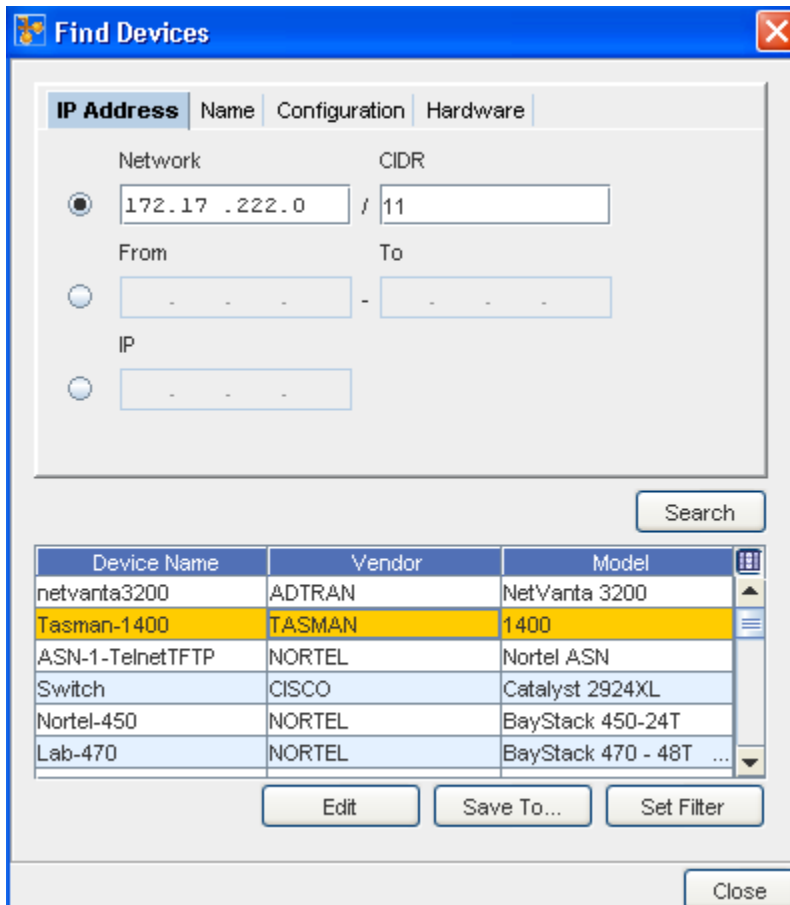


## Using Find in the Devices Window

Network **Find** capabilities include the ability for you to search configuration files with simple find criteria and RegEx. You can also search to find hardware attributes, such as line cards, as well as search by IP Addresses and Hostnames.



- 1 From the Devices View menu bar, select the **Find**  icon.
- 2 A Find Devices window opens. From here, determine the criteria you want to use in your find. You can search by selecting from the following tabs:
  - IP Address
  - Name
  - Configuration
  - Hardware
- 3 After entering your find criteria into the appropriate tab (shown here in the **IP Address** tab), click **Search**.







- **Edit** - to go to the Configuration editor, and edit if needed
- **Save To...** - to save the results to a specific location
- **Set Filter** - to change any existing filters

4 Click **Close** when you have completed working with the search results.

## Accessing Editors in the Devices View

From the Devices View menu bar, you can select an **Editor** from the Editor section. You can access the:

- Config (configuration) Editor 
- Configlet Editor 
- Interface Editor 
- Command Editor 

## Device States



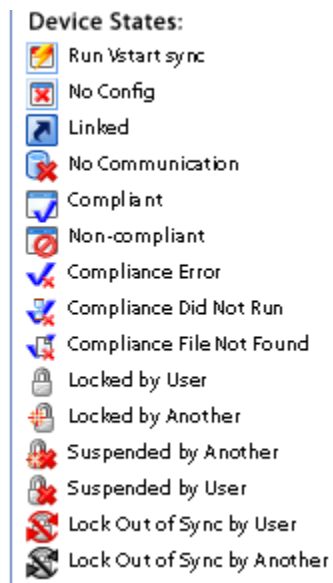
The Device State can be seen from either the Devices or Workspaces views.



Click the Legend icon to view the various states.

Listed are the classifications for **device states** :

- Run vs. Start (out-of-sync)
- No Config
- Linked
- No Communication
- Compliant
- Non-Compliant
- Compliance Error
- Compliance Did Not Run
- Compliance File Not Found
- Locked by you (the user)
- Locked by another user (with an entirely different login and password)
- Suspended by another
- Suspended by user
- Lock Out-of-Synch by a user
- Lock Out-of-Synch by another user



This column indicates, by icon, the *state (or status)* of the device in your local view, the view of the devices in your network is local. Therefore, a device can be *out-of-sync* with the network. To update a device's config, see [Scheduling Network Level Config and Hardware Spec Pull Jobs](#).

**Note** You can place your cursor on the icon within the **State** column to see the name (description) of that specific state.

## Devices View of Device State

Following is an example of the device states viewed from the Devices View. In this example, the device r7206-1-test has **not** been configured, and there is no configuration associated to it.

Device Name	Device Class	Compliance Severity	Model
r7206-1-test	Cisco IOS Ro...	Information	
r3640-1	Cisco IOS Ro...	Information	3640
Pix-501	Cisco PIX	Information	PIX-501
cat-3524	Cisco IOS S...	Information	WS-C3524-X...




## Sorting on Device States

You can click within any column to **sort** the contents of that column into either ascending or descending order. This holds true as well for the device State columns. Click on the device state icon to sort, then click again to reverse that sort order.

## Clearing Device Flags

The device state is displayed in the table format of the Devices View. Note that there are "flags" or icons that indicate the status of the device.

You can **remove Compliant and Non-Compliant flags** from the Devices view, and not have them visible. This will be in effect until you logout, and login again to Network Configuration Manager.

For example, this icon  alerts you that this device is in a **Non-compliant** state.

To remove a **Compliant or Non-Compliant flag** from the Device View State column, complete the following steps:

- 1 Create a **test policy** containing both a Standard and a Test. This then makes the device **Non-Compliant**.

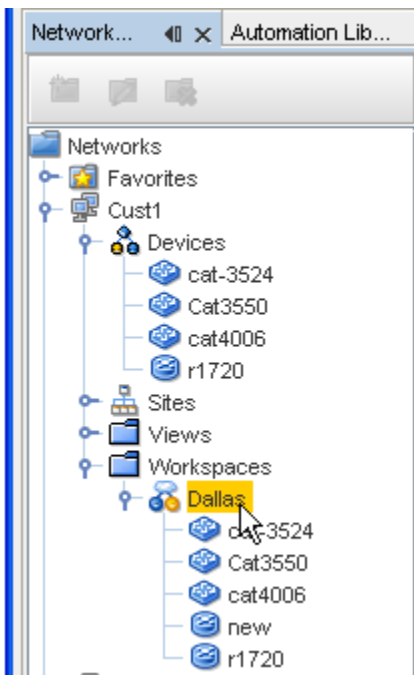
- 2 Create a **revision** on that device.
- 3 After the push is completed, refresh the devices view.
- 4 Now, create a **dummy policy** (without Standards included).
- 5 Select the device, then right-click the **Non-Compliant device** to get to the right-click menu. Select **System** from the Look In: drop-down arrow. Now, click **Open**. From the Select Item window, select the **dummy policy** you created, and click **Select Item**. At the confirmation message, click **Yes** to continue. The flag marking that device as Non-Compliant is now removed.

## Working with Virtual Devices

After creating the **Workspace**, you can begin configuring the layout using Virtual and Network devices.

To add virtual devices,

- 1 With the Devices View displayed, select the **Workspace**.

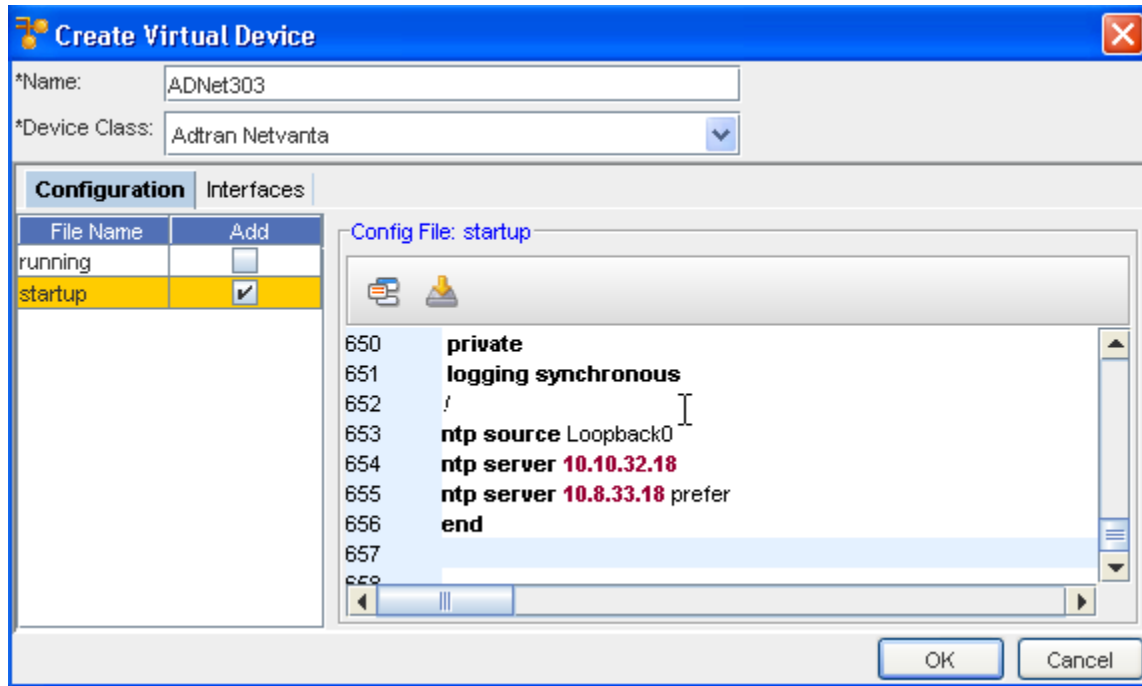


- 2 Select the **Virtual Device icon** from the menu bar. The Create Virtual Device window opens.



- 3 Type a Virtual Device **Name**.
- 4 From the **Device Class** drop-down arrow, make an appropriate selection from the list.

- Click **Ok**, or continue to make other selections in your virtual device using the Configuration and Interfaces tab.



Working with the Configuration tab,

- At the **Configuration** tab, click the **Add** check box to select the current running configuration.
- You are now linked to the **Library Manager**, and can select a template by going through the various windows. If the template you selected does not match the vendor of one or more of the devices, click **Yes** at the informational box, then make your template selections from the Template Variable Substitution window. Click **Preview** to see the preview of the template, then click **OK**.

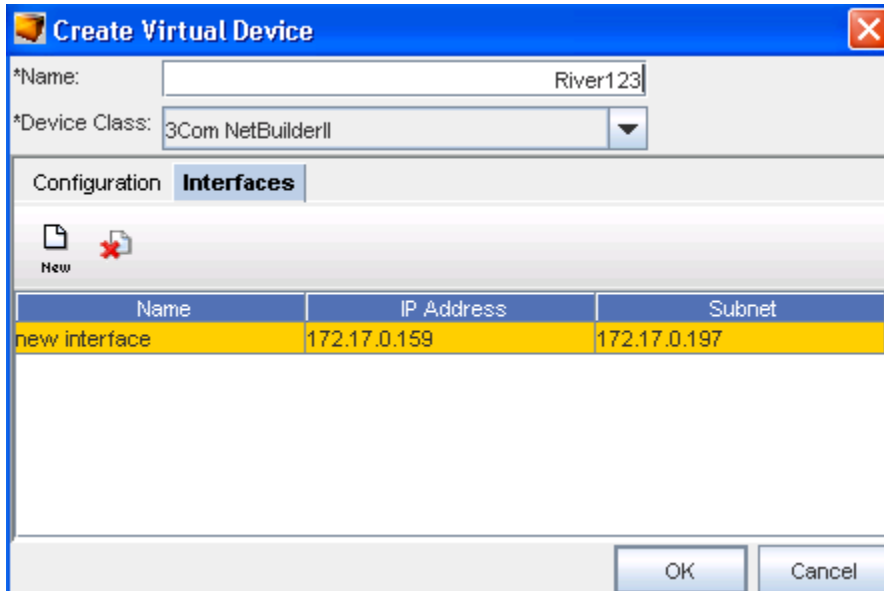
---

**Important** You can also select the **Insert File** icon  to insert a file contents. You can also select to insert a Template.

---

Working with the Interfaces tab,

- Click the **Interfaces** tab.
- To get the Add New Interface window in the **Interfaces** tab, click **New**
- Enter the **Name**, **IP Address** and the **Subnet** address in the fields.
- Click **Ok**.



5 Click **OK** to close the Create Virtual Device window.


The workspace refreshes as each device is added. Note the new state of the Device. The new state shows the device has been "Locally Modified".

## The Devices Legend

When visualizing any Network in the Diagram view, there are multiple icons that are used to represent connections, device states, and device types. Depending on the makeup of the Network, some of the components are shown.




The **Legend** is used to identify the devices and their connections, if any, within the network. There are three sections to the Legend:

- 


The first section is **Connections**. This identifies the connection method devices use to communicate with one another.

---

  - 

The second section is **Devices**. This identifies device types within the network. Each device in a network is represented by a corresponding icon.

---

  - 

The third section is **Device States**. This identifies the state of the device's configuration.
- Note** Note that Device States may change if the actual state of the device changes while in the Devices View.

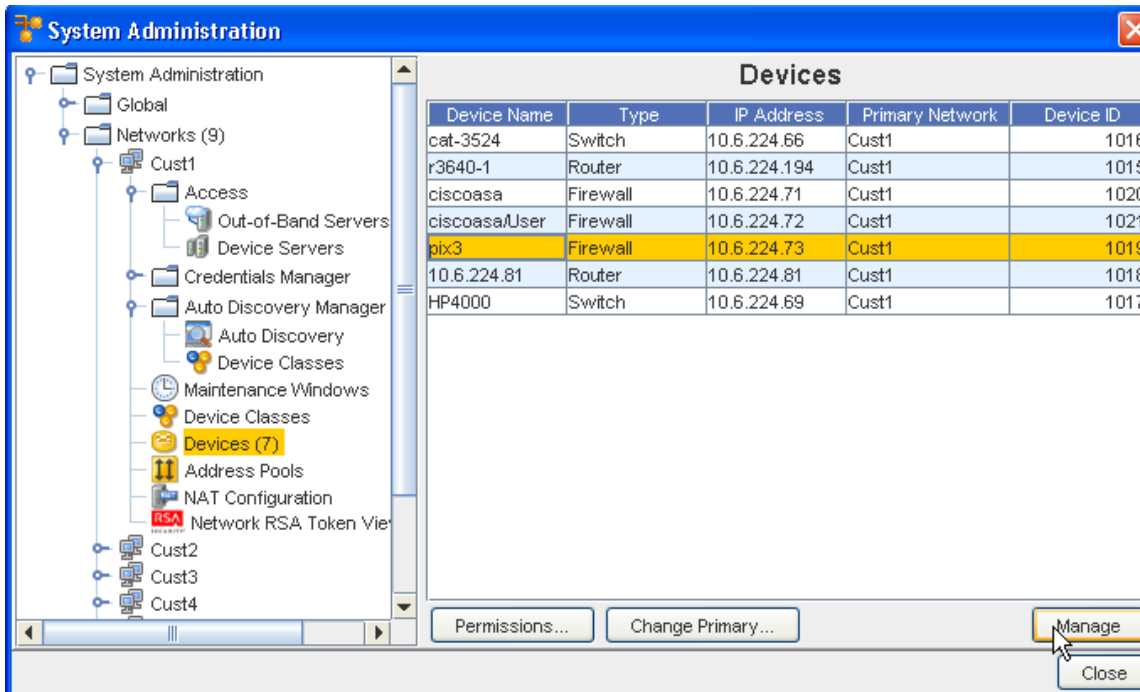
## Deleting a Device

**Important** To delete a device, you must first ensure the device has been unmanaged.

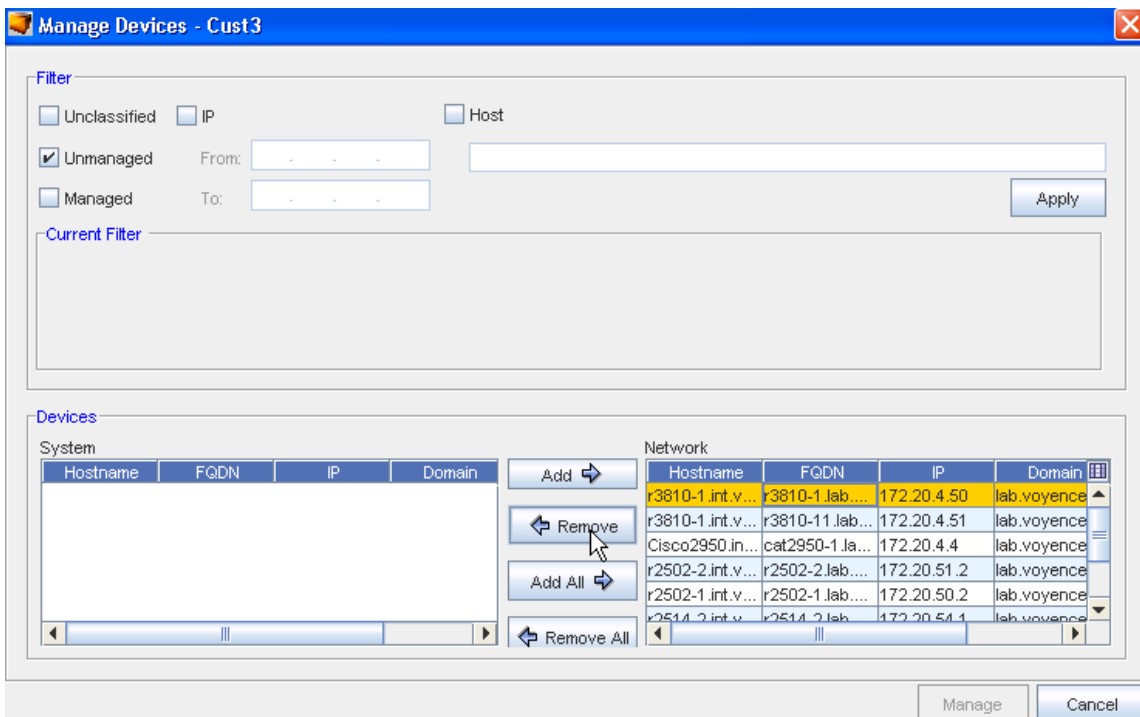
To delete a device,

- 1 At the System Administration tool, select **Networks**, then select **Devices**.

- 2 Select the device you want to remove from the list, then click **Manage**.

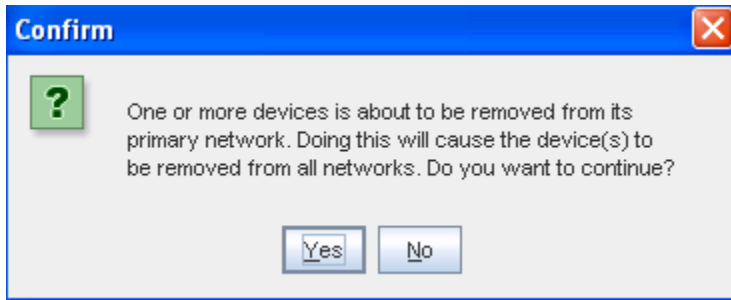


- 3 Select the **Unclassified** option in the top portion of the window, then click **Apply**. The Device is being retrieved.



- 4 Next, from the bottom **Devices** section, **remove the device** from the Network using the left arrow ( **<-Remove**), moving the device from the Network pane into the System pane.
- 5 Click **Manage**.

- 6 Select **Yes** at the confirmation message to remove the device from its Primary Network.



- 7 Next, select **Yes** .
- 8 You can now go to the System Administration tool, and from **Global -> Access select Devices** .
- 9 After selecting the device, click **Unmanage** to change the state of the device to Unmanaged.
- 10 Now that you have placed the device into the **Unmanaged state**, you can remove the device. Once again, select the device from the list, the click **Remove** .

## Using the Birds-Eye View

---

**Note** You must be viewing your devices in the **diagram layout** to use the Birds-eye feature.

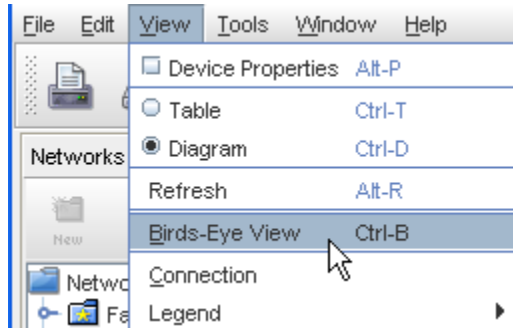
---

The birds-eye view is a snapshot of your network at a 1,000 foot view. The birds-eye view is similar to the **zoom** tool in the diagram toolbar. The zoom tool allows you to enlarge the window to a specific area of your network. Devices outside of the zoomed-in view are not seen in the browser window.

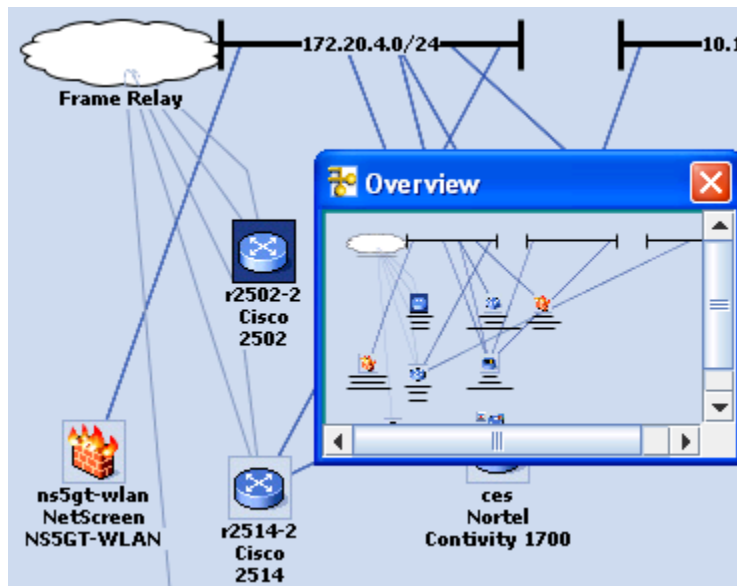
The birds-eye view actually zooms out far enough to see the entire network. A rectangle is used to identify the portion of the network that is seen in the browser window. The intent of the window is to allow you to have a spatial orientation of where you are in your network diagram.

To open the birds-eye view,

- 1 In the menu bar, click **View**. Note that you must first be in **diagram mode** displaying your devices.
- 2 Select **Birds-eye View** .



The Overview window opens in the upper left corner of the application. The birds-eye view is re-sizeable, as needed. Use arrows to enlarge the width or length of the view.



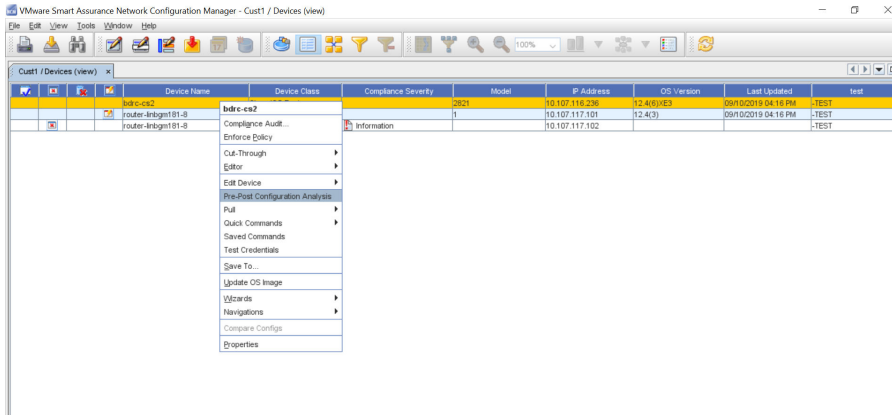
## Using Right-Click Options

### Right-Click Menu Options Overview

The right-click feature in a **Devices view** (when the view is shown in a Table format) provides access to the following links. You can also access the same options when you right-click a device in the Diagram format.

Using these links allows you to complete a number of tasks, and view a great deal of device information.





### Important Information!!

You must have the appropriate permissions to successfully complete some specific tasks you can access from the Devices View right-click menu options.

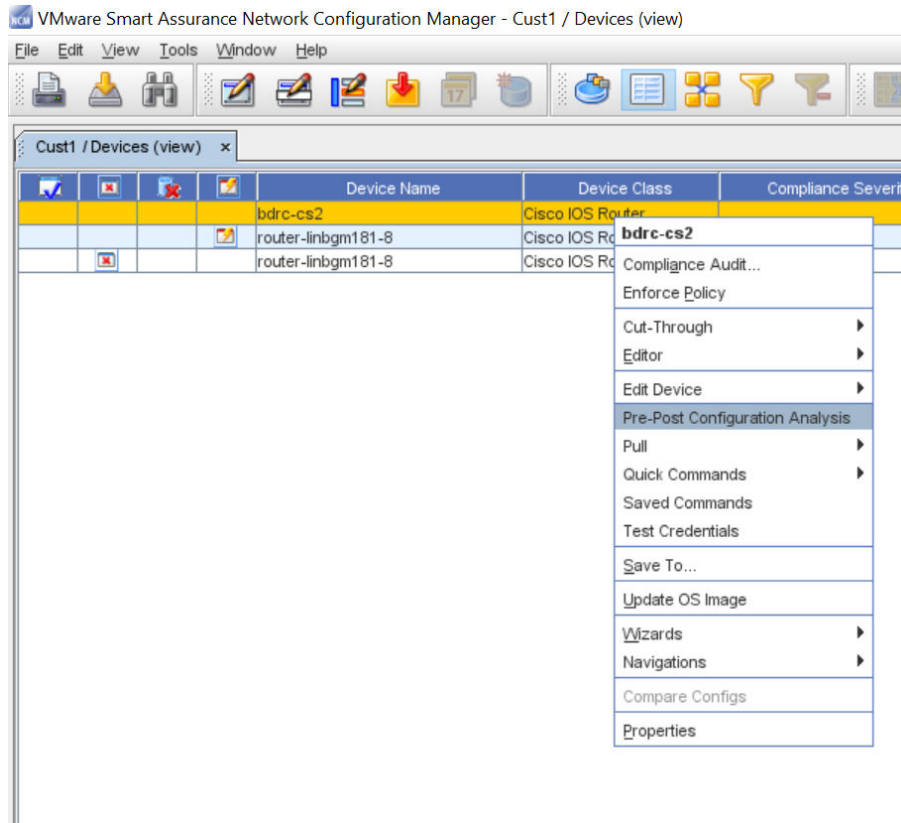
For example, in Cut-Through (In-Bound and Out-of-Bound), Quick Commands and Saved Commands, you are required to respond and correctly enter the appropriate information in the Job Credentials Input pop-up screen when this screen is displayed to continue to complete the selected task. See your System Administrator for more information.

---

**Note** Any task that is not accessible to you from the right-click options listing (appears dimmed), and automatically lets you know that you do not have the appropriate permissions to complete that task, or that you have not made a correct selection (as in Compare Configs - you must select two devices from the list).

---

You can also use the right-click menu in the Navigation tree . You can select any device within the Network, and right-click to display the options.



Access each link to get more information on the tasks you can complete.

- [Compliance Audit](#)
- [Enforce Policy](#)
- [Cut-Through](#)
- [Editor](#)
- [Edit Device](#)
- [Pull \(Immediately\)](#)
- [Using Quick Commands](#)
- [Using Saved Commands](#)
- [Test Credentials](#)
- [Updating OS Images](#)
- [Wizard Overview](#)
- [Navigations](#)
- [Compare Configs](#)
- [Compare Configs](#)
- [Device Properties Tabs\(when applicable\)](#)

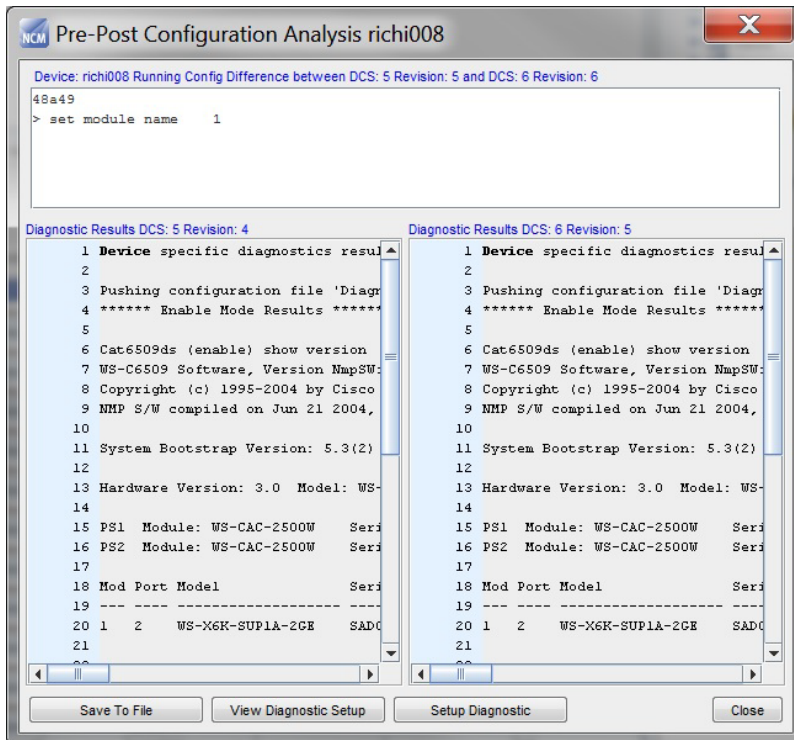
## Pre-Post Configuration Analysis

Network administrators may use the **Diagnostic Utility** to:

- Validate configuration changes made to a device.
- Create a report which functions as a proof of changes made to devices. You can download the comprehensive report which details the diagnostic results and differences between current and previous configuration revisions.

To generate a report:

- 1 Select **Pre-Post Configuration Analysis**. A comprehensive report displays.



- 2 You may perform these operations:

- Save to File (saves the results of the diagnostics to a Microsoft XLS file)
- View Diagnostic Setup
- Diagnostic Setup

## Compliance Audit

The Compliance Audit tool allows you to **create standards and tests used to compare with configured devices**. Devices that are out-of-compliance are not configured correctly, and must be put into compliance using this tool.

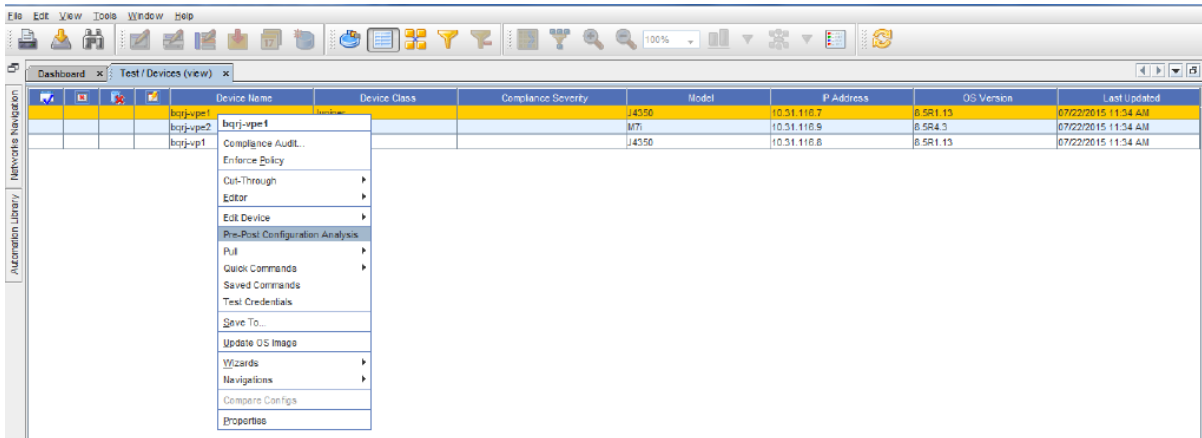
---

**Note** Compliance Audit can be executed on one or more devices.

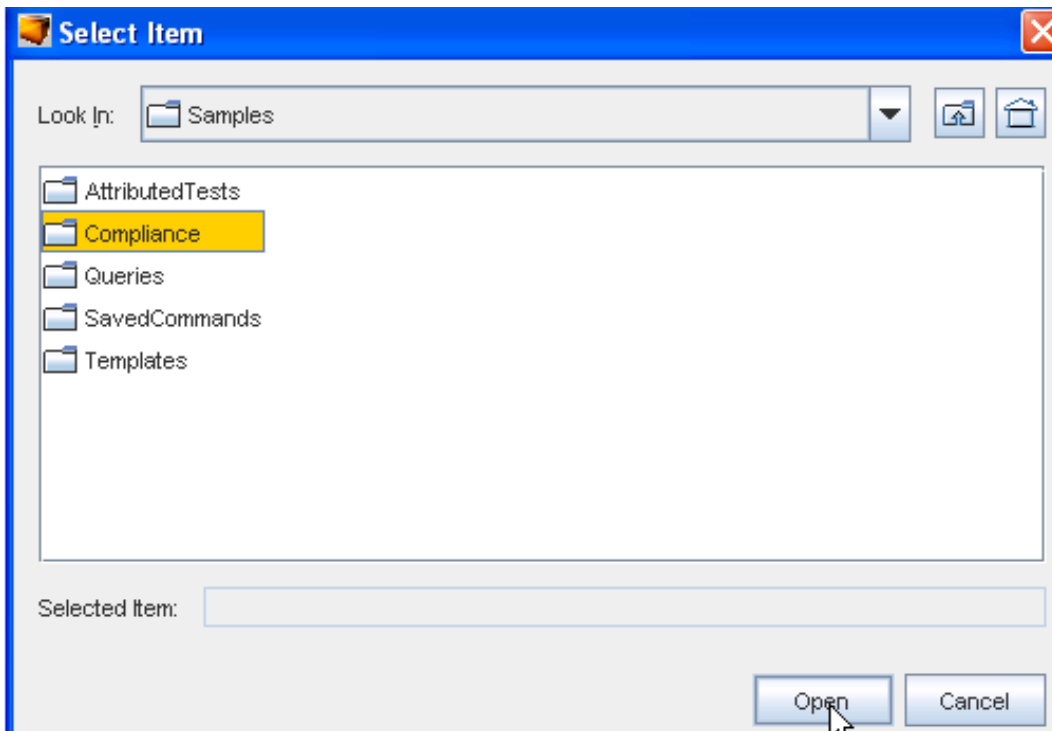
---

From the right-click menu in the Devices View, you can access the **Compliance Audit** tool for any device that is in the out-of-compliance state.

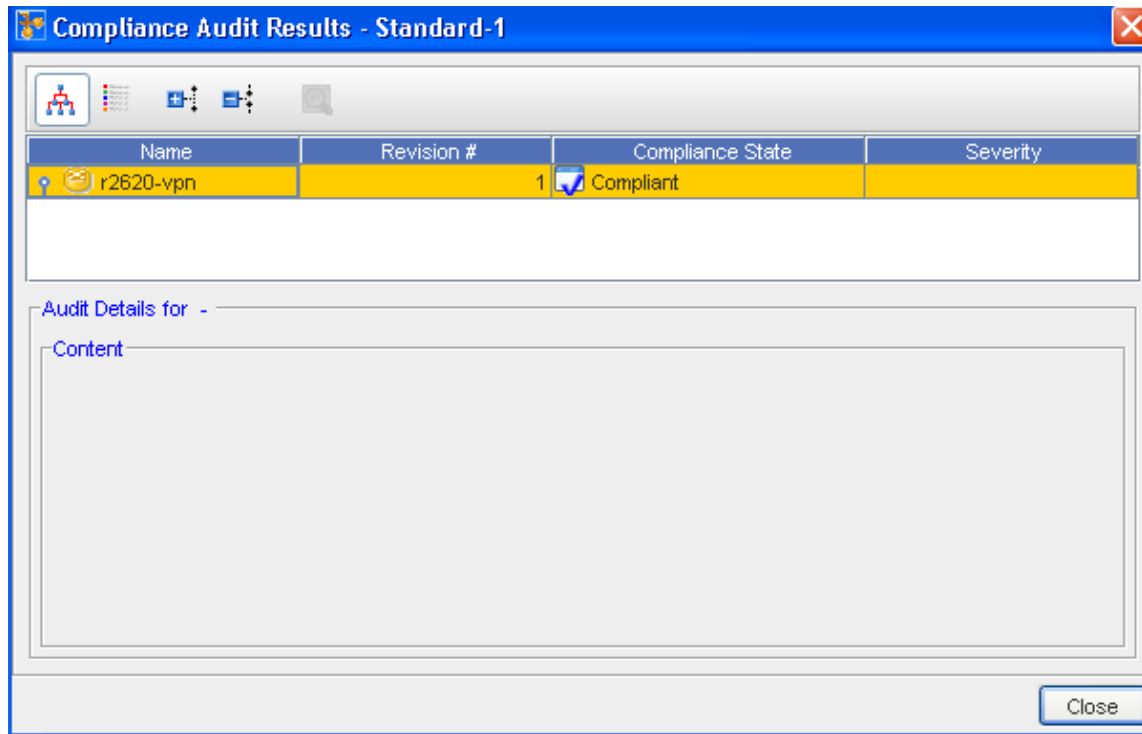
- 1 In the Device View, select **one or more devices**, then right-click to get the Device options.
- 2 Select **Compliance Audit** from the menu.



- 3 The Select Item window opens. From here, select the **Location**, then select the **item**.



- 4 After making your selection, click **Open**. The Compliance Audit Results window opens.



As you can see in the above example, the state for the device selected is **Non-Compliant**. The lower section (Audit Details) allows you to view the details of the audit results if needed.

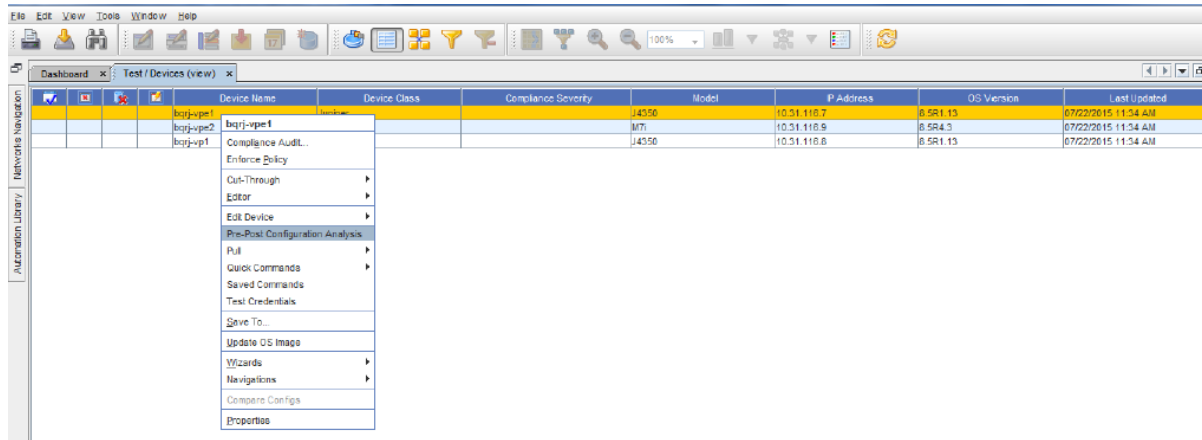
The icons located in the top left allow for the following:

- View in tree format
- View in a list
- Expand the selected view
- Collapse the selected view
- View the results of a selected device

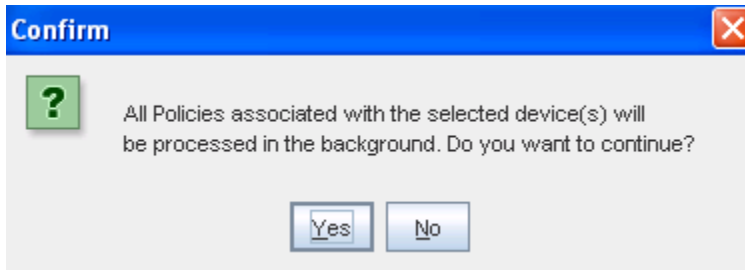
## Enforce Policy

From the Devices View, you can right-click on a device, then go through the steps needed to enforce a previously defined policy on that specific device.

**Enforce Policy** allows you to take a policy and **immediately** apply it against one device, or an entire group of devices. When Enforce Policy is selected, every other policy associated with that device is also enforced.



- 1 Select **one or more devices** from the Devices view.
- 2 Right-click, and select **Enforce Policy** from the options. A confirmation message displays.



- 3 If **Yes** is selected, all policies are then loaded, and enforcement is completed in the background. Click **Yes** to continue, or click **No** to stop the processing.

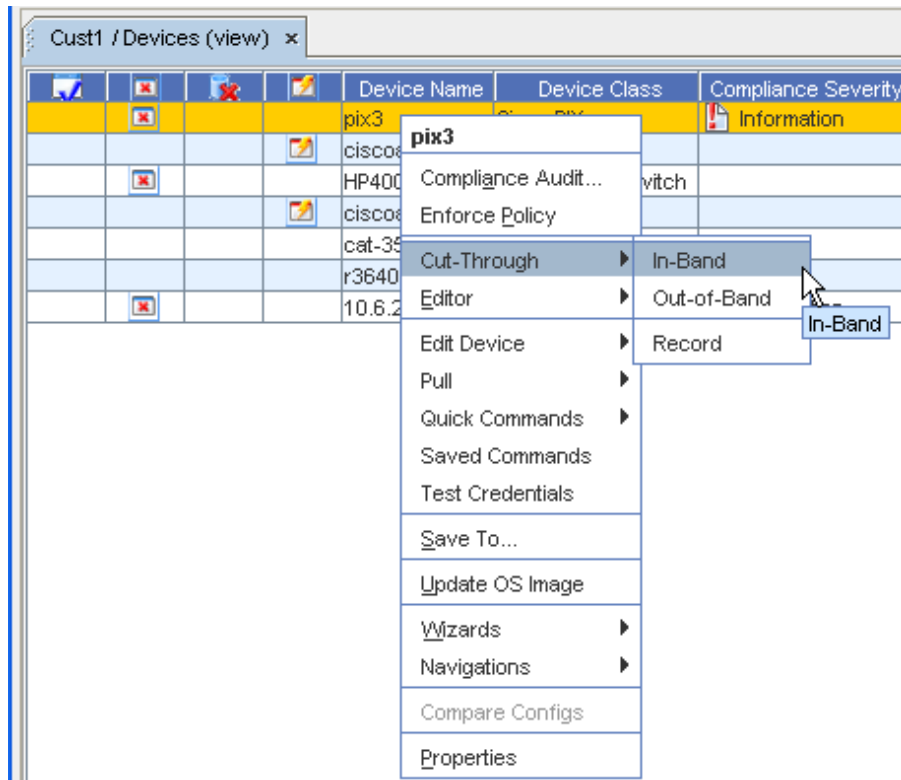
**Note** Devices are flagged as to their policy status (in or out-of-Policy). You can remove the device status (or state) flags. For example, if you prefer not to see any non-compliant flags for devices (for any reason). Go to [Clearing Device Flags](#) for more information and instructions.

## Cut-Through

The Device cut-through allows you to create a secure, 128-bit encrypted connection tunnel to a device. The secure tunnel uses a single port pair from client through application sever, and device server to the end device.

For most clients, you can establish which Telnet client you want to execute, such as PuTTY, CRT, or Secure\_CRT. Cut-through also supports creating recorded Save Commands.

From the right-click menu in the Devices View (either diagram or table format), you can access the Cut-through menu.



- 1 Select **one or more devices** from the devices listing that you want to complete a cut-through on, then **right-click** to get the right-click menu.
- 2 From the right-click menu options, select **Cut-Through**, then select a cut-through option.

From this option, you can select In-Band, Out-of-Band, or Record to work with device properties.

**Note** Any task that is not accessible to you from the right-click options listing (appears dimmed), automatically lets you know that you do not have the appropriate permissions to complete that task .

### In-Band

When the In-Band option is selected, the In-Band communications is established, and a Telnet session is opened where you can make needed changes or enter information. Notice that this is a **secure site** , and you must have permission to work within this feature.

From this session, you are communicating directly with the device , and can issue and execute commands to the device.

### Out-Of-Band

When the Out-of-Band option is selected, the Out-of-Band communications is established, and a Telnet session is opened where you can make needed changes or enter information. Notice that this is a **secure site** , and you must have permission to work within this feature.

From this session, you are communicating directly with the device, and can issue and execute commands to the device.

## Record

The recorder window displays behind the cut-through session. Recordings can be paused, saved, resumed, or cancelled during the cut-through session.

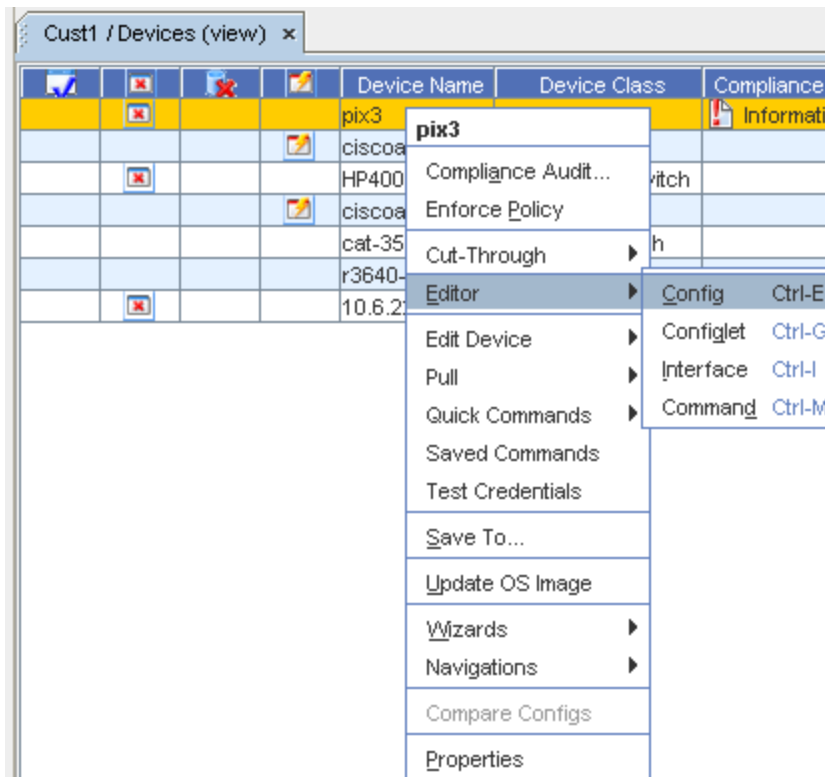
When this option is selected, you can determine if you want to select either the In-Band or Out-of-Band session for recording. This is used to automatically record, and then alert users to run tasks, or to follow instructions. What you enter into the window is automatically copied into another window, and is then recorded (much like a tape or VCR recording), and can be played back as directed.

- Recorded sessions saved in the Automation Library can be edited, moved, and copied from within the Automation Library.
- Recorded sessions can be executed and scheduled as Saved Commands.

## Editor

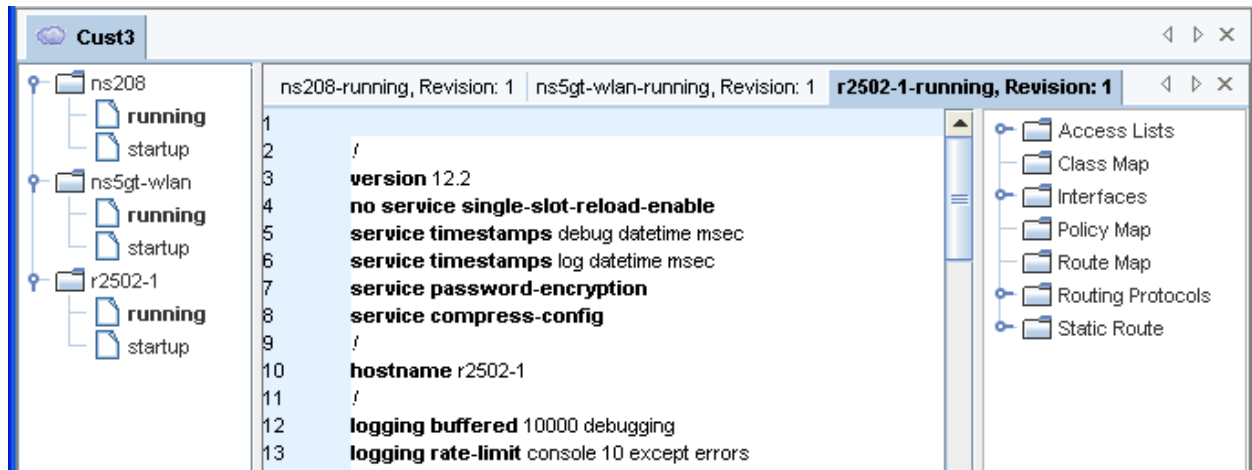
From this selection in the Devices View right-click menu options, you can access any one of the four editors.


- 1 Select **one or more devices** from the view.



- 2 Next, right-click, and select **Editor** from the listing. In this example, **Config** was selected.





You can now view the results of each device, using the separate device-named tabs that run along the top. You can also expand or collapse the device information displayed using the list in the left .

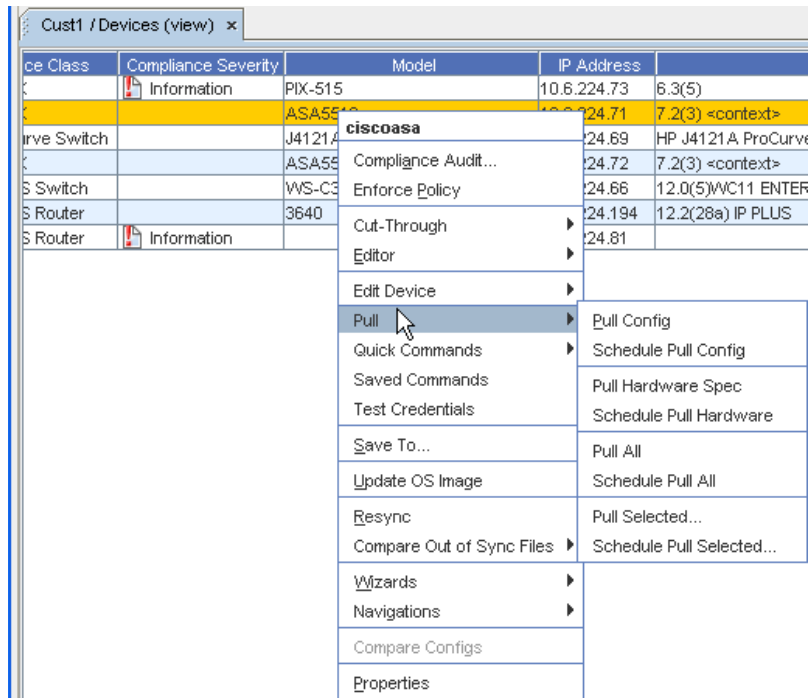
**Important** The listing on the **right** can be expanded to view additional information associated to the selected device.

For more information, see [Editors Overview](#).

## Pull (Immediately)

While viewing the Devices in either the Table or Diagram view, you can use the right-click feature to access a selection of **Pull** and **Schedule** options, including **Pull the Configuration**, or **Pull the Hardware Spec** (for a device immediately).

You can also use the option to go through the Schedule Manager, and then schedule the pull.



## Using Quick Commands

Quick Commands allow you quick access to standard diagnostic tools. Quick Commands are executed immediately, and the results are displayed in a separate window. Some Quick Commands can be executed across device classes. You can create additional Quick Commands through DASL scripting.

The **Quick Commands** option allows you to access quick commands, including Ping, Trace route, assorted Views, and more!

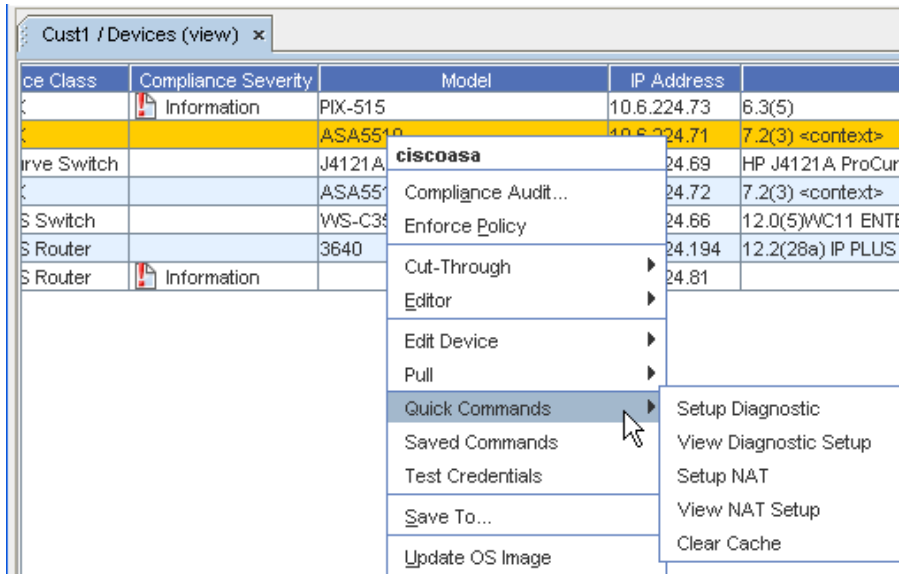
Quick Commands can be used with the following views:

- Devices
- Sites
- Workspaces

**Note** Any task that is not accessible to you from the right-click options listing (appears dimmed), automatically lets you know that you do not have the appropriate permissions to complete that task.

To access Quick Commands from Devices,

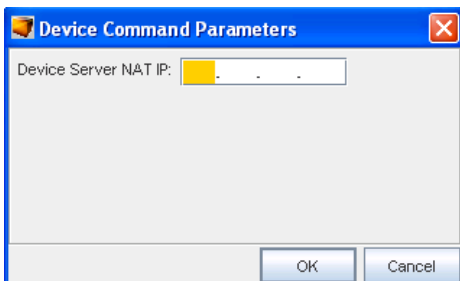
- 1 Expand **Devices** in the navigation pane to show the **Devices view** in table format.
- 2 Right-click to get the drop-down menu. You can also right-click on the device in the Diagram view.
- 3 From this menu, select **Quick Commands**.



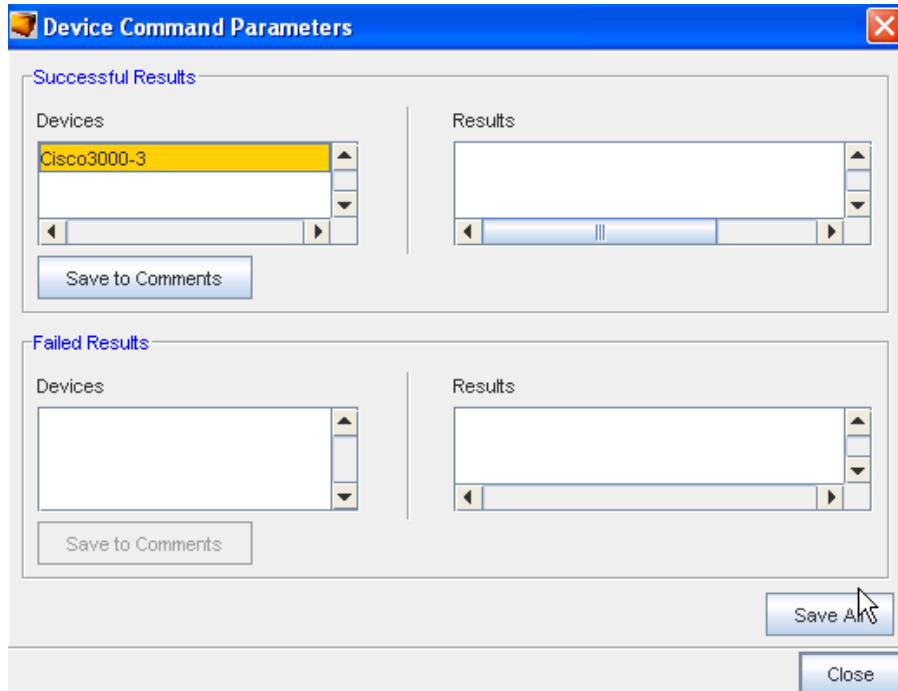
Quick Commands differ based on the device.

**Important** Some quick commands can only be executed if the devices are first set up with device credentials.

- When a command is selected, if there are command parameters needed to execute this command, you must include the parameter information in the **Device Command Parameters** window. If parameters do not need to be defined to execute this command, the command automatically executes.



- After entering the Device Command Parameters, click **Ok**, and the command executes. Results of the quick command are detailed. From this window you can **Save All**.
- After saving the quick command results, click **Close**.



## Using Saved Commands

Saved Commands can be created within the Automation Library, or through recorded cut-through sessions. Save Commands selected can be executed immediately, and can have the results displayed.

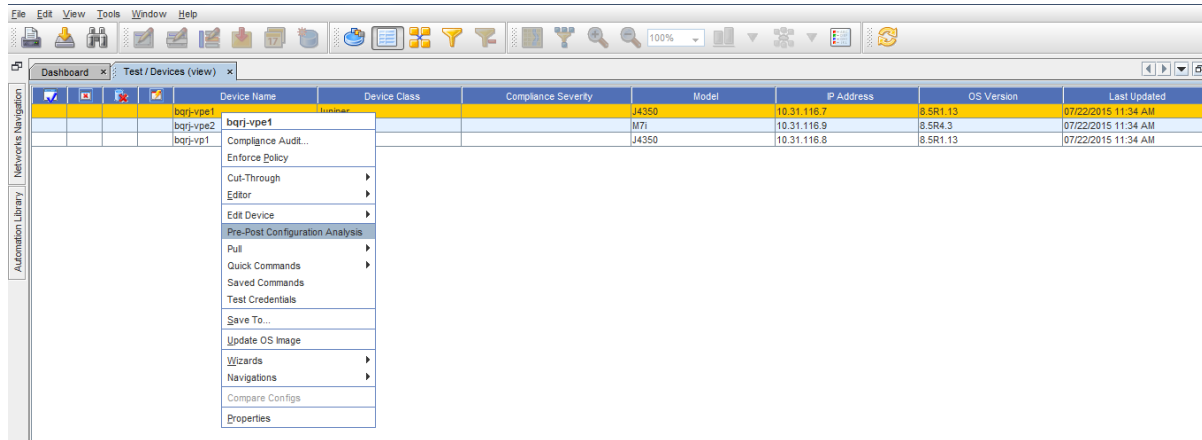
The Saved Command option allows you to **access saved commands** you have previously created, and **execute those commands** immediately.

---

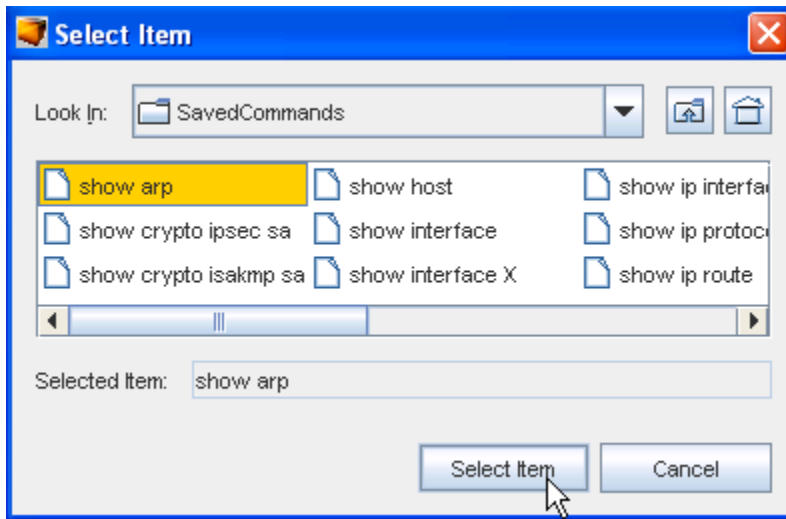
**Note** Any task that is not accessible to you from the right-click options listing (appears dimmed), automatically lets you know that you do not have the appropriate permissions to complete that task.

---

From the Devices View (in either the table or diagram format), you can access Saved Commands using the right-click feature.



- 1 From this window, use the drop-down arrow to select where you want to **Look In** to see any saved commands you may want to use.
- 2 Click **Select Item** when you have made your selection.
- 3 Next, click **Open**. The Saved Command is now executing.



The **Device Command Parameters** window is displayed for you to see if the command executed successfully, and where you can save the Results.

- 4 Click **Save All** to save these results, then click **Close**.

For more information on Save Commands, see [Creating a Command](#).

## Updating OS Images

From the Update window you can select each device to be updated, select the target location for the image, determine if there is adequate space for the upgrade, and set the device, memory, and partition preferences.

OS updates are scheduled in the same manner as any other job - through the Scheduler.

## Prerequisites to Updating OS Images

Prior to updating the OS Image you must ensure the following tasks have been completed:

- [File Servers Overview](#)
- [Adding OS \(Image\) Inventory](#)

---

**Important** Ensure that the File System information displayed in the [Device OS information](#) section is the most current information for the devices (as shown in the Last Hardware Pulled Time section, and from the Device Partition Information - see the following graphic).

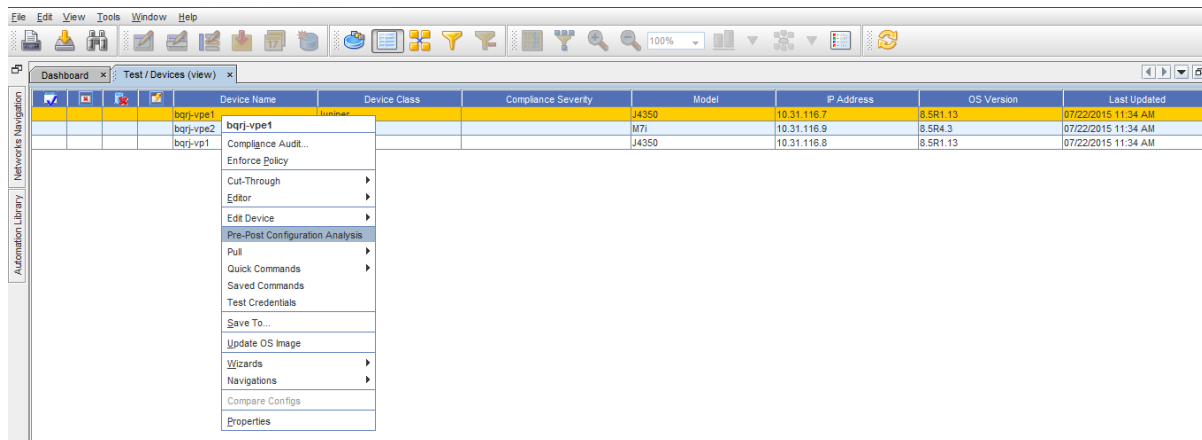
---

If the most current information is not displayed, you can complete a Hardware Pull on the devices. Go to the Devices View, and right-click to get to the [Pull option](#), then select Pull Hardware Spec from the options list.

To update the OS Image,

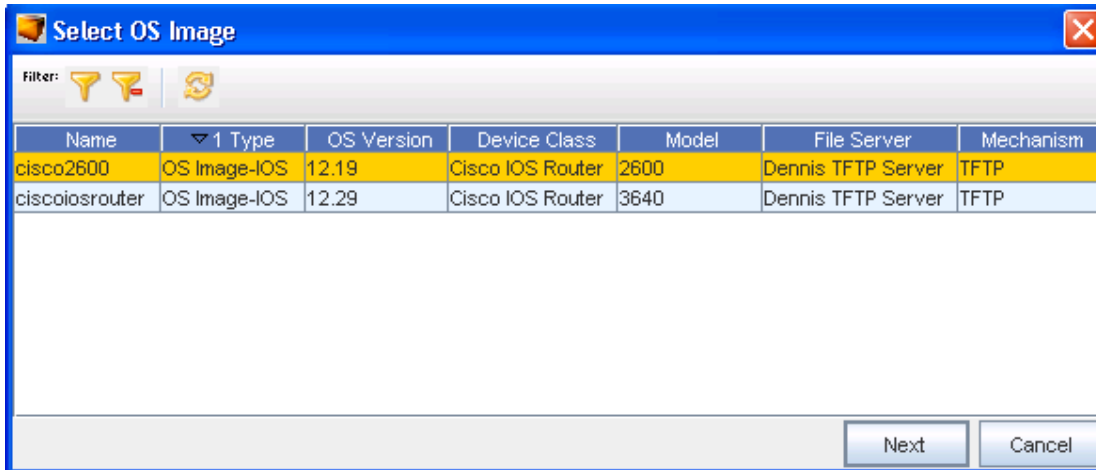
The Update OS Image option allows you to **replace** the device's current OS Image.

From the Devices View (in either the table or diagram format), you can access the Select OS Image window to update the OS image for the device.

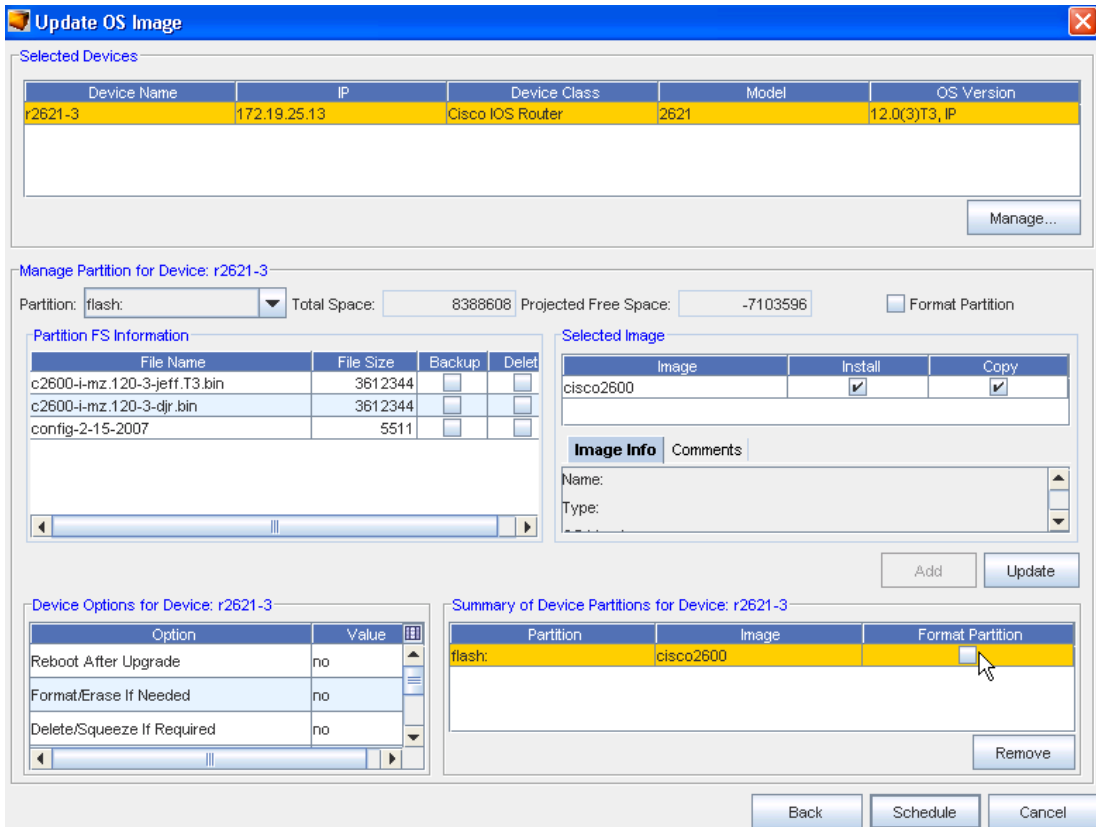


**Device (or a number of devices)** from the listing of devices, then right-click to see the menu.

- 1 From the menu, select **Update OS Image**.
- 2 From the Select OS image window, select any **existing OS Image** . You can also create a new OS Image (if needed).

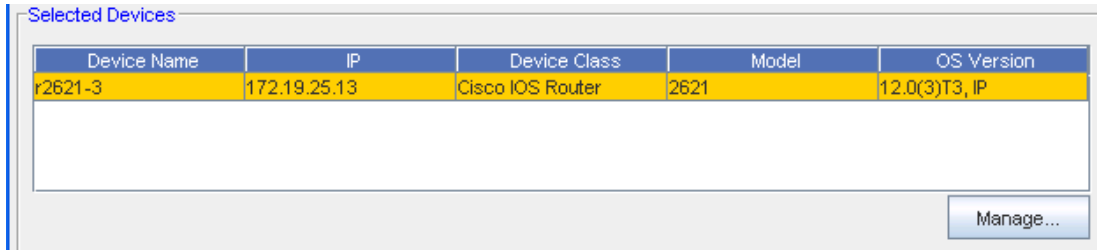


- 3 Click **Next**. The Update OS Image window is displayed. You may get an informational message, inquiring if you want to continue. Click **Yes** if appropriate. Note that there are three sections to this window.

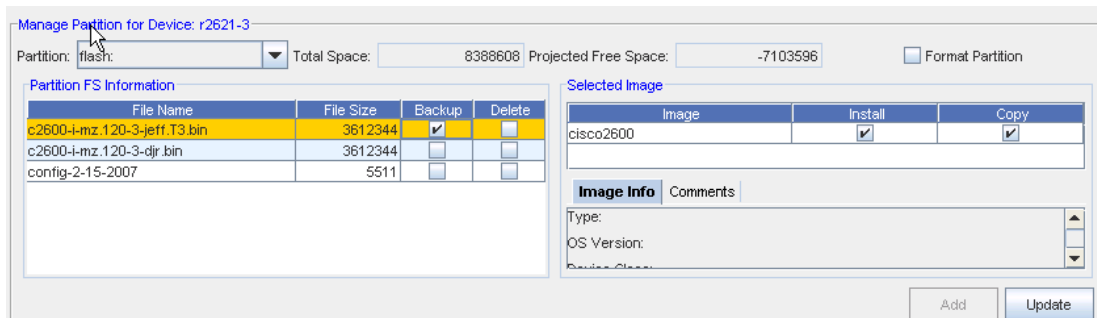


- 4 At the first section, you can view the **Selected Devices** , and the information for that device.

**Note** From this window you can also click **Manage** to see a listing of devices to add more devices to the Selected Device list (from the Update Device).



- 5 If more than one device was selected (from the Devices View) and is displayed, select a **Device** from the list.
- 6 In the next area ( **Manage Partition for Device:**) there are several steps that need to be completed.
  - In the Partition section, either accept the **default Partition** , or click the drop-down arrow to select another Partition. This area of the window also shows the Space; both Total and Projected Free. Note that you can select to Format the selected Partition if needed from this area. If you select to Format the Partition, you will start with a clean partition and all the available free space.
  - To force a format of the partition during the OS upgrade, click within the **Format Partition** check box.



**Important!!** If you select the Format Partition, you will lose all data on the specific partition of the device.

**Important** Do not use a partition where there is insufficient Projected Free Space for the OS Image. The Image size is noted in the Image Info tab.

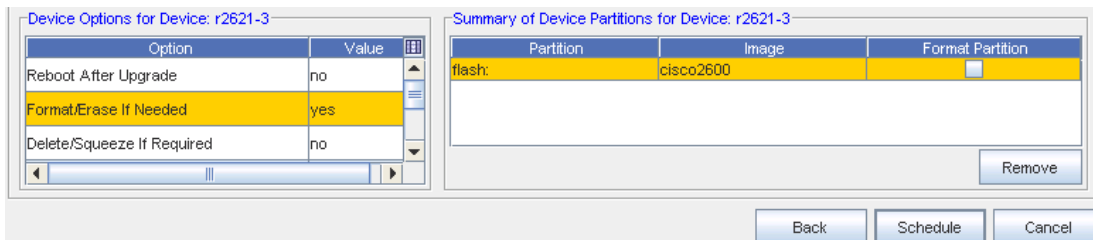
- From the **Partition FS (file system) Information** section, you can determine if you want to **Backup** or **Delete** existing files. If Backup is selected, these files will be backed up before the new OS Image is installed. If you select to Delete these files, they will be deleted before the new OS Image is installed.



- To add a selection from this partition information, first select the File Name from the list, then click **Add**. This adds the information into the Summary section (at the bottom of the window).

**Note** To ensure that the displayed information contained within the Partition FS Information section is the most current information, complete a Hardware Pull on the device. Go to the Devices View and right-click to get to the Pull option, then select Hardware Spec pull from the options list.

- At the **Selected Image part** , you can select the OS Image by **clicking on the image name** , and see the Image Info and Comments tab. This information and the comments were created when the OS image was created. Once the Image is selected, the **Image Info** and **Comments** tabs are displayed. Use the scroll bars to go to the top and bottom of the **Image Info** data. Click the **Comments** tab to view any comments previously recorded.
- 7 Once you have determined the Partition, Partition FS Information, and the Selected Image, click **Add**. This ensures that the OS image is now added and designated as the **Selected Image** . The selected image is now shown in the last portion of the Update OS Image window. The **Update** button is used if you make changes to the **Install or Copy check boxes** in the OS Image section, or if you decide to use the **Format Partition checkbox** (and force a partition) in the Partition section. Once changes to existing selections are made, click **Update** to make sure the current selections are used.



- 8 At the **Device Options for device:** section you can view the options, and then make any changes to the Value if needed. Click within the **Value** column to see and select options.

**Note** Some Device Options (in the Option section) may vary from Device Class to Device Class. For example, the following options are currently supported for CISCO IOS Routers and CISCO IOS Switches, but not supported for Juniper Device Classes.

Option	Meaning
Reboot after upgrade	This reboots/reload the device at the end of the OS Image upgrade process.
Format/Erase If Needed	<p>If yes is selected, this option allows Verifying Installation. After the installer completes, you can verify the installation (if desired) by completing the following steps:</p> <ul style="list-style-type: none"> <li>■ From any Network Node Manager sub-map window, select Tools. You should see a Network Configuration Manager menu item.</li> <li>■ From any Network Node Manager sub-map window, select Tools-&gt;SNMP MIB Browser. Then double-click Private and Enterprises. You should see voyence listed.</li> <li>■ From any Network Node Manager sub-map window, select Options-&gt;Event Configuration. You should see voyence (Enterprise ID .1.3.6.1.4.1.6615) listed in the Enterprise Identification window. (You may need to scroll through the window.) Selecting voyence populates the Event Identification window with all the Network Configuration Manager events.</li> <li>■ From the Event Configuration window, complete the following: Network Configuration Manager to reformat the partition to create more free space (if needed).</li> </ul> <p><b>Note</b> If the Format Partition check box is checked, the partition will always automatically be formatted, whether you select Yes or No as the value for this option.</p>
Delete/Squeeze If Required	If yes is selected, this option allows Voyence to delete and squeeze the partition to create more free space (if needed).
Delete Old Image After Upgrade	This deletes the old OS Image from the device partition.
Backup Current Image	This backs up the current OS Image to the Network Configuration Manager Device Server directory (\$VOYENCE_HOME/data/devserver/cm/devxfr) before the OS Image upgrade process begins.

**Note** Specifically for CISCO IOS Class B and Class C devices are supported.

#### Supported Options for Compacting CISCO IOS Non-Volatile Memory:

**Class A** - squeeze/format <partition> - Delete/Squeeze If Required or Format/Erase If Needed

**Class B** - erase <partition> - Format/Erase If Needed

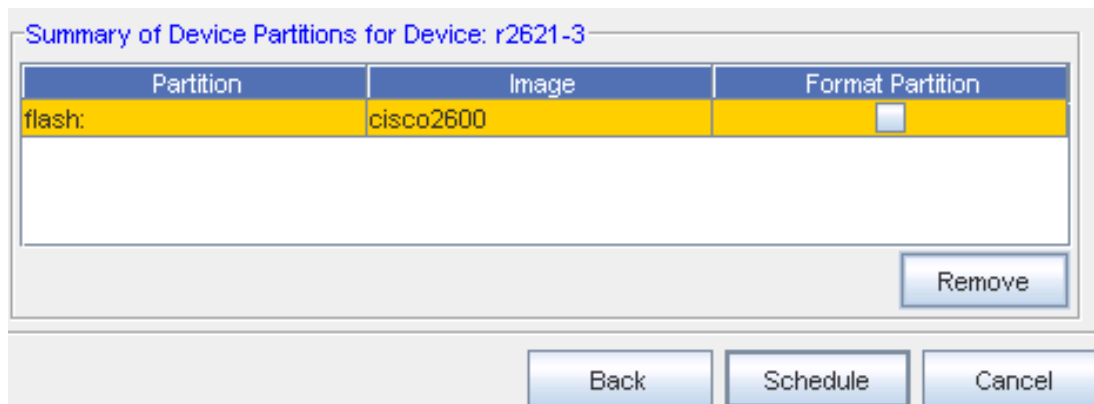
**Class C** - format <partition> - Format/Erase If Needed

If there is not enough free space available, and you have not checked the Format Partition check box, but you want Network Configuration Manager to free the space needed, select the **Format/Erase** option, or the OS Image upgrade will fail.

At the **Summary of Device Partition for Device** section, this information automatically displays a summary of the selections made for this device, after the Add or Update button has been selected. From this section, you can also Add or Remove partitions, and the eventual ending information is once again displayed within the Summary section.

To change the information contained with the Summary section, begin again from the **Selected Devices** section of the window, and then re-select options, then click **Update**. These new selections (options) are now displayed in the Summary section.

**Note** In the Partition section of the **Summary of Device Partitions** (for a specific device) there may be more than one default, however, the highest priority of the default is displayed. For example, the highest priority default for CISCO IOS devices is flash.



You can select information within the Summary section, then click **Remove** to completely remove any updates to a partition on a device. This removes the partition from the Summary listing, as well as from the Partition FS section.

- You can also use the **Back** button to return to the previous screen to begin the process again by selecting a different OS Image.
  - If you previously checked the **Format Partitions** check box, the check is also displayed as checked in this Summary section.
- 9 With all the selections made from this window, you can now click **Schedule** to schedule this OS Image Upgrade (Schedule a Push Job).

## Resyncing Devices

While viewing the Devices in either the Table or Diagram view, you are alerted (by the out-of-sync icon in the State column) that you have devices that are out-of-sync. This indicates that the running configuration for a specific device is not "in sync" with the saved device configuration, and should be **brought back into sync** to preserve the running configuration when the application is rebooted.

There are three ways to get the device back "into sync":


- Using the **Resync** button provided in the Device Properties

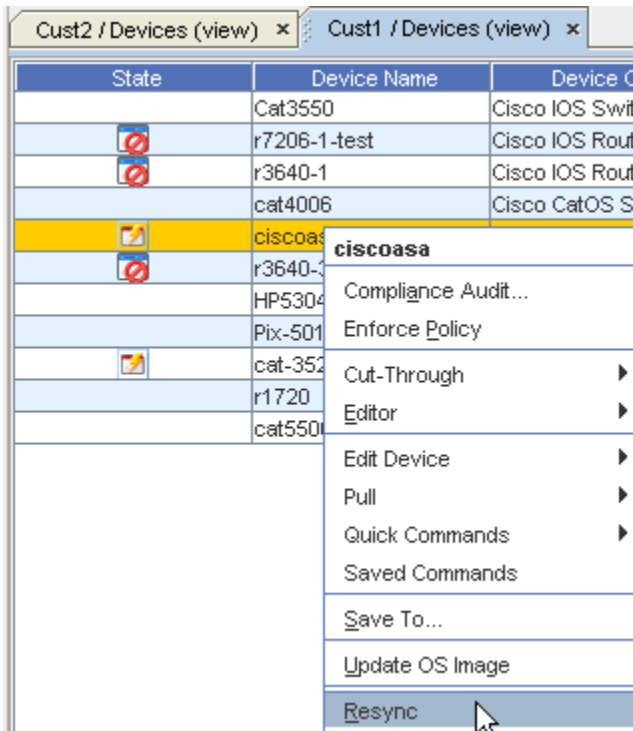
- Using the **Schedule Manager** to complete a config pull
- Using the option in the **Devices View right-click** menu

**Note** Any task that is not accessible to you from the right-click options listing (appears dimmed), automatically lets you know that you do not have the appropriate permissions to complete that task.

**Important** Make sure you refresh the Devices view after each resync is completed .

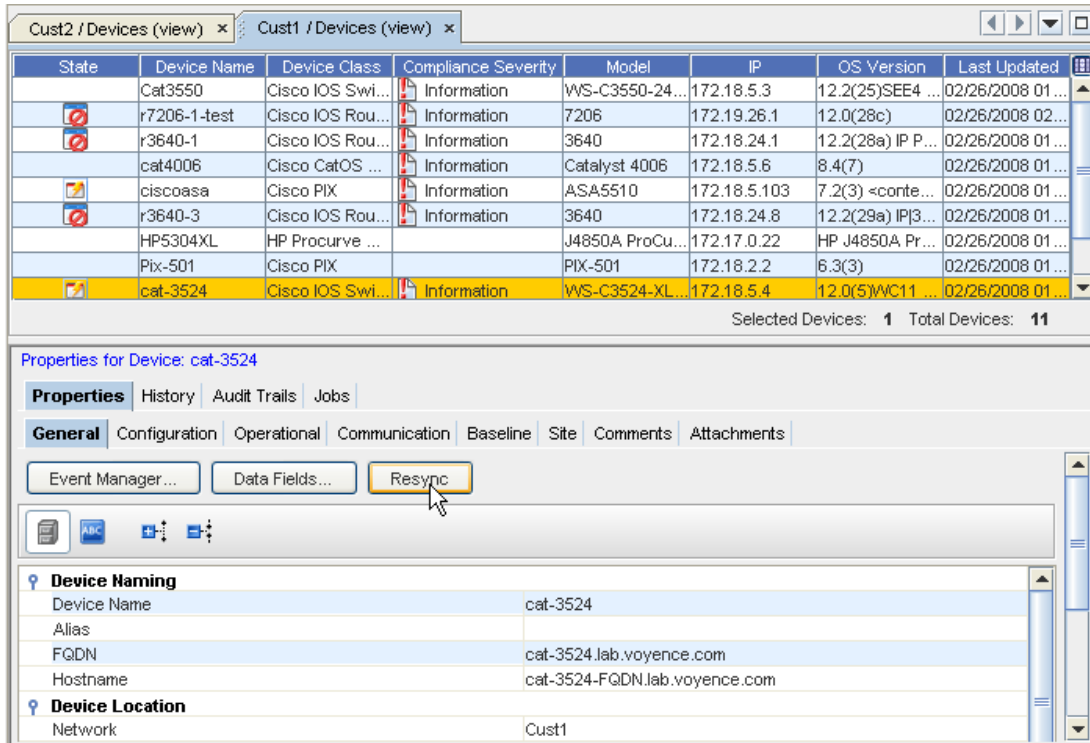
Using the right-click menu to Resync,

- 1 To bring a single device, or **multiple devices configuration** back into "sync", display the devices using the table layout.
- 2 From the Navigation tree, display the listing of devices to determine if you have any devices out of sync, as indicated by the icon  in the **State** column.
- 3 Select the **device**, then right-click on the device to show the options in the right-click menu.



- 4 Select **Resync** from the list of options to resync the device configuration.
- 5 Now, the **Schedule Push Job** window opens.

You can also view and "Sync" the device using the Properties - General tab.



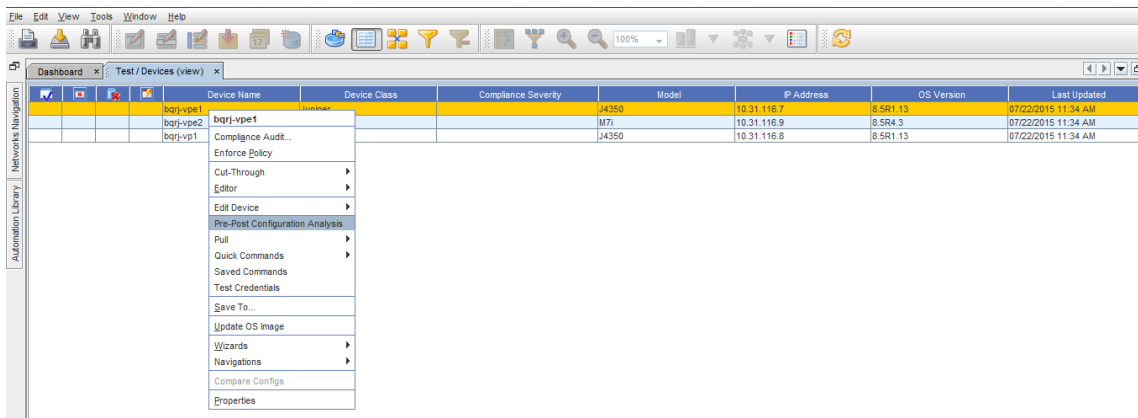
## Comparing Run/Start in Devices

For more information on **Compare Run/Start** in the Devices View, go to [Compare \(Run/Start\) Out-of-Sync Files](#).

## Wizards

Building on the concept of standardized templates, Wizards deliver intelligent automation to configuration tasks. Wizards generate Cisco IOS 12.0 and above code.

- 1 Wizards are accessible in the T able or Diagram view of any network. Select at least once device, then right-click on a device, and select **Wizards** from the right-click menu.



- 2 For more information, go to [The DNS Wizard Overview](#).

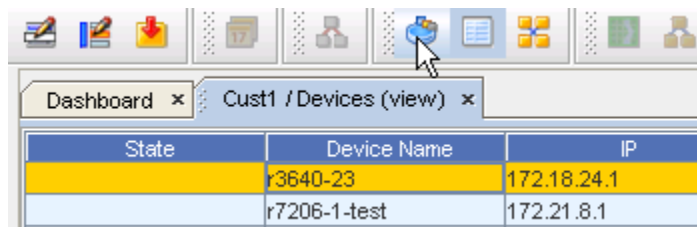
## Device Properties

### Device Properties Tabs

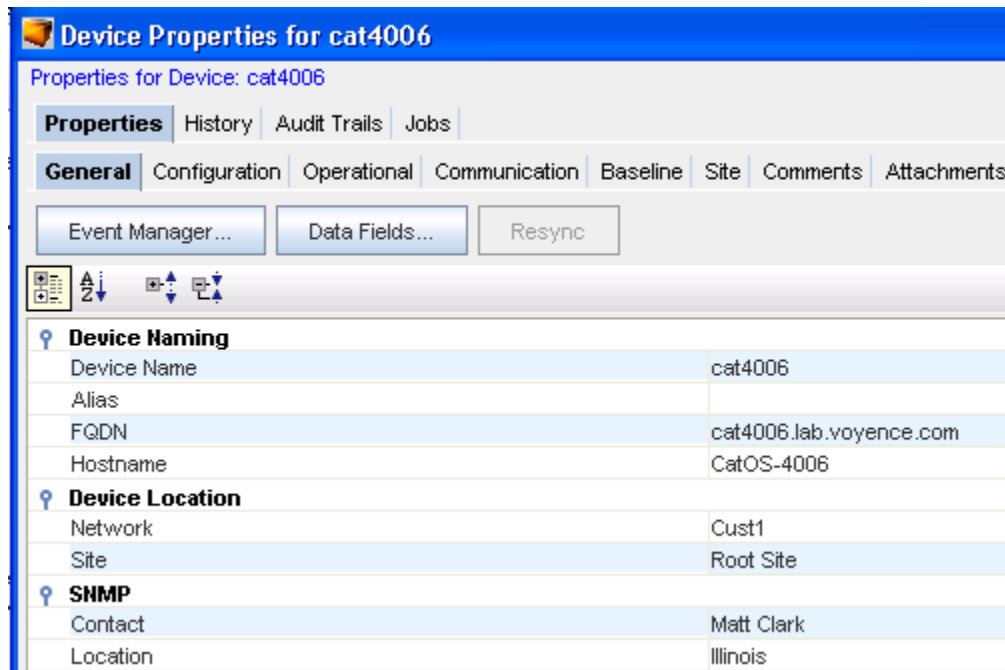
**Device Properties** contain some of the same information as do the right-click Device Properties options, however, the information is displayed differently, and may include additional information. Instead of being listed in the right-click menu, the Device Properties are displayed in tabs at the lower section of the Devices View window.

 Not all of the tabs are selectable at any one time .

This window can be displayed by selecting the **Properties** icon of the tool bar.



**Note** The properties information changes relative to the device selected in the current view.



**Device Properties for cat4006**

Properties for Device: cat4006

**Properties** | History | Audit Trails | Jobs

**General** | Configuration | Operational | Communication | Baseline | Site | Comments | Attachments

Event Manager... | Data Fields... | Resync

**Device Naming**

Device Name	cat4006
Alias	
FQDN	cat4006.lab.voyence.com
Hostname	CatOS-4006

**Device Location**

Network	Cust1
Site	Root Site

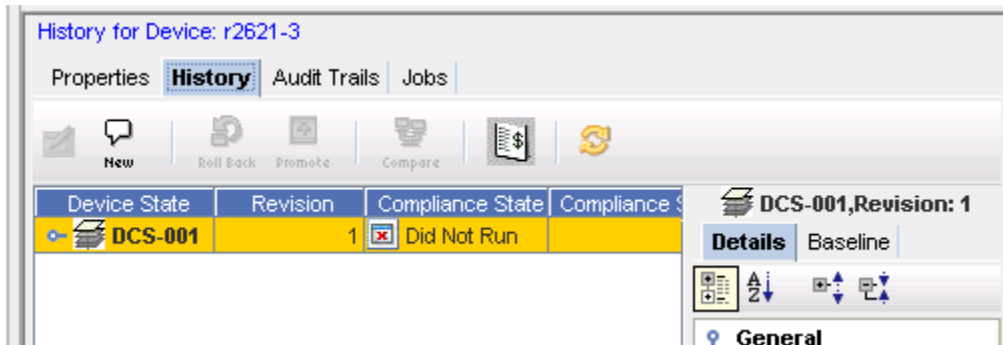
**SHMP**

Contact	Matt Clark
Location	Illinois

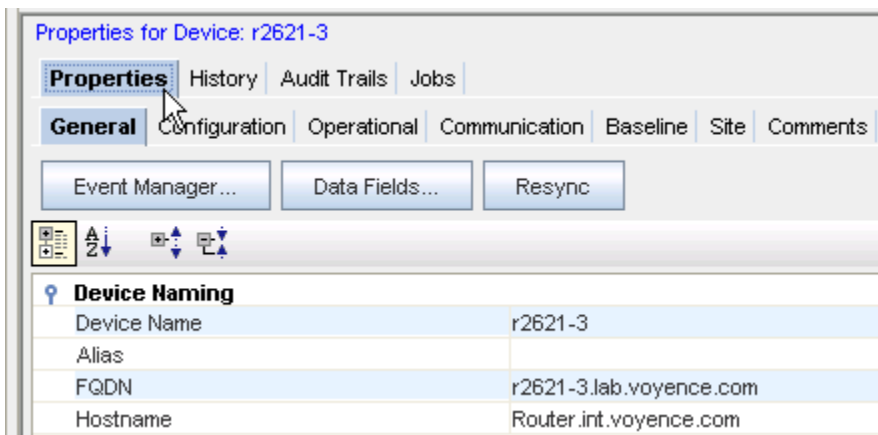
The first tab ( **Properties**) displays with **History**, **Audit Trails** , and **Jobs** tabs available.

Once Properties is accessed, the **General tab** is displayed. You can select any tab, in any order, to view information. When working with only those tabs at the Properties level (History, Audit Trails, and Jobs), the other tabs located beneath the Properties (Configuration, Operational, and so on) close.

For example, When you are viewing the **History** tab, the only tabs now available are **Audit Trails** and **Jobs**.



To once again view all tabs, click the **Properties** tab again.



Tabs contained within the Properties view are also the location where various tasks can be completed, such as in the History tab, where you can select **two or more revisions**, and then compare the revisions to view the changes made in each revision.

This table details the content of each tab within the Properties view.

<a href="#">The General Tab Overview</a>	Contains specific device information, including name, location, Device Properties, Server Location, and more
<a href="#">History Tab Overview</a>	Contains the history of tasks that have been completed on this device, including revisions. It is also where Rollback and Audits can be selected, and Data Fields can be added.
<a href="#">Working with Audit Trails</a>	Details the state of the device in reference to compliance, and when the compliance audit test was run
<a href="#">Working with Jobs</a>	Lists any jobs that have been scheduled for that device
<a href="#">Configuration Tab Overview</a>	Lists any running configurations, any previous configs, the config status, and more
<a href="#">Operational Units Tab Overview</a>	Contains a list of the data that was pulled for the device
<a href="#">Communication Tab Overview</a>	Contains all the In-Band, Out-of-Band, Cut-through communications, and allows you to update credentials
<a href="#">Baseline Tab Overview</a>	Allows you to review the network baseline config that affects the device

<a href="#">History Tab Overview</a>	Allows you to review the history on the config file
<a href="#">Site Tab Overview</a>	If the device has been assigned to a site, the site information displays on the Site tab.
<a href="#">Comments Tab Overview</a>	Allows you to enter device specific comments
<a href="#">Attachments Tab Overview</a>	Allows you to associate an external file to the network

## The History Tab

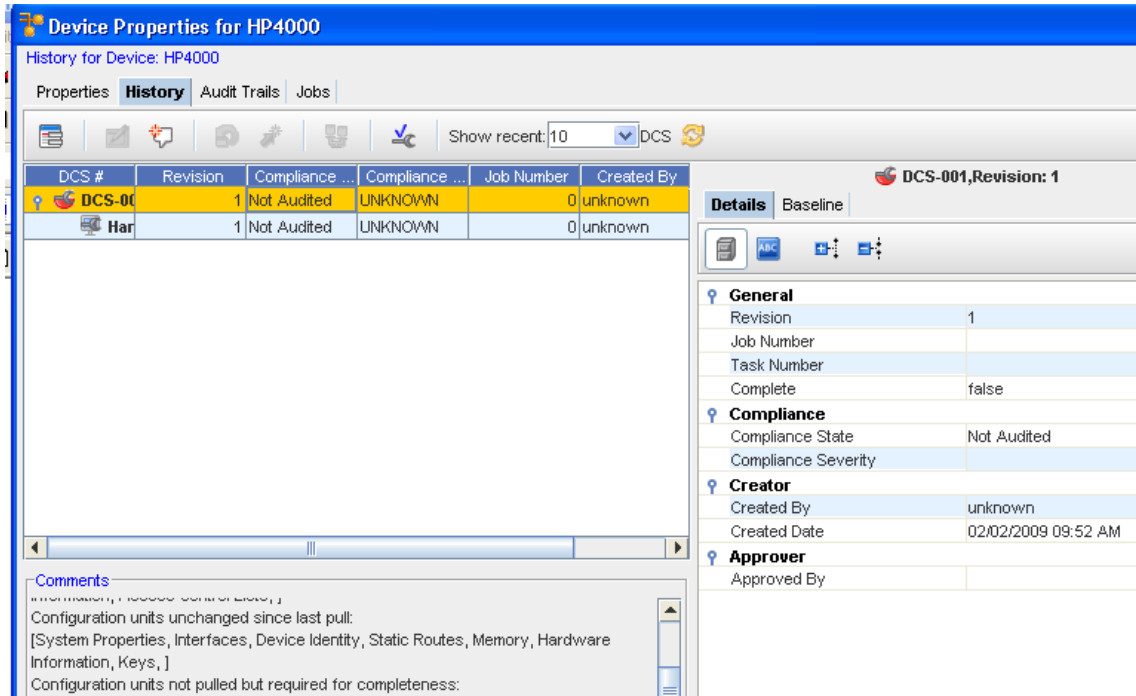
### History Tab Overview

The **History** tab displays an actual history of that device. The History tab Allows you to:

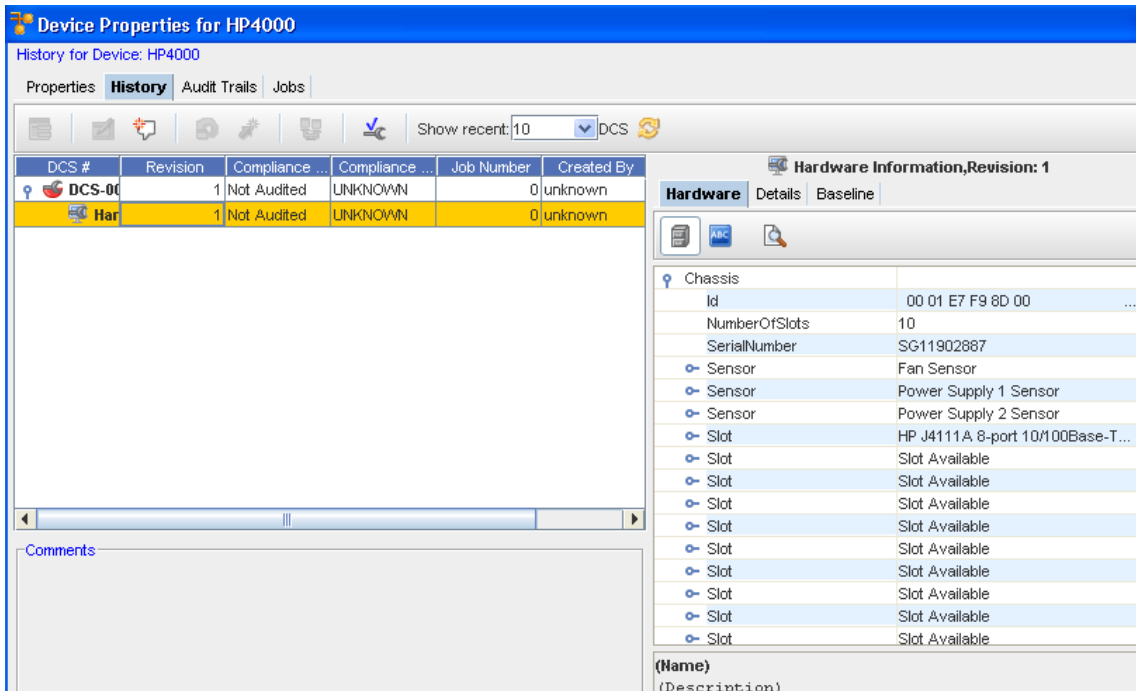
- Review the device's history and past events
- Access the Config editor
- View or Update existing Data Fields
- Create a new Revision Comment, and review all previously added comments
- Review the Baseline and Config details
- Rollback to a previous configuration revision
- Promote a Configuration
- Compare one or more configurations
- Audit the configuration - allowing you to select the Standard, and then run a Compliance Audit. You can multi-select revisions and audit against a Standard to find historical compliance (when the device has gone out of compliance).
- Refresh the view after changes
- View the hardware details (when **Hardware** is selected from the Device State column)

You can also Audit the **Device Properties** feature.





You can review the **Hardware**, the **Details**, and the **Baseline** of the current config.

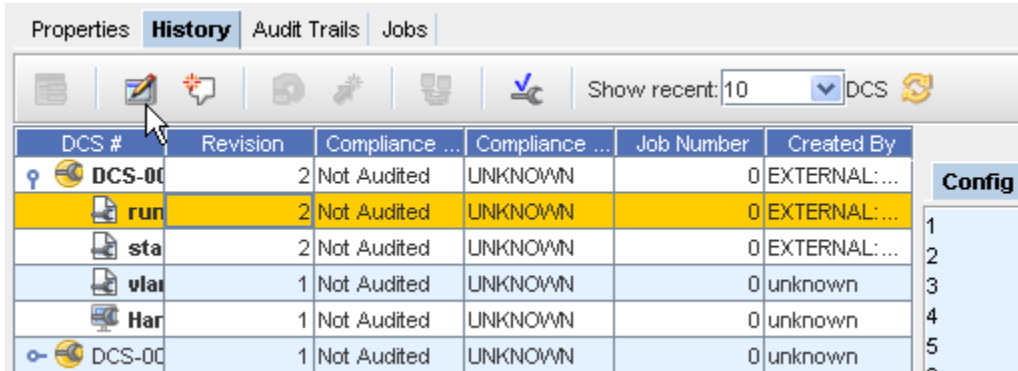


- **Comments** on the Configuration can be viewed as well.
- Note that you can view ... the Device State Configurations by selection the drop-down beside the **Show Recent** option.

### Changing the Config file

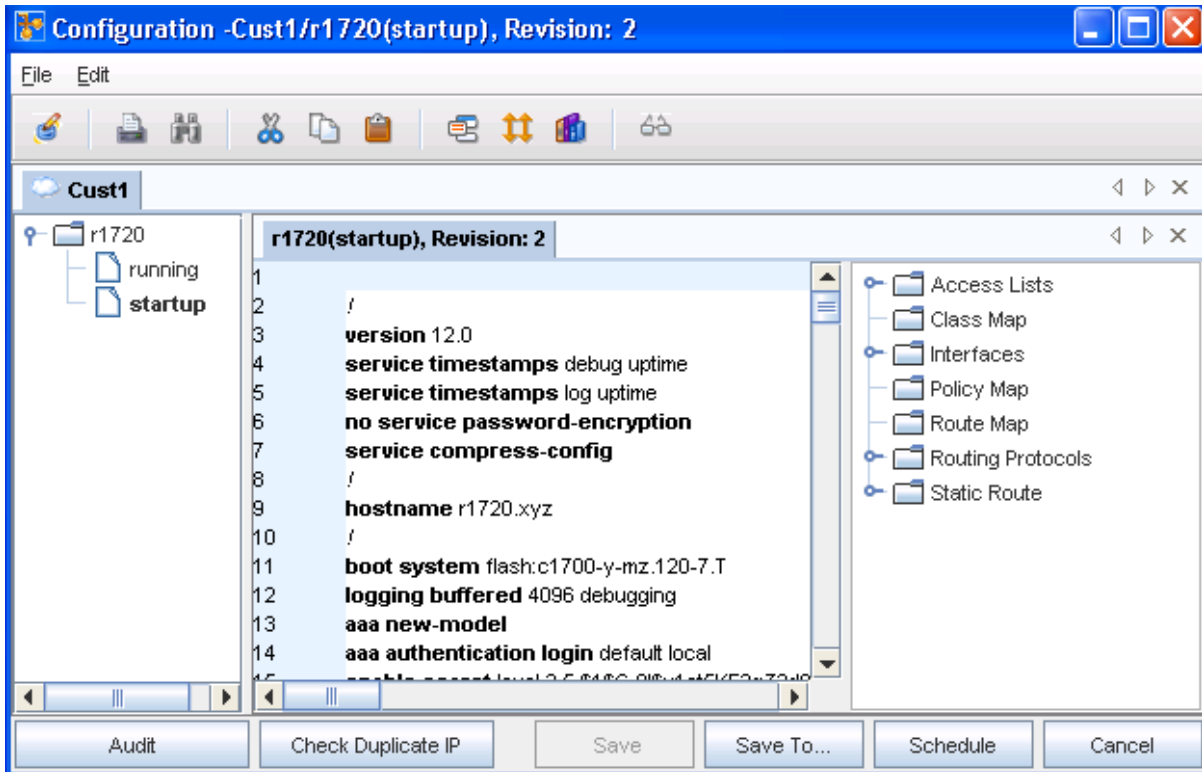
To make changes to the Config file,

- 1 In the **History** tab, select a running config , and then click the **Config Editor** icon.

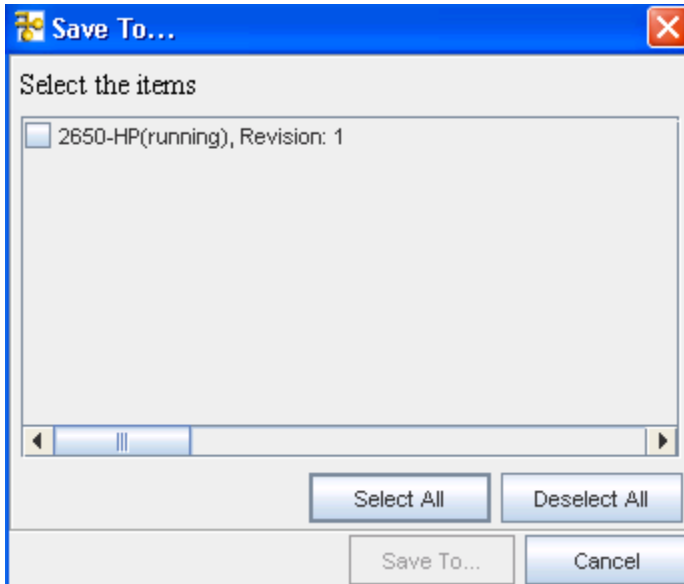


The Config Editor window opens.

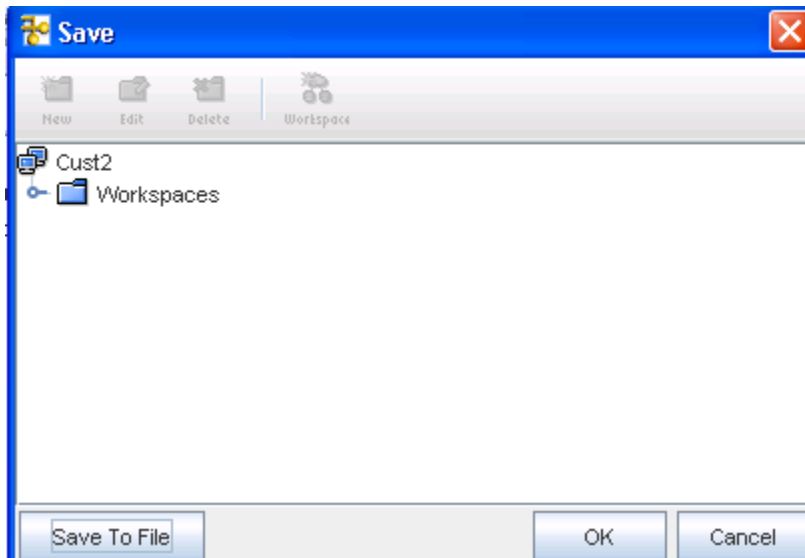
- 2 Make any needed revisions to the information.
- 3 Click **Preview** to preview your changes, and then click **Save To...** to save your changes.



- 4 From there, in the **Save To..** window (shown below), you can select the items to save by clicking in the check box beside each device, or by using the **Select All** bar. then clicking **Save To....**



5 Now, use the **Save** window to determine where you want to save this.



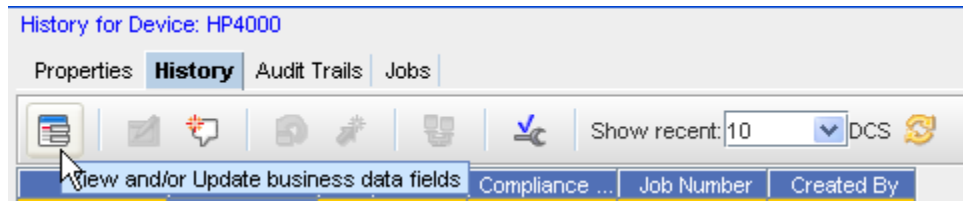
6 Click **Ok** when you have made your save location selection.

#### Viewing or Updating a Data Field from the History or Interfaces tab

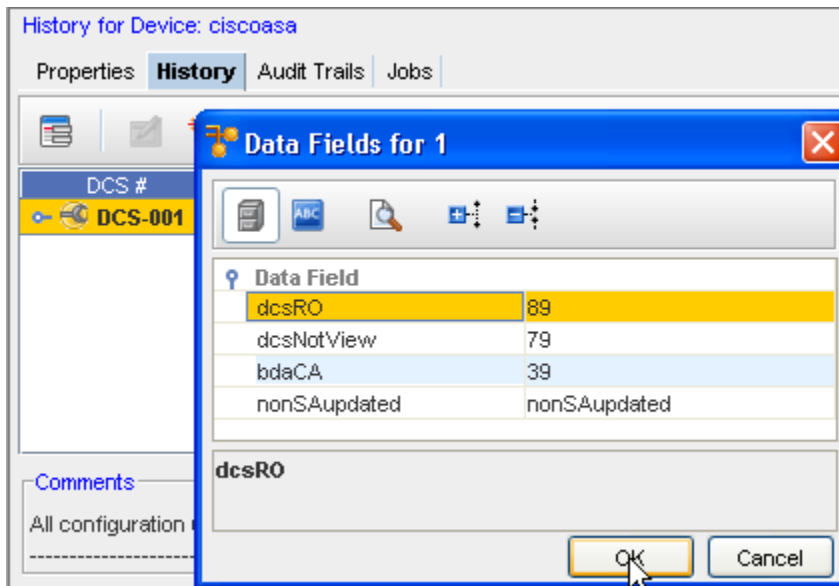
---

**Note** Data Fields are used to create attributes, and to assign values to devices.

---



- 1 From the **Devices View**, select to show the Device **properties** of a single device. Once the Properties tabs are displayed, click on the **History** tab (or the **Interfaces** tab).
- 2 Select the **View/Add Data Fields** icon to open the Data Fields window where you can select to add any of the available fields. If needed, expand the Data Fields listing, then select the appropriate option from the list.



- 3 Click **Ok**.

---

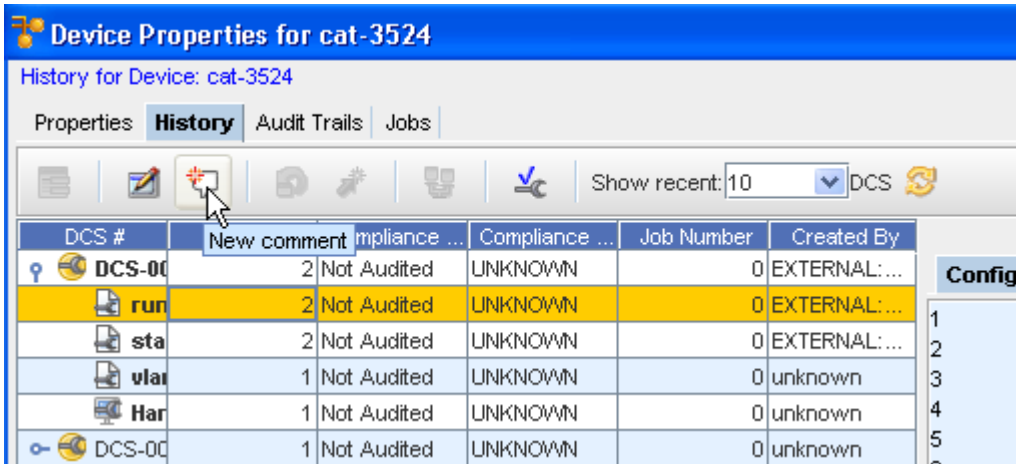
**Note** You must have System Administration privileges to work with the Device Data Fields. You must also have View Permissions to view the data fields information.

---

### Adding Revision Comments

To add revision comments,

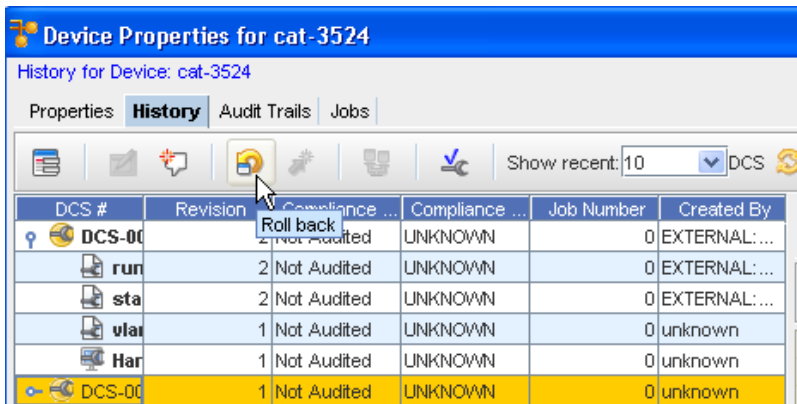
- 1 In the **History** tab, click the **New** icon to see the Revision Comments window for that device.



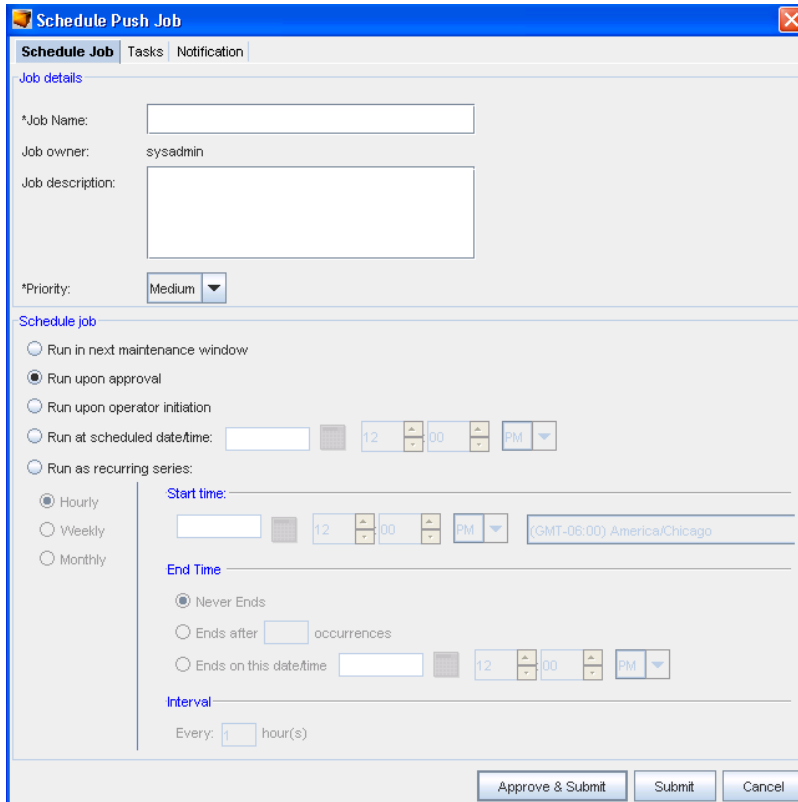
- 2 Enter any **new comments** in the Add Revision Comments window, then click **OK**. Your latest comments are now added to the top of the comments window.

### Rolling Back to Baseline option

- 1 From the **History tab**, select a revision, then select the **Roll Back** icon. This will roll the device back to the previous configuration level, prior to the latest configuration changes.



The Schedule Push Job window then displays.



- 2 For information on using this window, go to [Scheduling a Run Time](#).

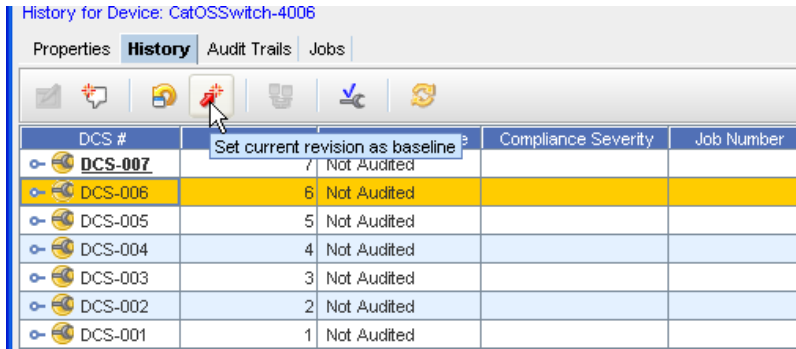
### Set the Current Revision as the Baseline

---

**Important** A Baseline must have already been set for the Network.

---

- 1 From the **History** tab in the Device Properties, you can access the **Set Current Revision to Baseline** icon to set the baseline to the current configuration version.
- 2 After selecting a Device from the Devices View, then selecting the **Properties** icon, you can then access the **History** tab.
- 3 If there is more than one revision shown (in the **Revision** column) you can promote the latest revision. For example, if you have two revisions shown; a number 1 and a number 2, then you can surmise that changes to the baseline have been made, and you need to promote the latest baseline revision (2).



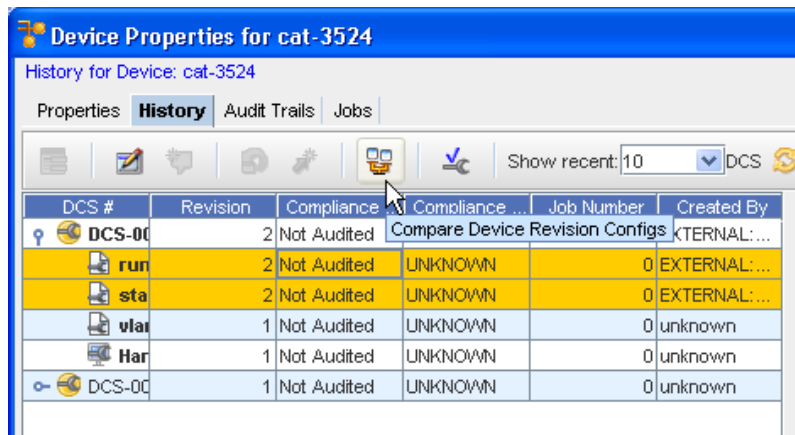
- 4 Select the **latest revision**, then click the **Set Current Revision to Baseline** icon to set the current configuration version. This will then be the current baseline configuration for the Device.

### Comparing Configs

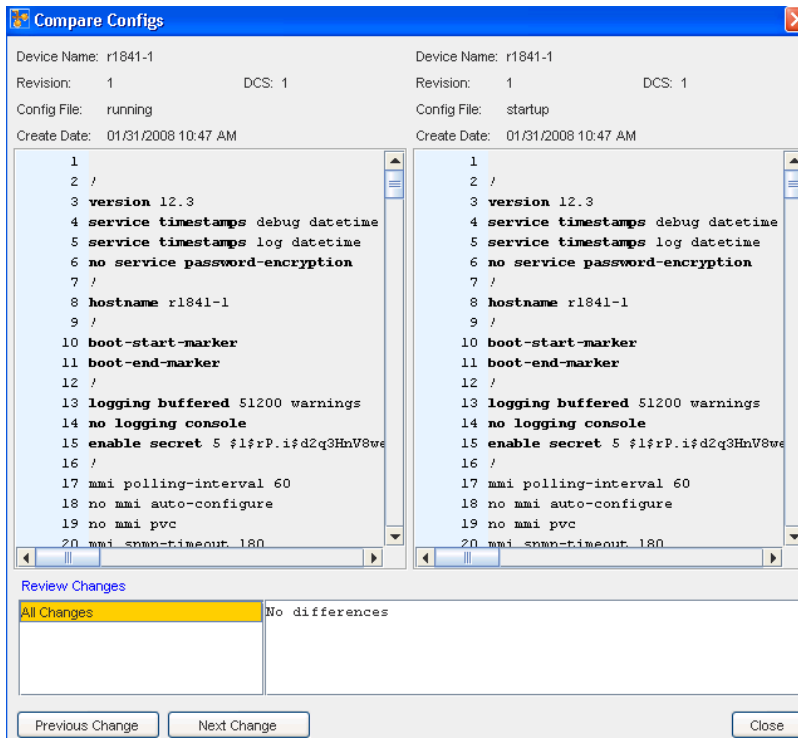
This feature allows you to compare two configuration file revisions. In the Compare Configs view, each configuration displays in its own window, and is not editable. When viewing the changes, red indicates lines deleted, blue indicates lines modified, and green indicates where lines have been added.

To Compare Configs,

From the **History** tab, you can compare any two revisions that you select.



- 1 Select (highlight) the **two revisions** you want to compare (holding down the Shift key, and then clicking the revision).
- 2 Now, select the **Compare** icon (as shown above). The Compare Configs window opens.



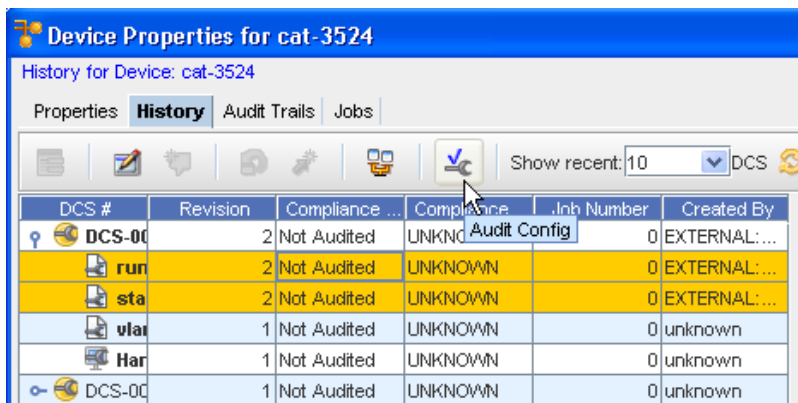
- 3 Review the previous changes by accessing the **Previous Change** button, then continue reviewing all the subsequent changes using the **Next Change** button.
- 4 Click **Close** when you have reviewed the Config comparison information.

### Running a Compliance Audit

You can see which of the configurations are **Compliant or Non-Compliant** .

To complete an Audit,



- 1 From the **History tab**,select a Revision, then select the **Audit Config** icon.



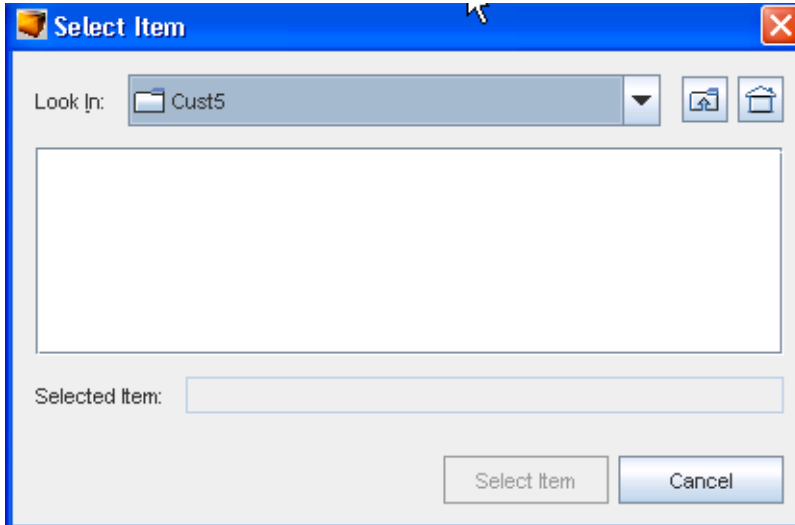


- From the Select Item window, click the drop-down arrow.

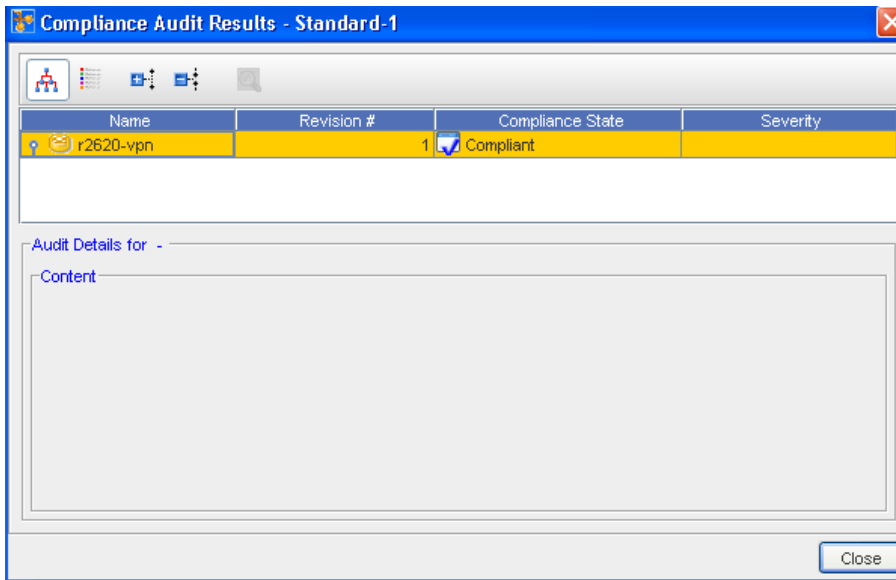
---

**Note** You can use the two icons   (Up one Level and Home) to expand or contract the listing contents).

---



- Make your selection from the list, then **select** the Item.
- At the Compliance Audit Results window, your results are displayed.




---

**Note** **Green** is Compliant, and **red** designates Non-Compliant.

---

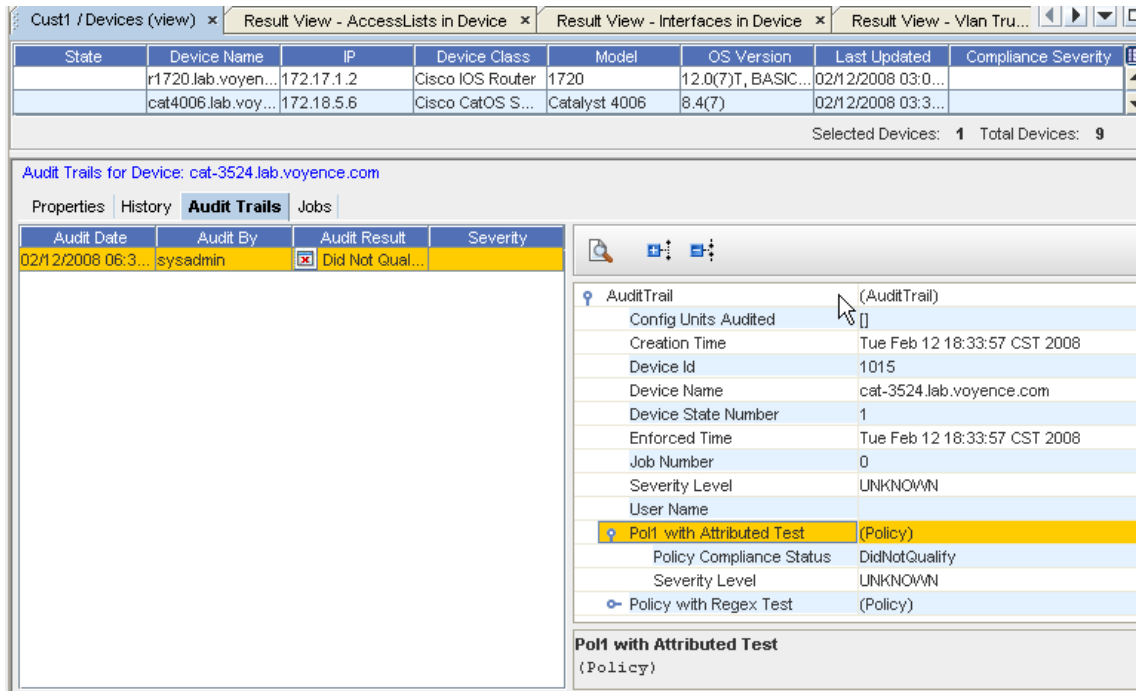
- Click **Close** when you have reviewed the audit results.

## The Audit Trails Tab

### Working with Audit Trails

In the **Properties** tabbed view, you can access the **Audit Trails** of any device.

Once the Audit Trails are accessed, information pertaining to any audits for that device are listed. Information contained within this tab is **read only**.



To see detailed information, click on the items listed in the right, and expand the topics.

Within the Audit Trail information you can use the following:



- Show/Hide the Description area
- Expand or Collapse the Audit Trail items

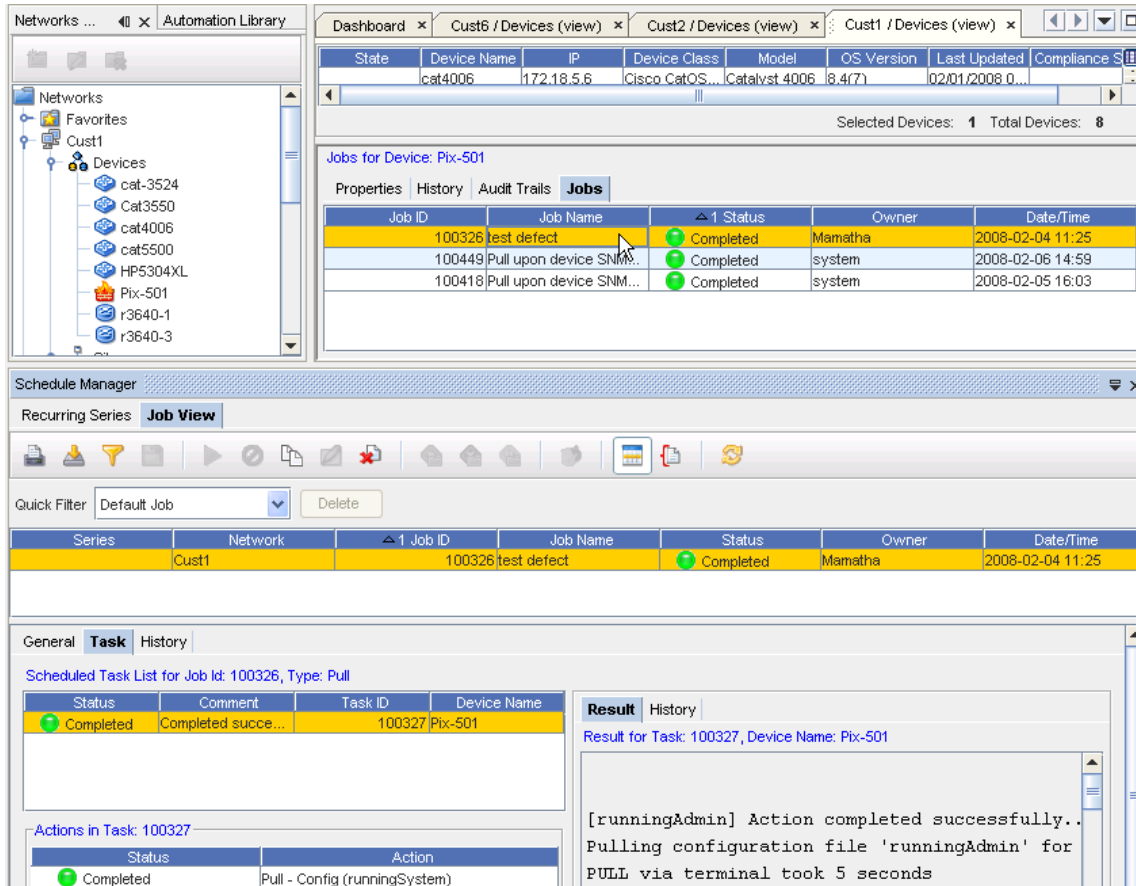
## The Job Tab

### Working with Jobs

From the **Properties** tabbed section, you can view any jobs that have been run against any device. By first selecting a device, then selecting the **Jobs** tab in Properties you can retrieve job information. This information is **read only**.

Make sure to click within any **column heading** to see if more columns headings are available for display, and thus more job information is available.

While reviewing the job information on any specific device, clicking on any actual job information in any column will open the **Schedule manager** .



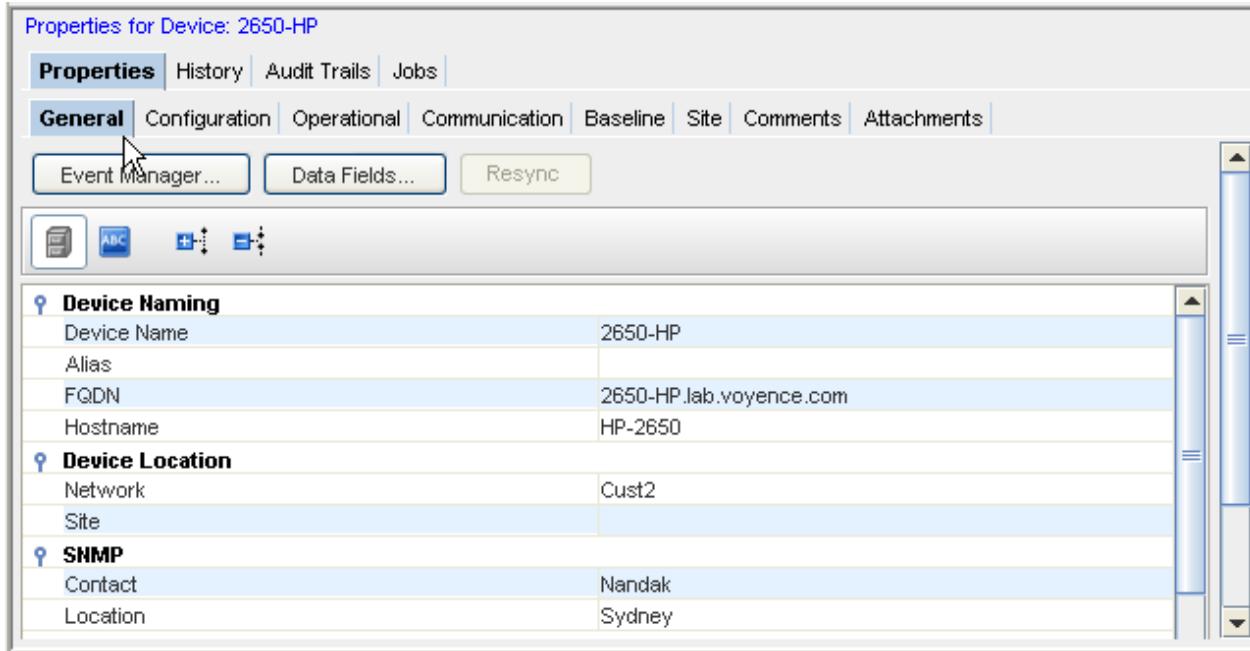
For more information, go to [Schedule Manager Overview](#)

## The General Tab

### The General Tab Overview

This window can be displayed by selecting the **Properties** icon in the menu bar, or from **Properties** when displaying the Devices view. The General tab contains specific Device information.

**Note** To expand the properties window, **drag and drop** the line separating the listing from the Properties tabs. This allows you to display more device properties information.



### Using the General Tab

You can access the [Event Manager Overview](#) from the General tab. Notice the Event Manager opens to display logs of event information and activity.



From this tab, you can also access **Data Fields** . This allows you to view extra Metadata attributes (data fields). The attributes are set up using Public API's, or from System Administration, as described in [Adding a Data Field](#).

You can also use this tab to [Resync Device Configurations](#) devices. This designates if the current running configuration is different than the start-up configuration. You can use the **Resync** button to bring your device's configuration back into sync with the database. This is only displayed if you actually have some devices that are currently out-of-sync.

### Task bar



These tasks can be completed within the General tab.

Icon	Task
	Categorize
	Sort Alphabetically



Expand the listing



Collapse the listing

### Information included within this tab,

Following are the sections of information contained within this tab.

#### Device Naming

This includes:

- Device Name
- Alias
- Fully Qualified Device Name (FQDN)
- Hostname

#### Device Location

This section of the General tab displays the device location.

- Network
- Site

#### SNMP

This section gives SNMP information.

- Contact
- Location

#### Device Properties

This includes:

- Device ID
- State
- Type
- Vendor
- Model
- Operating System
- Serial Number
- and All column headings you selected from the Devices View. See [Displaying Column Headings in the Devices View](#) for more information.

#### Server Information

This section details the server information.

- Name
- Type

Data Fields

## Resync Device Configurations

While viewing the Devices in either the Table or Diagram view, you are alerted (by the out-of-sync icon in the **State** column) that you have devices that are out-of-sync.

This indicates that the running configuration for a specific device is not "in sync" with the saved device configuration, and should be brought back into sync to preserve the running configuration when the application is rebooted.

There are three ways to get the device back "into sync":


- Using the **Resync** button provided in the **General tab** of Device Properties
- Using the **Schedule Manager** to complete a config pull
- Using the option in the **Devices View** right-click menu

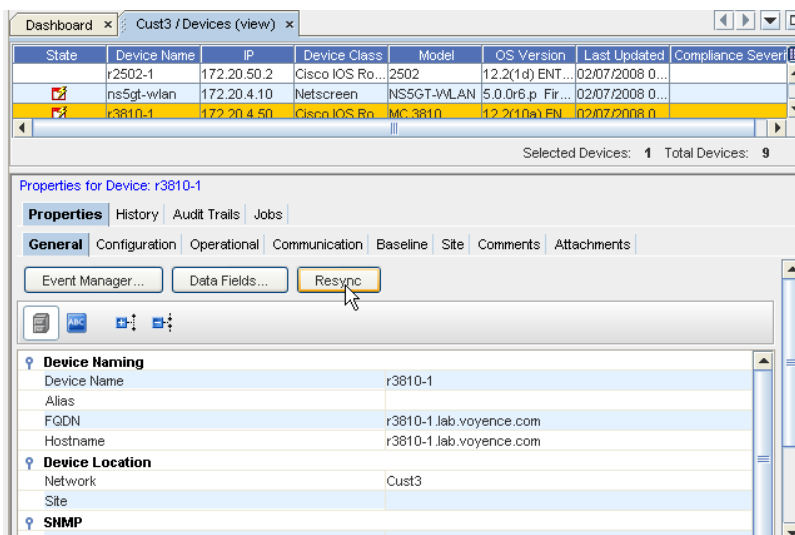
---

**Important** Make sure you refresh the Devices view after each resync is completed .

---

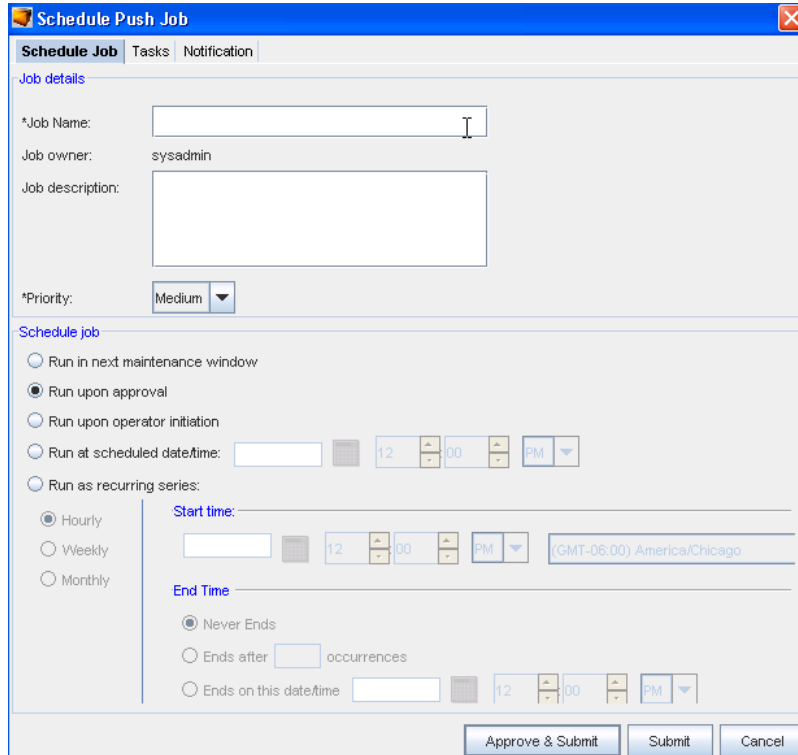
Using the Resync button,


- 1 To bring a single device, or **multiple devices** configuration back into "sync", display the devices using the Table layout.
- 2 From the Navigation tree, display the listing of devices to determine if you have any devices out of sync, as indicated by the icon  in the **State** column.
- 3 Next, select that single device, or select multiple devices from the list, then click the **Properties** icon on the menu bar.



**Note** This Resync button is only available if there are any "out-of-sync devices" in the Device list.

- 4 With the Device Properties displayed, go to the **General** tab. With the device selected, click the **Resync** button. The **Schedule Push Job** window opens, where you complete the information needed for the push job.



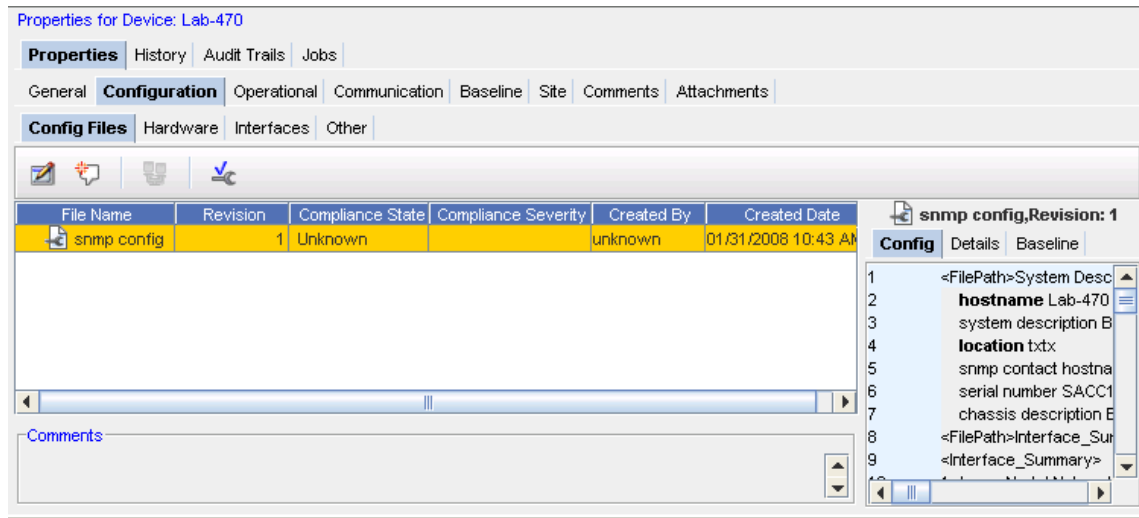
- 5 See [Schedule Push Job](#) for details on how to complete this action, including how to work with each tab.
- 6 After the application completes a Config pull (to bring the device configuration into sync) **select the Refresh icon**  to refresh your Devices view.

**Note** The device is no longer in the "out-of-sync" state in the Devices View. This indicates that the device's running configuration is now identical to the start-up configuration .

## The Configuration Tab

### Configuration Tab Overview

From the Devices View, when Properties is selected from the tool bar, the **Configuration** tab is available.



From this tab you can access:

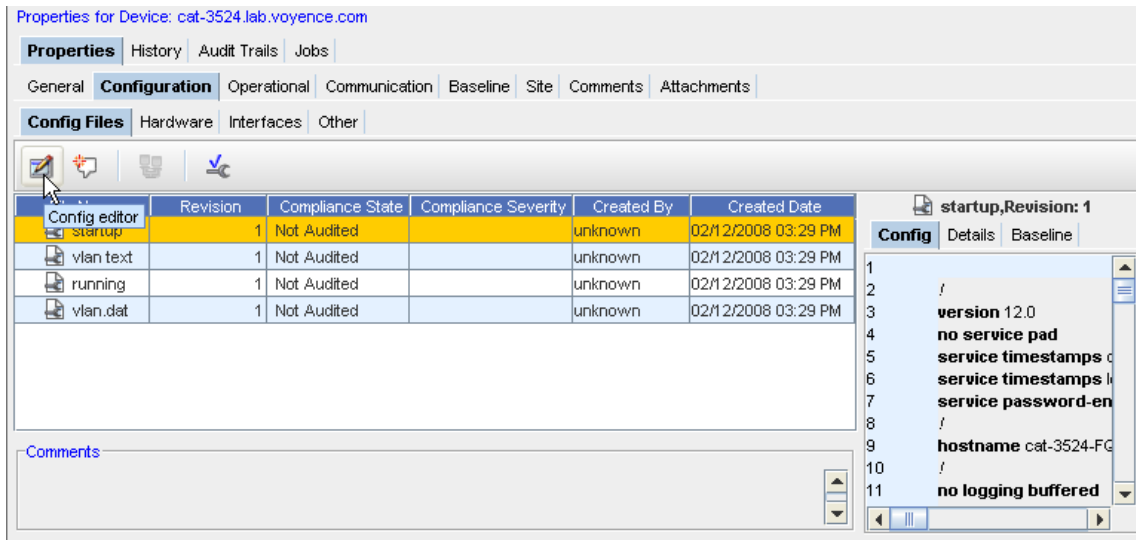
- Config Files
- Hardware
- Interfaces
- Other

## Config Files

### Accessing and working with Config Files


To make changes to the Config file,

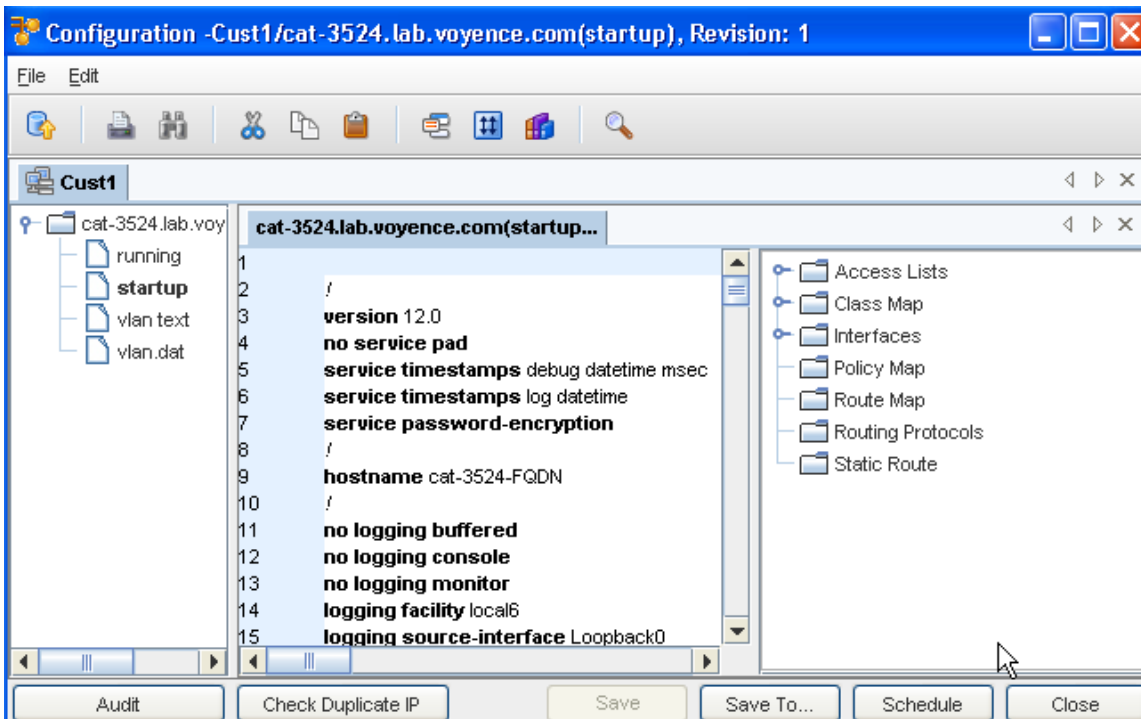
- 1 In the **Config Files** tab in the **Configuration** section of the **Device Properties**, select a running config, and then click the **Config Editor** icon.



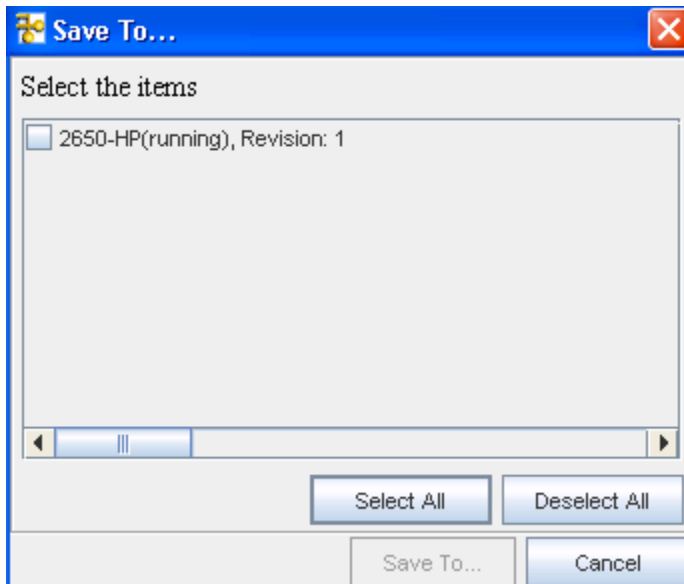
The Config Editor window opens.



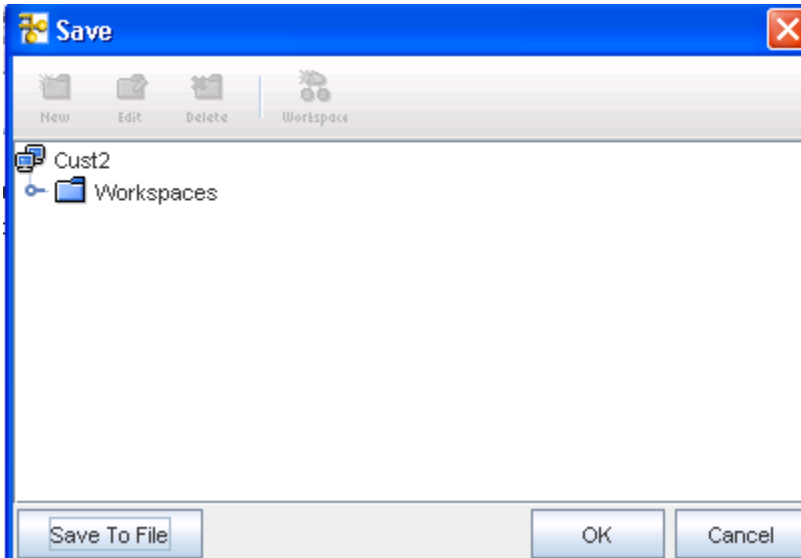
- 2 Make any needed revisions to the information.
- 3 Click **Preview**  to preview your changes, and then click **Save To...**, to save your changes.



- 4 From there, in the **Save To..** window (shown below), you can select the items to save by clicking in the check box beside each device, or by using the **Select All** bar., then clicking **Save To....**



- Now, use the **Save** window to determine where you want to save this.

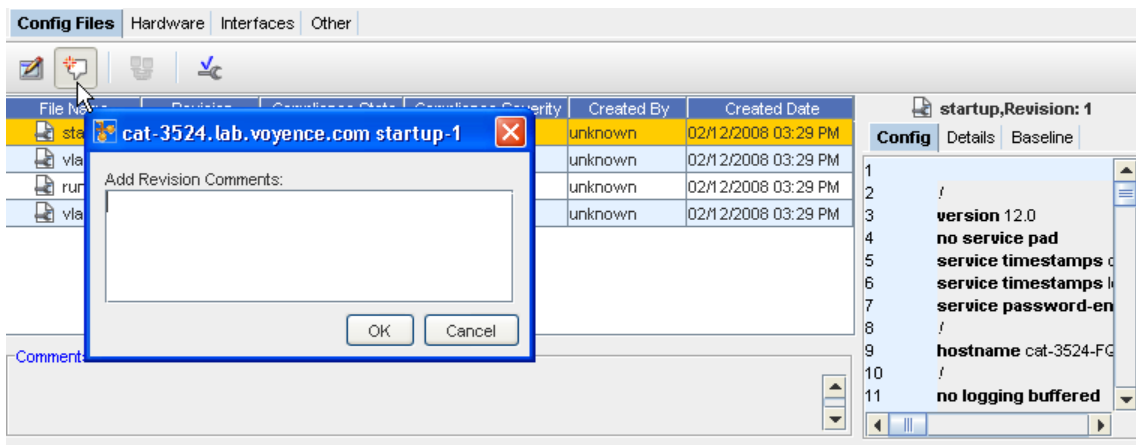


- Click **OK** when you have Saved your config.

### Adding a New Comment

To add revision comments,

- In the **Configuration** tab, click the **New** icon to see the Revision Comments window for that device.



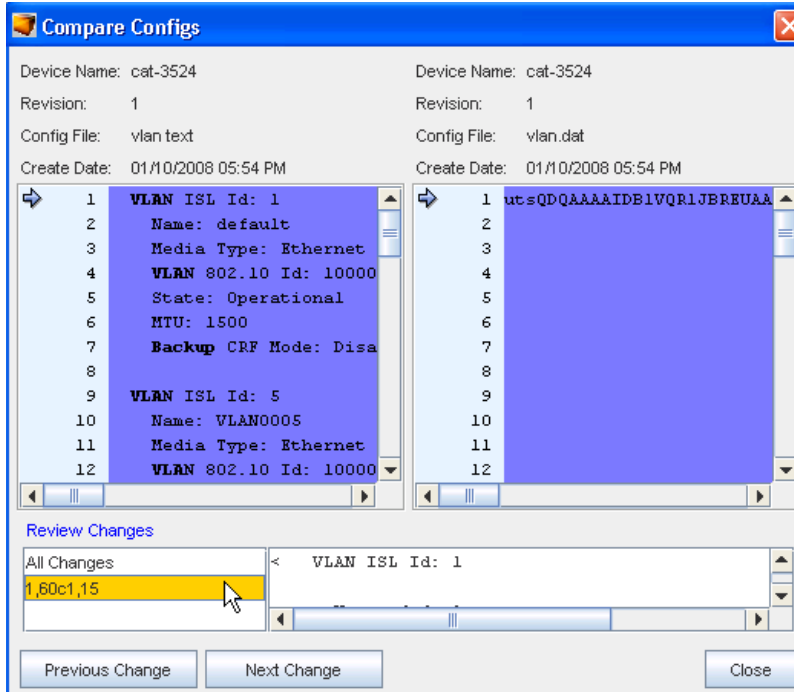
- Enter any new comments in the Add Revision Comments window, then click **OK**. Your latest comments are now added to the top of the comments window.

## Comparing Device Revision Configs

- 1 From the **Baseline** tab, select two revisions , then click the **Compare Device Revisions** icon



. At the Compare Configs window, you can compare the difference in configurations.



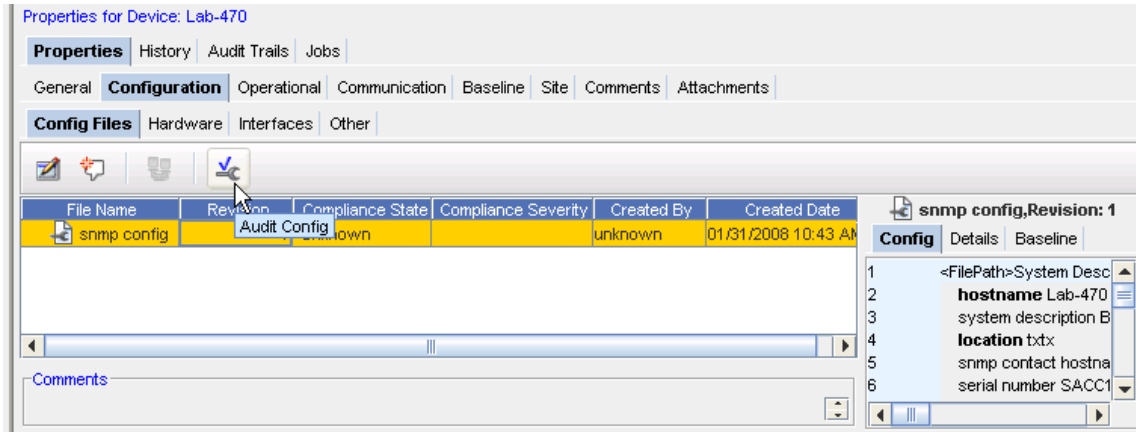
- 2 You can also select to view **Previous** and **Next** changes, or click within the **Review Changes** window.
- 3 Click **Close** when you have completed your review of this information.

## Audit Configuration



You can see which of the configurations are **Compliant** or **Non-Compliant** by the icons displayed in the Compliance State column.

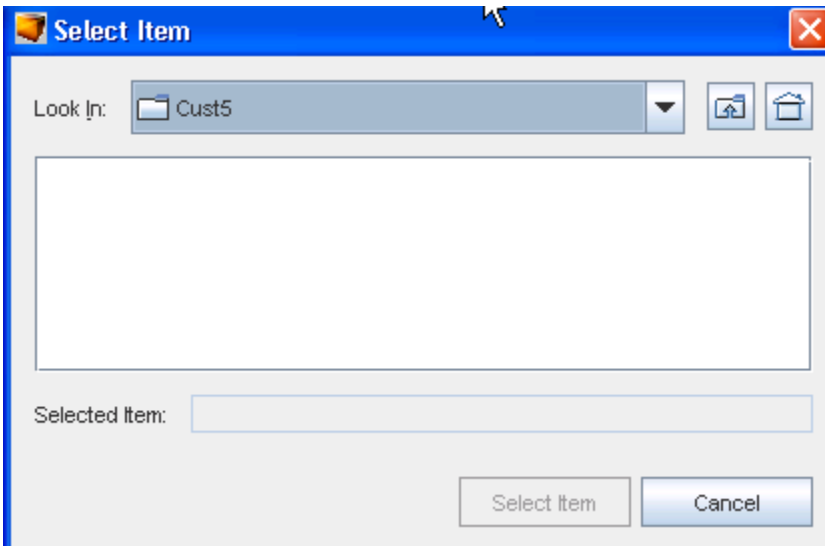
To complete an Audit,

- 1 From the **Configuration** tab,select a Revision, then select the **Audit Config** icon.

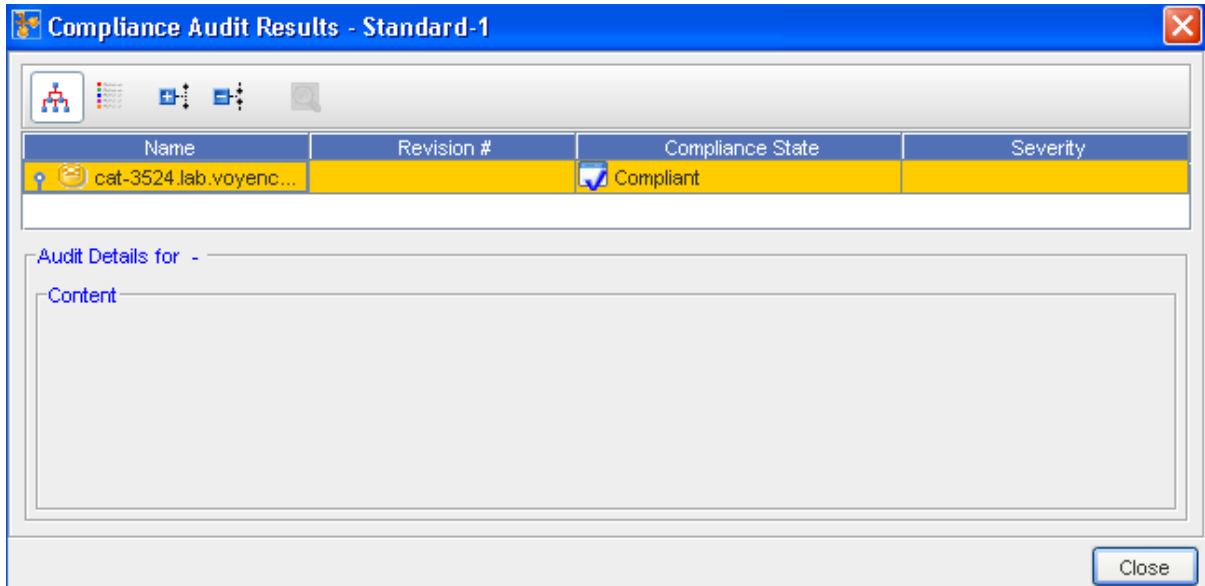


- From the Select Item window, click the drop-down arrow.

**Note** You can use the two icons   (Up one Level and Home) to expand or contract the listing contents.



- Make your selection from the list, then **select** the Item.
- At the Compliance Audit Results window, your results are displayed.



**Note** Green is Compliant, and red designates Non-Compliant.

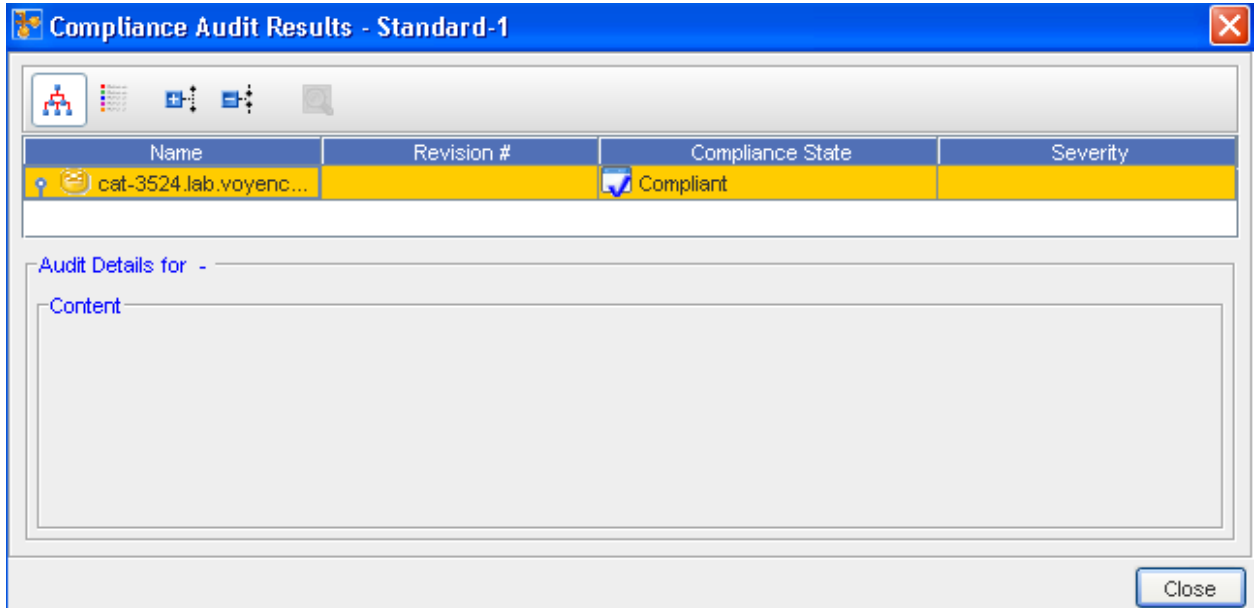
5 Click **Close** when you have reviewed the audit results.

See [Audit Compliance Window](#) for additional information.

### Audit Compliance Window

1 To work within the **Audit Compliance Results** window, first select the device from the listing.

2 Next, use the icons to view or hide information, or to rearrange the order of devices.



Move your cursor over the icons to view the various options.


You can see the Compliance State.

## Hardware

### Hardware Information

The **Hardware** information can be viewed from within the Configuration tab when Device Properties are displayed.



- You can Categorize or put in Alphabetical order
- You can also select to Show  or Hide the hardware description (located at the bottom of the form).

The screenshot shows the 'Hardware' tab in the Network Configuration Manager. The 'Physical Hardware' section is active, displaying a table of device properties. The 'SerialNumber' field is highlighted in yellow. Below the table, the 'SerialNumber' is also displayed as a text field.

Property	Value
Chassis	Cisco Catalyst c2950 switch with 24 10/100 BaseT...
Description	Cisco Catalyst c2950 switch with 24 10/100 BaseT...
FirmwareVersion	12.1(22)EA4
HardwareVersion	B0
Model	WS-C2950-24
Revision	12.1(22)EA4
SerialNumber	FAB0530W1LX
Memory	
Port	10/100BaseTXFast Ethernet
Port	10/100BaseTXFast Ethernet
Port	10/100BaseTXFast Ethernet
Port	10/100BaseTXFast Ethernet

**SerialNumber**  
FAB0530W1LX

Note that you can access both Memory and File System information.

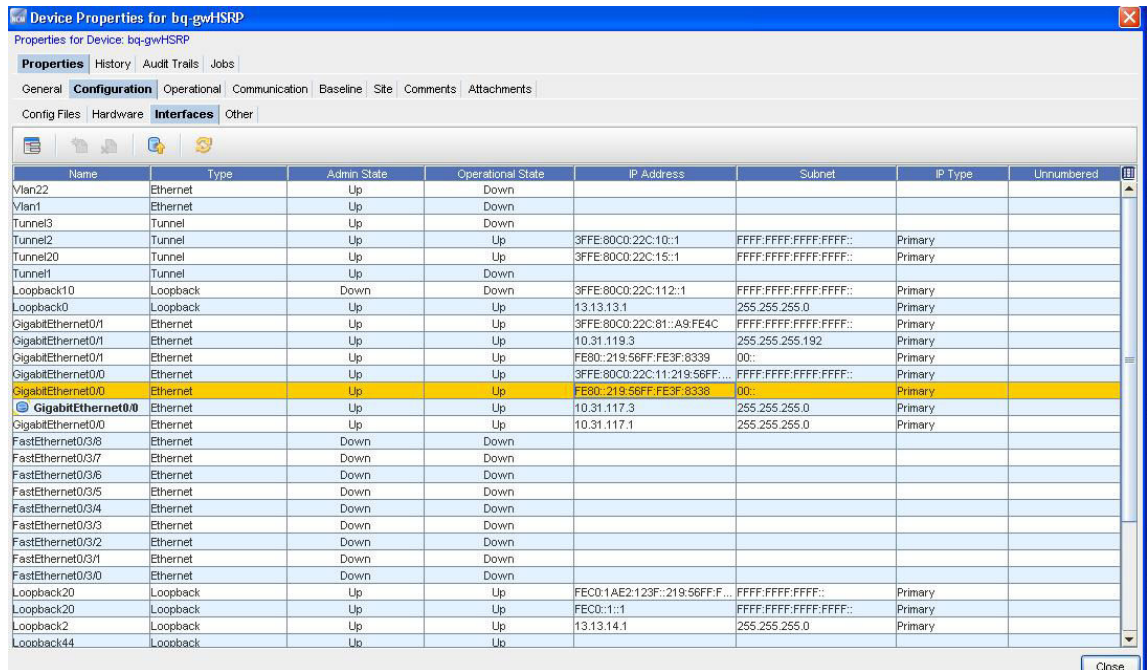
- 1 Click **Memory** or File **System** (under the **Physical Hardware** heading).
- 2 Click **Close** when you have viewed the Device OS information.

## The Interfaces Tab

### Interfaces tab (within Configuration)

The **Interfaces** tab provides a listing of all the **physical and logical** interfaces that are configured on the selected device, including their status. The Management interface is the Interface IP used to manage the device in Network Configuration Manager. Management Interfaces can be changed from this tab.

This information can be displayed by selecting the **Properties** icon, and from the **Configuration** tab from the Device Properties.



The **Interfaces** tab provides a listing of all interfaces that are defined in the config file. This tab details the interfaces information, including Name, Type, Admin State, IP Address, Subnet Mask, Tags, and DNS Interfaces.

The Interfaces tab also allows you to [Viewing or Updating a Data Field from the History or Interfaces tab](#) for a specific interface.

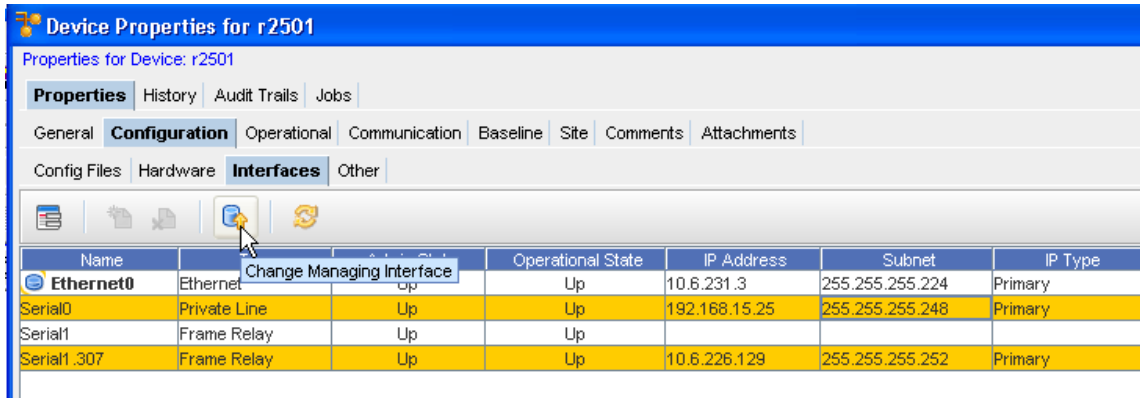
**Note** Notice that the **Add** and **Delete**, as well as the **Change Managing Interface** icons are grayed out. You cannot add, delete, or change the managing interface anywhere but **within a Workspace**.

To manage the Interfaces, see [How to Managing Interfaces](#)

### Managing Interfaces

To change the managing interface,

- 1 Select an **IP Address** from the list that you want to change to the current managing interface . When you select another IP Address from the list of addresses, the **Change Managing Interface** icon is enabled.
- 2 Click the **Change Managing Interface** icon.



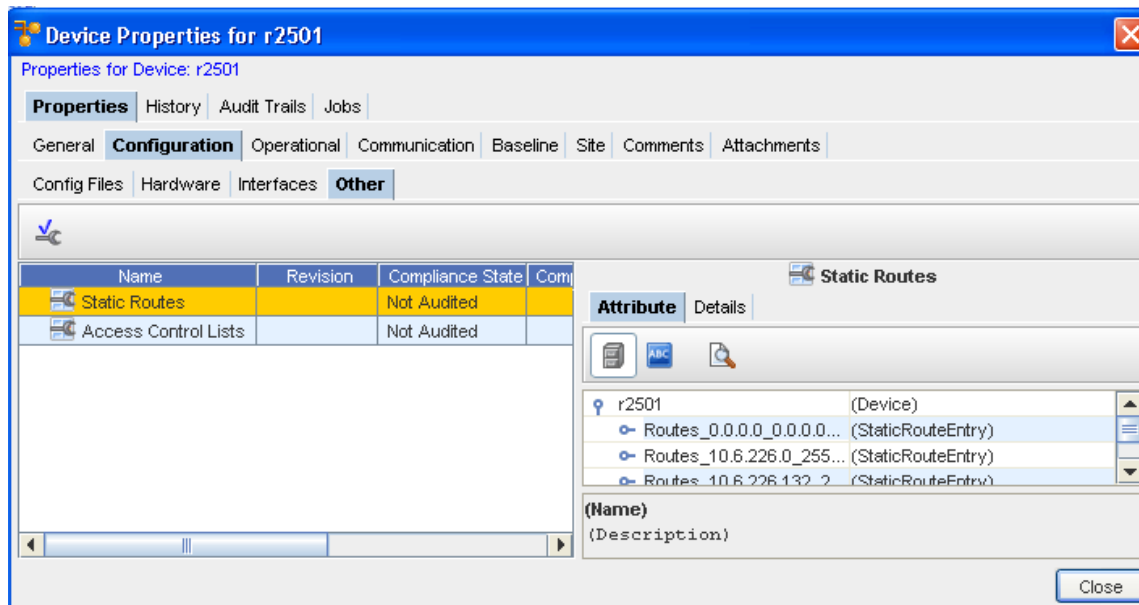
- 3 At the confirmation message, click **Yes**.
- 4 Click **Close** to close this window.

**Note** When you change the IP Address, a Config Pull and a Spec Pull are automatically scheduled, and a notification is sent to you if a Warning or Failed state occurs.

## Other

### Other Overview

This section is designated to store additional information that may not have a specific category. For example, information included here does not fit categorically into the Hardware or Interfaces informational classes.



In this instance, the "other" information consists of Statics Routes.

## Operational Units



## Operational Units Tab Overview

This displays a generic table listing of all configuration units that are not marked as "revisionable", and mostly contains the attributed units.

Typically, these operational units are not expected to be used for **rollback**. Note that there are configuration units that are revisionable, but yet not available for rollback. For instance, Hardware and Diagnostic Results.

Viewing this tab allows you to view additional information on the table, by clicking the **Attribute** and **Details** tabs.

The screenshot shows the 'Device Properties for r2501' window. The 'Operational' tab is selected, displaying a table of configuration units. The table has columns for Name, Revision, Compliance State, Compliance Severity, Created By, and Created On. Two rows are visible: 'ARP Table' and 'ACL Match Counts', both with a 'Not Audited' compliance state. The 'ARP Table' row is highlighted in yellow. To the right of the table is a sidebar with a tree view showing the device 'r2501' and its configuration items, including '10.6.23...' (ArpEntry) entries. Below the tree view are fields for '(Name)' and '(Description)', and a 'Close' button at the bottom right.

Name	Revision	Compliance State	Compliance Severity	Created By	Created On
ARP Table		Not Audited		unknown	02/02/2012
ACL Match Counts		Not Audited		unknown	02/02/2012

The only task that can be completed from this tab is an **Audit** on the Config. See [Running a Compliance Audit](#) for more information and procedures to complete this task.

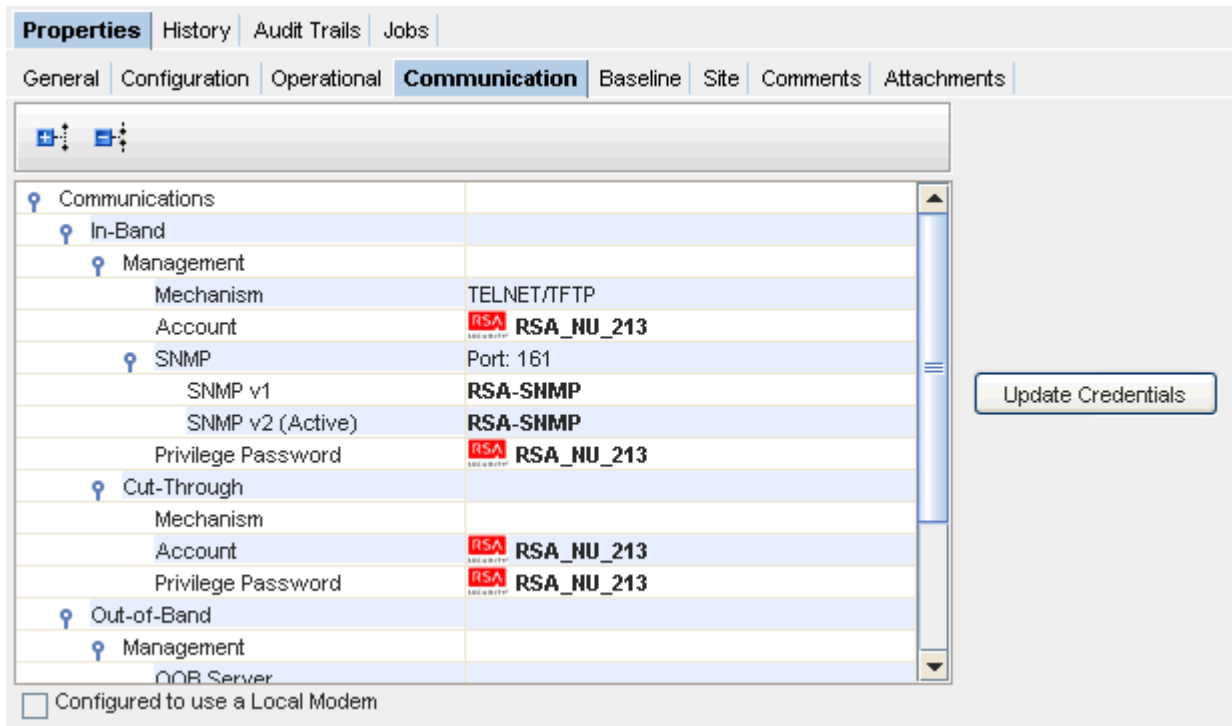
## The Communications Tab

### Communication Tab Overview

This tab can be displayed by selecting the **Properties** in the menu bar when you are in a Devices View or in a Workspace.

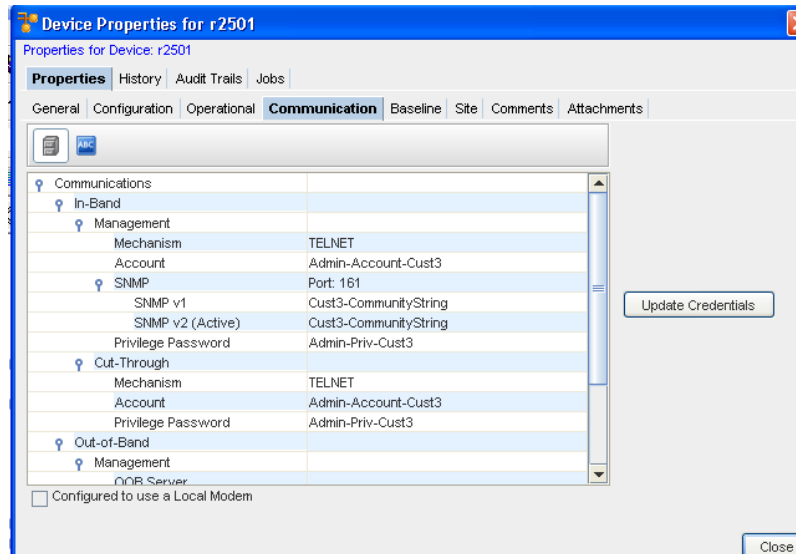
From this tab you can view your In-Band and Out-of-Band Communications, Management, Account, SNMP and Cut-Throughs. You can also **Update Credentials**.

The Communication tab allows you to manage the mechanisms for SNMP, Telnet, Telnet.TFTP, and both In-band and Out-of-Band communications with the device.



**Note** The **Configured to use a Local Modem** check box is only available if you have previously enabled a local modem.

## Editing In-Band Communications



To Edit In-Band,

- 1 Click the **Update Credentials** bar to get to the Update Credentials window.
- 2 Select the **In-Band** tab.

- In the **Management** section, you can select from the options in the following drop-down lists:
  - Mechanism
  - Account Credential
  - Privilege Password
- In the **SNMP Credentials** section, you can select from the options for SNMP Credentials:
  - SNMP Port - or no change
  - SNMP v1, v2, or v3, and select these to be Active
- In the **Cut-Through** section, you can select from the options in the following drop-down lists:
  - Mechanism
  - Account Credential (this can either be **User Prompted** or **User Account**).
  - Privilege Password
- When you have made selections for both Management and Cut-Through, you can then click **Schedule** to push your changes to the devices, or click **Save Only** to update the database associations only.

---

**Note** You can click **Cancel** to leave this window and cancel any selections.

---

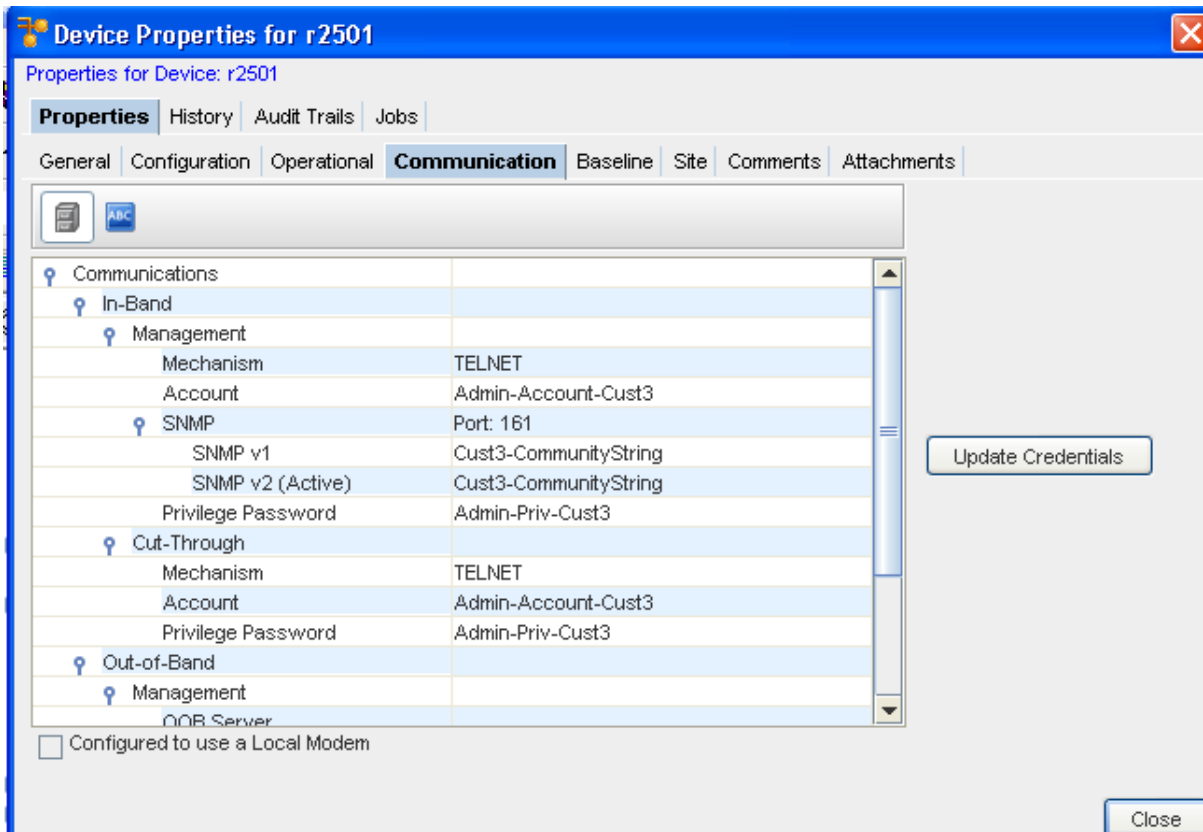
**See:** [Edit Out-of-Band](#)

## Managing Device Communications

Setting credentials at the device level allows you to override the network and system credentials to which other devices in your network respond.

To set credentials at the device level,

- 1 With a workspace displayed, select a **device**, then right-click to go to **Properties**.
- 2 With the Properties window displayed, select the **Communications** tab.



- 3 Select the **Update Credentials** button, then click the **In-Band** tab.

Update Credentials

Click "Schedule" to push your changes to the device(s).  
Click "Save Only" to only update the database associations.

**In-Band** Out-of-Band

**In-Band Communications**

**Management**

Mechanism: No Change

Account Credential: No Change

Privilege Password: No Change

**SNMP Credentials**

SNMP Port:   No Change

SNMP v1: No Change  Active

SNMP v2: No Change  Active

SNMP v3: No Change  Active

**Cut-Through**

Mechanism: No Change

Account Credential: No Change

Privilege Password: No Change

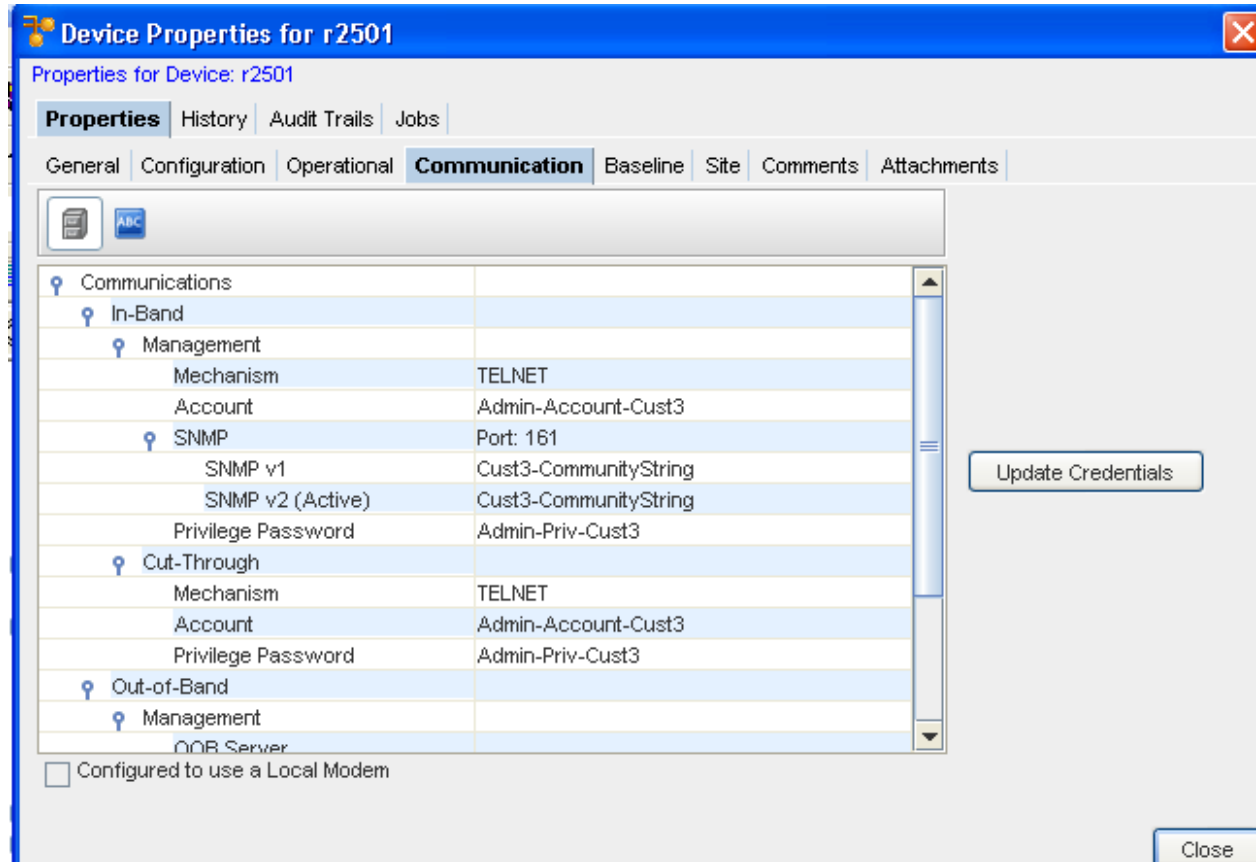
Schedule Save Only Cancel

- 4 Make your needed changes within each section of this window, then click **Ok**.

## Managing and Viewing Privilege Password Levels

Privilege Password levels associated with Devices determines the level of access and activity a user can have pertaining to any one device. Users are limited to the device tasks they can complete, based on their Privilege level.

- 1 From a table view of the Devices, click **Properties**, and go to the **Communications** tab.
- 2 In the information section, you can view all Privilege Passwords associated with this device.
- 3 You can use the **Expand** and **Collapse** icons to display information. You can also select [Updating Credentials](#) to make changes to the current credentials.



**Note** Multi-level can have **more than one** Privilege Password per device. Single-Level can have **only one** Privilege Password per device.

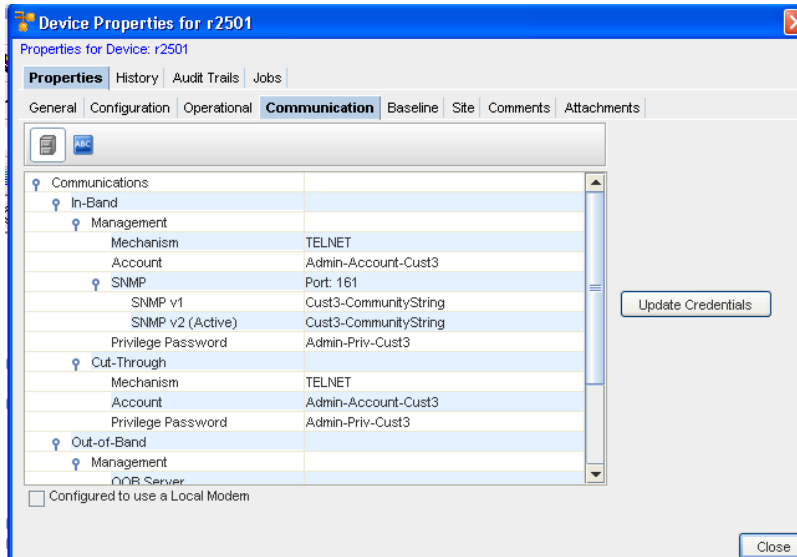
## Updating Credentials

**Important** You will only be allowed to Update Credentials using the **Update Credentials** bar on this **Communication** tab if you have previously been granted the appropriate permissions from your System Administrator. If the Update Credentials bar is grayed out, you do not have the appropriate permission.

**Note** You can also use the **Override button** on the **Schedule Manager** menu bar to get to the Update Credentials windows.

Updating Credentials on Multi-Levels includes the following process.

- 1 From the devices view, select the **devices** that support levels.
- 2 Select **Communications** from the Device Properties tab.
- 3 Select **Update Credentials**.



At the In-Band tab,

- 1 At the Update Credential window, you can select either In-Band or Out-of-Band tabs.

---

**Note** You have the option of selecting to **Schedule** to push your changes to the devices.

---

Click "Schedule" to push your changes to the device(s).  
Click "Save Only" to only update the database associations.

**In-Band** | Out-of-Band

**In-Band Communications**

**Management**

Mechanism: No Change

Account Credential: No Change

Privilege Password: No Change

**SNMP Credentials**

SNMP Port:   No Change

SNMP v1: No Change  Active

SNMP v2: No Change  Active

SNMP v3: No Change  Active

**Cut-Through**

Mechanism: No Change

Account Credential: No Change

Privilege Password: No Change

Schedule Save Only Cancel

2 In-Band tab, make the selections from the drop-down arrows in the **Management** section:

- Mechanism
- Account Credential
- Privilege Password

3 Make the selections from the drop-down arrows in the **SNMP Credentials** section:

- SNMP Port
- SNMP v1, v2, or v3, and select these to be Active

4 Make the selections from the drop-down arrows in the **Cut-Through** section:

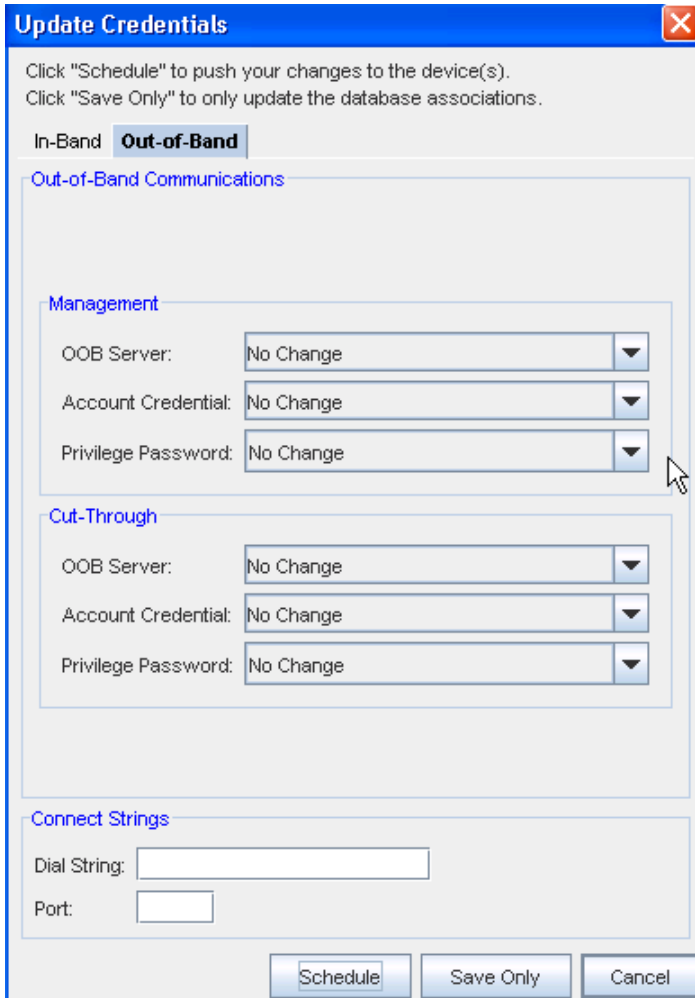
- Mechanism
- Account Credential (this can either be **User Prompted** or **User Account**).
- Privilege Password

5 Select to Schedule, Save Only, or Cancel the information you have selected from this window.



At the Out-of-Band tab,

- 1 At the Update Credential window, you can select either In-Band or **Out-of-Band** tabs.



- 2 At the Out-of-Band tab, make the selections from the drop-down arrows in the Management section:
  - Out-of-Band (OOB) Server
  - Account Credentials
  - Privilege Password
- 3 From the **Cut-Through** section, make your selections from the:
  - Out-of-Band Server
  - Account Credential
  - Privilege Password
- 4 At the **Connect String** section:
  - Enter a Dial string

- Enter a Port Number
- 5 When you have made selections for the Management, and Cut-Through sections, and entered the needed information in the Connect String section, you can then click **Schedule** to push your changes to the devices, or click **Save Only** to update the database associations only.

**Note** You have the option of selecting to **Schedule** to push your changes to the devices.

## The Baseline Tab

### Baseline Tab Overview

When a Network is baselined, the current revision for all devices in that Network are tagged. A baseline allows you to create a production state for all device in the Network, providing a quick mechanism to rollback any device configuration to its defined production revision.

Baselines are created in Network properties. A Network rollback to any baseline can be executed from Network properties.

**Important** A Baseline must have already been set for the Network.

The Baseline tab allows you to review the **network baseline config** that affects the device.

This tab can be displayed by selecting the **Properties** in the menu bar when you are in the Device's View.

The screenshot shows the 'Properties for Device: HP4000' window with the 'Baseline' tab selected. The main area contains a table with the following data:

DCS #	Revision	Compliance State	Compliance Severity	Created By	Created Date
No B...		Not Audited			
<b>Current</b>	1	Not Audited		unknown	03/23/2009 11:3

On the right side, the 'Details' panel shows the following information:

- General**
  - Revision: 1
  - Job Num...: 0
  - Task Num...: 0
  - Complete: False
- Compliance**
  - Complian...: Not Audited
  - Complian...:
- Creator**
  - Created By: unknown

At the bottom, the 'Comments' section contains the text: 'Configuration units not pulled but required for completeness: [running, ]'.

- From this tab you can add **comments**
- **Roll back to the** previous device settings

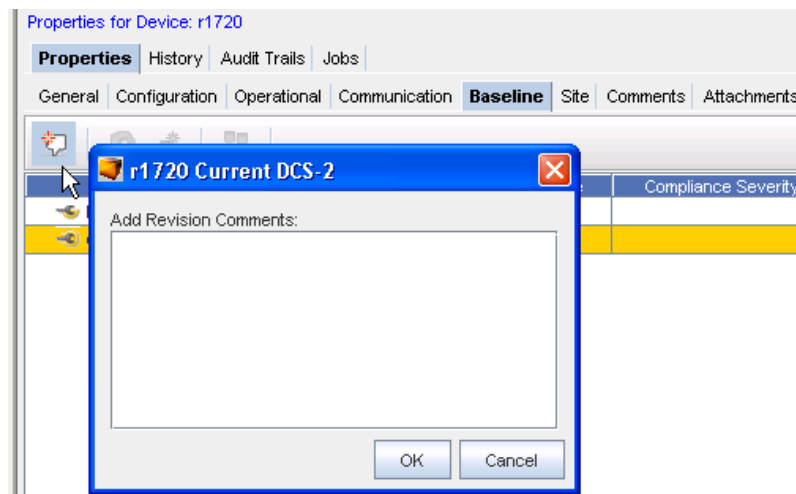
- **Set the current revision** as the baseline
- **Compare** revisions
- View the compliance state

## Adding Baseline Revision Comments

While in the Baseline tab, you can add additional comments to the current baseline.

- 1 Select from the **Device Configuration State Number** from the listing ( **DCS#**), then click the **Add Revision** icon.
- 2 At the Add Revision Comments: section, enter any comments you may have on this current state.
- 3 Click **Ok** when you are completed.

Your comments are now at the top of the Comments listing.




## Rolling back to Baseline

**Important** A Baseline must have already been set for the Network.

From the **Baseline** tab in the Device Properties, you can access the **Roll Back** icon. This allows you to rollback to the previous device settings.

To Roll back to the Baseline,

From this window, you can roll back to the baseline - back to the beginning.

- 1 Click the **Roll Back** icon  to display the Schedule Push Job window.
- 2 From here, you can make any need revisions to the **Job Details**, **Schedule Job Details** , and revisions to **Tasks** and **Notification** if needed. For more information, go to [Using the Scheduler](#).

- 3 After making your revisions, or adding additional information, click **Submit**. This starts your job in the process, with your revisions.

---

**Note** Each device packaged in Network Configuration Manager defines its own Roll back procedure. For example, for Cisco Devices, this is to push the content to the Start Config. Doing this will not affect the running config of the device. Also, the device must be rebooted for it to take affect.


---

## Setting the Current Revision to Baseline


---

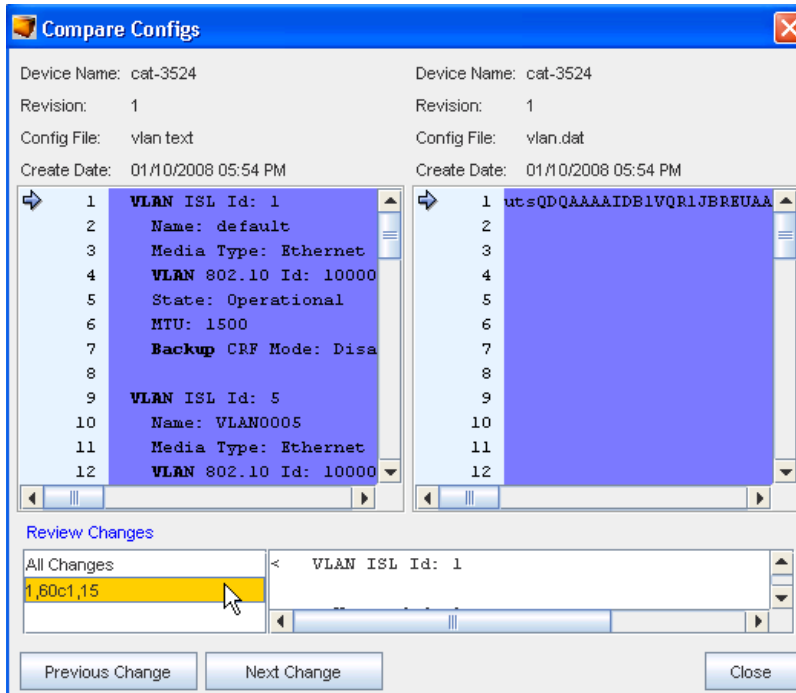
**Important** A Baseline must have already been set for the Network.

---

- 1 From the Baseline tab in the Device Properties, you can access the **Set Current Revision to Baseline** icon to set the baseline to the current configuration version.
- 2 After selecting a Device from the Devices View, then selecting the **Properties** icon, you can then access the **Baseline** tab.
- 3 If there is more than one revision shown (in the **Revision** column) you can promote the latest revision. For example, if you have two revisions shown; a number 1 and a number 2, then you can surmise that changes to the baseline have been made, and you need to promote the latest baseline revision (2).
- 4 Select the latest revision.
- 5 Click the Set Current Revision to Baseline icon  to set the current configuration version. This will then be the current baseline configuration for the Device.

## Comparing Device Revision Configs

- 1 From the **Baseline** tab, select two revisions , then click the **Compare Device Revisions** icon . At the Compare Configs window, you can compare the difference in configurations.



- 2 You can also select to view **Previous** and **Next** changes, or click within the **Review Changes** window.
- 3 Click **Close** when you have completed your review of this information.

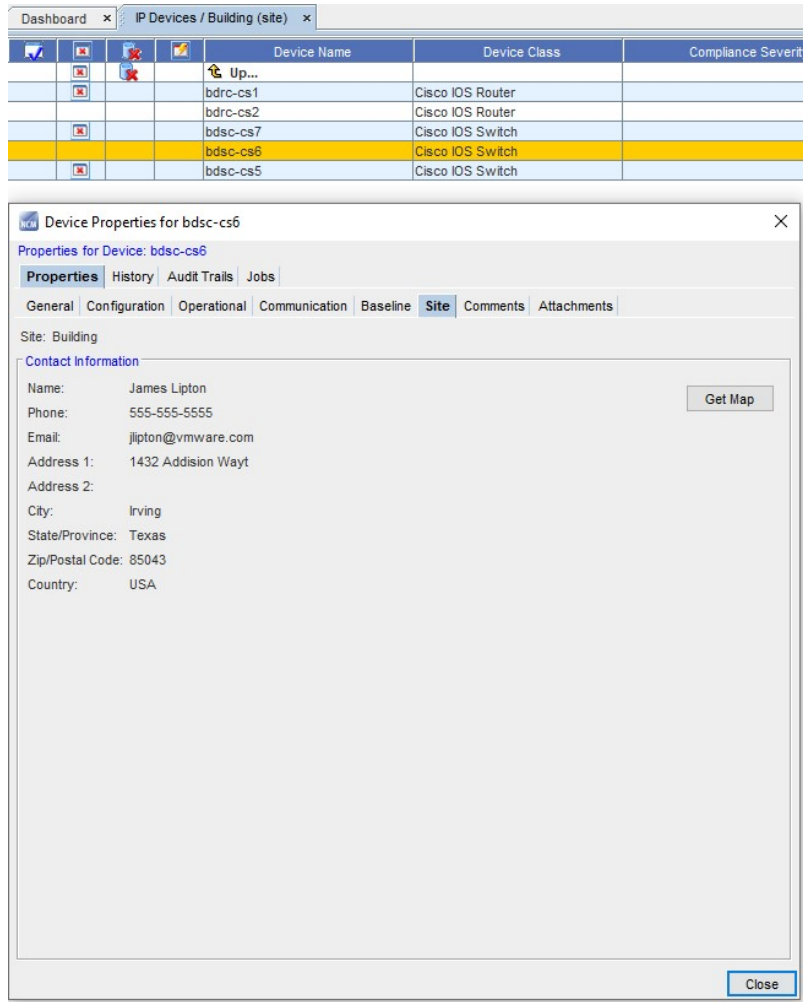
## The Site Tab

### Site Tab Overview

When a device is placed in a hierarchical Site structure, location and contact information can be entered that will be inherited by any devices within that Site. When address information is available for the device, clicking the Get Map option will display a **MapQuest map** of the Site.

This window can be displayed by selecting the **Properties** icon in the Devices View tool bar.

- The site information displays when the **Site** tab is selected.
- The **Site** tab allows you to review the Site information, if a device has already been assigned to a site.



**Note** When the contact information is displayed, you can click **Get Map** to go to the "map finding" feature for directions to that specific Site. For example, you may be directed to the MapQuest link.

See [Adding Site Information](#) for more details.


## Adding Site Information

To add Site information,

- 1 Select **Site**, then right-click to select **Add Site** from the Navigation pane.

**New Site**

\*Name:

\*Type:  

Description:

Override

Contact Name:

Contact Phone:

Contact Email:

Address 1:

Address 2:

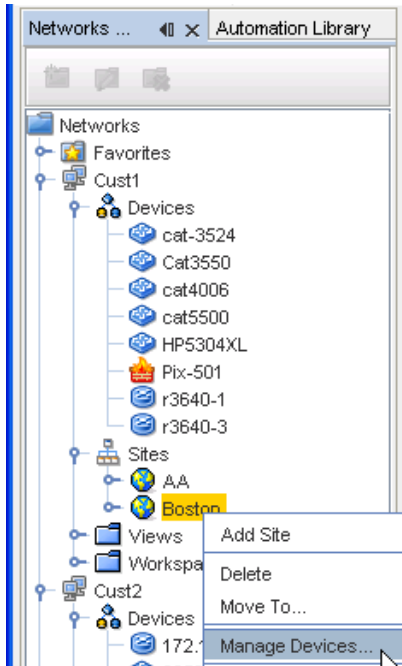
City:

State/Province:

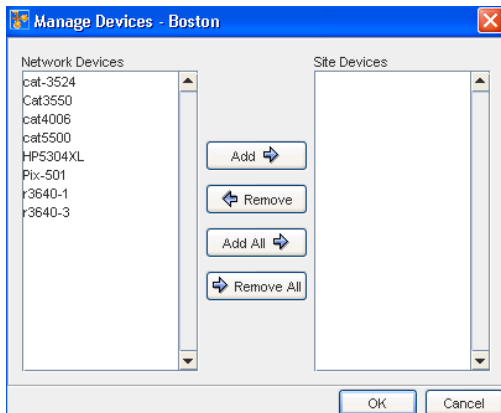
Zip/Postal Code:

Country:

- 2 At the New Site window, enter the information needed.
- 3 Click **Ok** when you have entered all the information you want visible in the Site tab of the Devices Properties.
- 4 Now, from the Navigation pane, select the site you just created, then right-click to select **Manage Devices**.



- From the Manage Devices window, select the devices you want to add to the Site. Use the **Add** or **Add All** arrows.



- Click **Ok** when you have completed moving devices into the Site Devices pane.

## The Comments Tab

### Comments Tab Overview

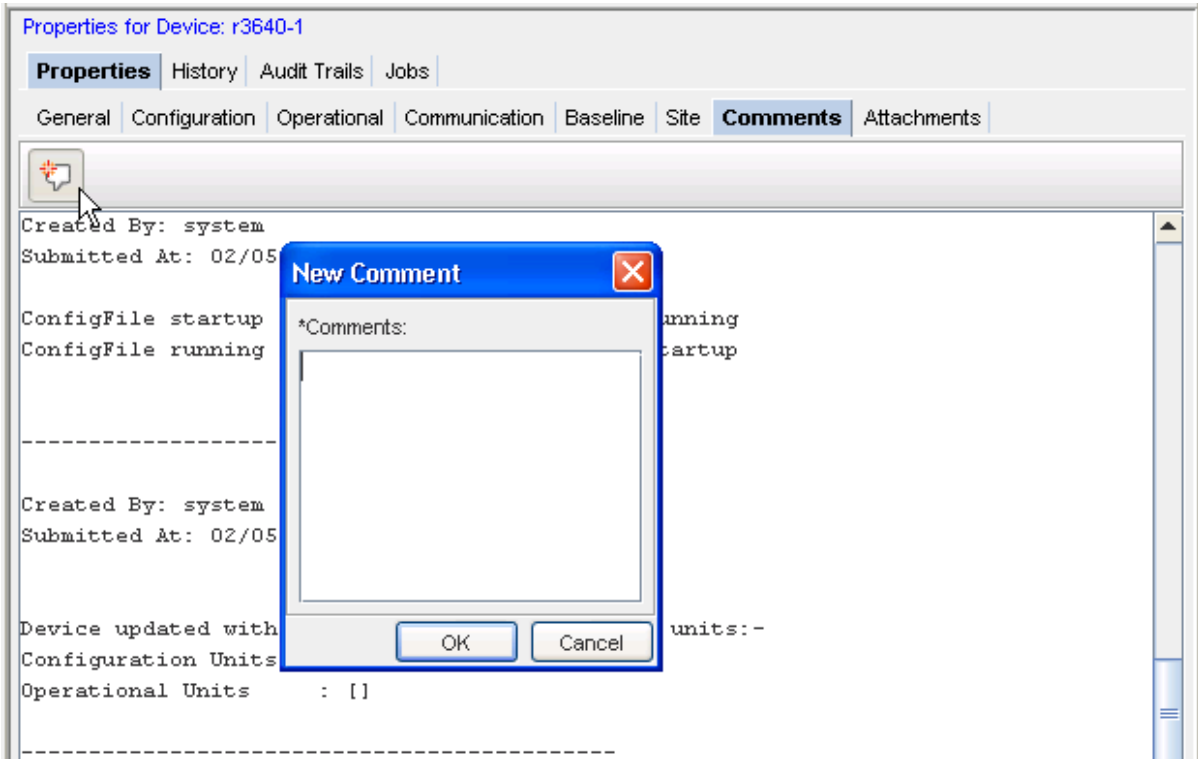
The Comments tab allows you to enter device-specific comments. This tab can be displayed by selecting the **Properties** icon in the menu bar. From this tab you can add new comments.

To add a new comment,

- With the Device Properties displayed, select a **device** from the Devices View.
- In the Comments tab, click the **New** icon. The New Comments window opens.



- 3 Enter your comments, then click **Ok** to add this new comment. Each comment is recorded in this section by the date the comment was entered.

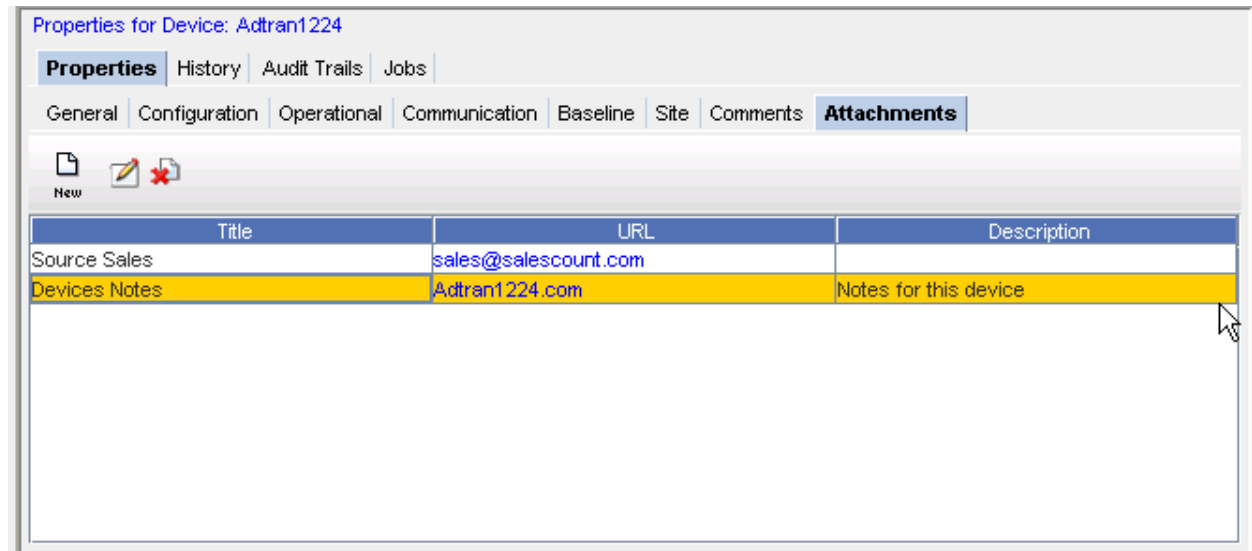


- 4 Click **Cancel** to close this window without saving your comments.

## The Attachments Tab

### Attachments Tab Overview

The Attachments tab allows you to associate an external file to the network.



This tab can be displayed by selecting the **Properties** icon in the menu bar when you are in a Workspace or Devices view.

From this tab you can:

- [Adding an Attachment](#)
- [Editing an Attachment](#)
- [The Dashboard](#)

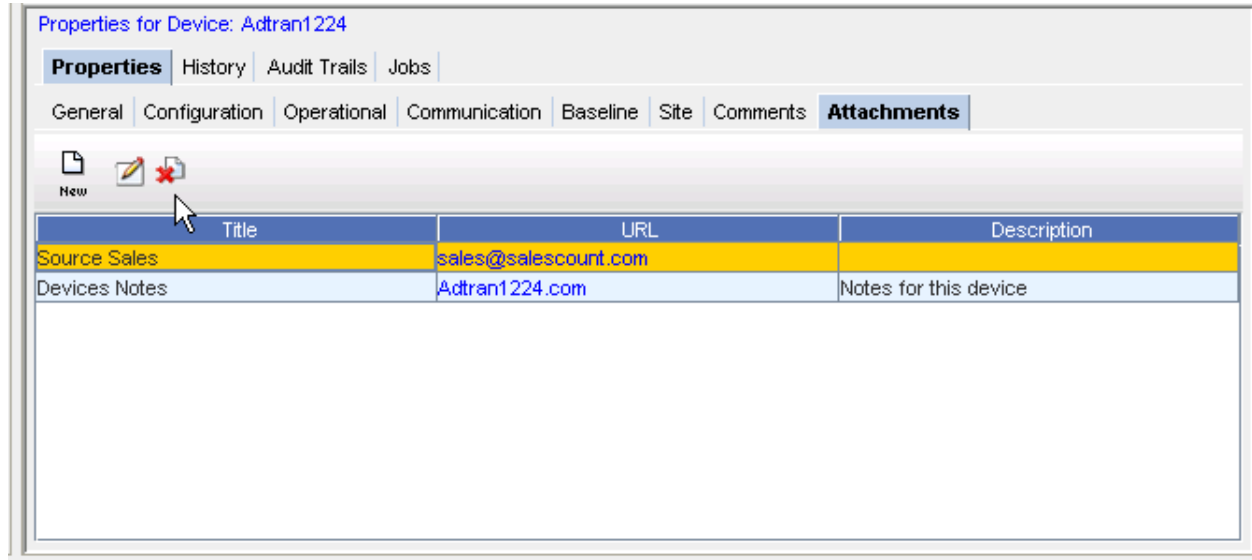
## Editing an Attachment

To edit an existing attachment,

- 1 First, select an **attachment** from the listing of attachments.
- 2 On the Attachments tab, click the **Edit** icon. The Edit Attachments dialog window opens. The Title, URL and Description fields can all be edited.
- 3 Make any changes as needed.
- 4 Click **OK**. The Edit Attachments window closes.

The attachment row updates with the edited details.

## Deleting an Attachment



To delete an attachment,

When deleting an attachment, the actual document that you are referring to is not deleted. You are removing its **linked reference** from Network Configuration Manager.

- 1 First, select an **attachment** from the listing of attachments.
- 2 On the Attachments tab, click the **Delete** icon. The Confirm dialog window opens asking, "Are you sure?".
- 3 To delete, click **Yes**.
- 4 Click **OK**. The Confirm window closes.

The Attachment tab refreshes.

## Working with Sites

## Sites Overview

- Each network in Network Configuration Manager contains a single-site hierarchy construction, which is created at the same time as the network. However, there is no requirement to create and manage sites within each network. For example, there may be times that the construct of a geographical relationship for network devices is not beneficial to the management of the network.
- By default, devices are not assigned to a site, but they do display at the top of the site hierarchy, ready to be managed into a site structure (if needed).
- A Site is a physical view of network devices that can be segmented into a hierarchical structure representing the location of a device. There exists an explicit order to site relationships, determined by the site type. All networks contain the ability to create a site hierarchy for network devices. By default, all devices are available in the Devices tree branch.
- Site types allow you to segment devices based on geography, building, floor, room, and rack. Each site type can contain its own site. For example, a geography can contain a geography, and a room can contain a room.
- A site hierarchy contains the following site types. The site types are listed in the order of how they must be configured when creating a site hierarchy. It is not required to have each site type, but you must construct the site types accordingly.
- Navigating down a network site hierarchy is accomplished by selecting a site and opening it, and then repeating the process to open any other sites further down the hierarchy. Navigating up a site hierarchy is possible by selecting an Up Site icon on any site diagram that has a parent site.



**Geography** - for example, Country, State, City, Province. A geography can contain another geography, building, floor, room and/or rack



**Building** - for example, Headquarters, Street Location, or Complex Number. A building can contain a floor, room and/or rack



**Floor** - within the building, the floor on which devices reside. A floor can contain a room and/or rack



**Room** - on the floor, the exact room where the devices reside. A room can contain another room and/or rack

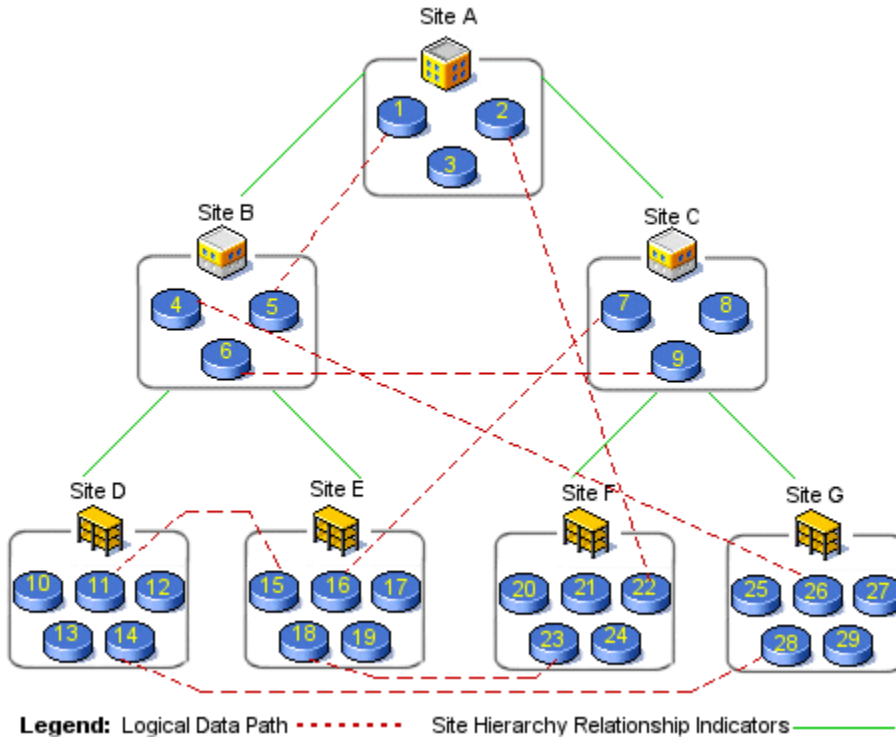


**Rack** - in the room, the rack on which the servers are located. A rack can contain another rack

A site hierarchy has no depth limitations or restrictions. For example, your corporate office may need to consist of a large network site hierarchy, including a geography containing multiple buildings, each containing multiple floors, each containing multiple rooms, and each in turn, containing multiple racks.

In this scenario you might locate all your devices at corporate within the rack site containers. However, within the same network it would be acceptable to have a single building container holding a few devices located at each small regional sales office.

Sites have parent/child hierarchy relationships. A physical representation of a site shows the relationships within the site hierarchy. A logical connection indicates the connection between devices and sites, regardless of the hierarchical layout.



The previous diagram shows a sample visualization for a possible network site hierarchy. In this hierarchy, there exists a root building site **A**.

- Site A contains two lower-order floor sites, **B** and **C**, and three devices.
- Site B also contains two sites, in this case, rack sites **D** and **E**, and three devices.
- Each rack site contains five devices.
- Assuming that all attribute information for each site is the same, and is not overridden at any site, attributes can be entered at site **A**, and then inherited at all other sites.

All site hierarchy is user-defined, and managed. It can not be shared between networks. Permissions to modify a site depend on the membership filters. See [Permissions and Site Security](#) for more information. Sites can not be seen in other views, as each view is unique. Sites can be viewed by other users who have access to the networks.

As each site hierarchy is created for each network, devices are added to sub-sites. All devices associated with the network resides within a site. **A device can reside in one site only.**

When devices are used that actually reside in another network, these devices have an "off-site" connector symbol to the outside network. This connection uses the off-site connector to indicate that the devices are not managed by the open network. You are not allowed to move a device that is not managed by the primary network, because the device can only be placed into the site hierarchy of its primary network.

The following are characteristics of sites:

- Each network has a single-site hierarchy.
- A site contains both sub-sites and devices.
- Sites can not be shared with other networks.
- Sites are recursive, and have no depth limit.
- Sites are user-managed, and are a physical representation of a network.
- Only users with adequate permissions can create and name sites.
- All information entered into a higher level site is propagated to the lower tier sites, such as, contact and address information. When inherited by sub-sites, this information can be overwritten.

Once you have created a site hierarchy for your network, you can define the layout when viewing the layout:

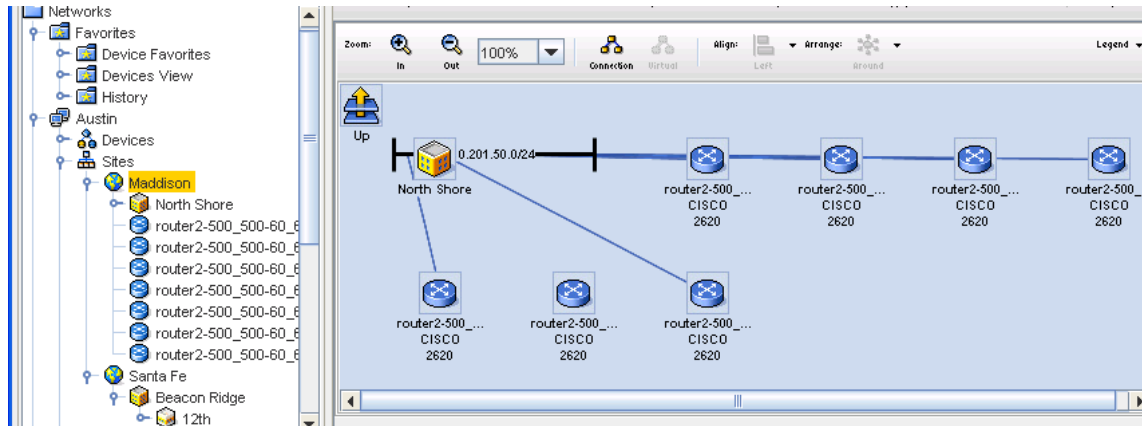
**Table** Shows the devices in a sorted table layout

**Diagram** This is the default view, and shows the devices using icon representation.

This is an example of the **Table** view.

Device Name	IP	Devic...	Model	OS Versi...	Devi...
<b>North Shore</b>					
router2-500_500-60_60-...	10.2...	Cisco ...	2620	12.1(8) E...	
router2-500_500-60_60-...	10.2...	Cisco ...	2620	12.1(8) E...	
router2-500_500-60_60-...	10.2...	Cisco ...	2620	12.1(8) E...	
router2-500_500-60_60-...	10.2...	Cisco ...	2620	12.1(8) E...	
router2-500_500-60_60-4	10.2...	Cisco ...	2620	12.1(8) E...	
router2-500_500-60_60-...	10.2...	Cisco ...	2620	12.1(8) E...	
router2-500_500-60_60-...	10.2...	Cisco ...	2620	12.1(8) E...	
Up...					

This is an example of the **Diagram** view.



- Sites Hierarchy and Logical Connections
- Sites Best Practices
- Permissions and Site Security
- Sites Filters
- Creating the Site Hierarchy
- Attributes
- Editing the Site Hierarchy
- Removing a Site Hierarchy level
- Right-click Features
- Right-click Features - Diagram View
- Assigning Devices to Sites
- Editing Device Associations to Sites
- The General Tab - Editing Site Properties
- The Sites Comments Tab
- The Attachments Tab
- Using Quick Commands
- Sites - Legends

## How Sites and Views Work

Network Configuration Manager offers a flexible and dynamic way to efficiently segment the management of devices in your network, through the use of Sites and Views. Sites and Views allows you to implement and manage device containers within your network that best reflects your management needs.

Sites	Allows you to segment device management physically, by a geographical location
Views	Allows you to segment your devices by technology type, vendor, departmental responsibility, or any other preferred logical segmentation

In this way, each user with the proper Network Configuration Manager network credentials can customize the way they organize and access devices in the network.

## Sites

Regardless of the number of networks you construct in your Network Configuration Manager environment, Sites and Views provide you with the ability to physically or logically segment the devices contained within each network. Sites, as the name indicates, reflects a physical, geographic segmentation of devices.

To track the physical location of managed devices for asset tracking, maintenance or repair purposes, or just work better with devices organized in a physical relationship, implement Sites within Network Configuration Manager.

## Views

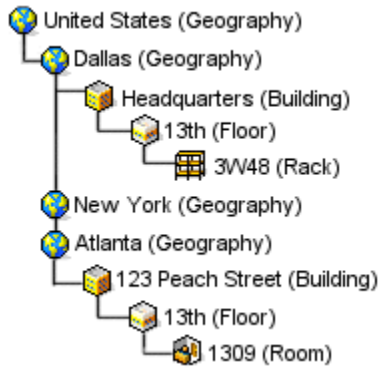
Views provide a logical segmentation of devices, meaning there is no need for a physical relationship to exist between devices within a View.

If you operate across geographical boundaries, and segment network management responsibilities by technology or vendor, you will find that Views will address the need for device organization. However, it's likely that a combination of both Sites and Views will be the **most effective** method for providing the flexibility to manage network environments.

### How Sites and View Work

- Sites are constructed in a hierarchy. As such, sites can contain other sites, as well as devices. There exists an explicit order to site relationships determined by the site type.
- By using the site Hierarchy, you can diagram the physical relationships devices have with one another. Sites provides a "snapshot" allowing you to focus on any part in the network. You can then segment the site to allocate devices into sub-sites. For example, the following is a site hierarchy, and the possible site type relationships.





- This example indicates that your devices are divided into four possible geographical locations: United States (Primary Site), Dallas (sub-site1), New York (sub-site2), and Atlanta (sub-site3).
- Within Dallas, the devices have been further segmented to the exact **rack location**, and in Atlanta, the devices have been segmented to the **room** where the devices are located. In this hierarchy, New York's relationships remain hidden.
- In the example, notice the duplication of the 13th floor being used. When naming sites, you cannot use duplicate names when the types are on the same level in the hierarchy. However, it is permissible to duplicate a name, when in separate site levels .
- Also, note that all site types were not used in either Dallas or Atlanta. In the Dallas site, a room has not been indicated. In Atlanta, a rack is not indicated. This is to emphasize the ability to create the site types that best reflect your locations.
- As each site is diagrammed, note that the physical layout of a site does affect the logical connections of devices.
- Views have no relationship to one another as they contain flat, and sometimes unrelated groupings of devices. As such, views have no relational hierarchy in a network. However, for organizational purposes, views are maintained in a folder structure within a network. In this way, for example, you could create a vendor folder named Cisco™, containing sub-folders for routers models, each of which would contain views holding routers sorted by connection type. For example, Frame, ATM, or Point-to-Point.
- Sites and Views are designed as public, or shared containers under each network. As such, any Network Configuration Manager user with **view access** to a network can access and see the sites and views created in that network. There is one default view created for all networks called the **All Devices** view. It is a view created to provide a single reference to all devices in a network.

---

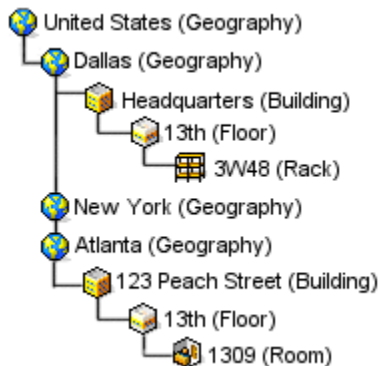
**Important** It is not recommended that you use the All Devices view for device management, especially for large networks, as system performance is proportional to the number of devices in a view. Opening up and operating in the All Devices view could cause slowed performance, and use considerable resources.

---

## Sites Best Practices

Best Practices are recommend methods of completing tasks or tips that should be used, based on a typical scenario.

- The Site hierarchy was constructed to provide your organization with an effective way to track the physical location of devices in your network. While it is acceptable to use the Site hierarchy for day-to-day network management, it is recommended that Views be used for managing devices, especially when a deep site structure is created. This will greatly speed the navigation to the devices you frequently manage.
- When creating networks and adding sites and views, construct the site hierarchy from the bottom up. Start with the **rack location**, and work backward. By creating the site in this manner you only have to move the devices that belong in each site type to their location, rather than moving all of them from the upper-most location downward.
- Hierarchical rules apply to the site hierarchy. For example, site names are unique at each level of the hierarchy. In the hierarchy graphic (shown below) when naming site types, there cannot be two New York locations under United States. There can, however, be duplicate floor names (such as 13th), as they reside under two different sub-site locations.



- When making changes to a site type, all set attribute values are lost and must be reset.

## Sites Hierarchy and Logical Connections

Sites and Views provide the ability to display connections between devices. Connection types are identified by different line styles in your View or Site. Connections can be displayed in two formats:

Physically This displays clouds for certain WAN technologies, giving a layer-2 visualization of your network.

Logically This provides layer-3 visualization.

Because of the hierarchy of sites and the association rules of devices in views, this is where the similarity of connections ends between the two.

## Views

Views are flat in nature, having no relation to other views. Connections in Views are visible only between devices within that view.

Since a required relationship between any device in a view is not needed, you could create a view in which there are no connection associations between any of the devices.

A good example of this would be a view containing all firewall devices in an enterprise. Each firewall could be providing outbound access from the enterprise, and have no actual direct connectivity to each other. In this view, the diagram would display an icon for each device, but there would be no connections.

## Sites

Sites, because of their hierarchical relationship and physical nature, have a complex connection construct. This is due to the three-dimensional effect created by the site hierarchy when in a site diagram.

Before explaining the concept of connections in sites, it is important to remember that ALL connections in Network Configuration Manager are ultimately device-to-device. Also, connector lines in a diagram can represent a single connection, or at times, a group of connections conveniently associated by a connection type.

Imagine a site diagram containing three devices and two other sites. The two sites would be considered children, or sub-sites, of the current site, as they are 'down' the hierarchy chain. In this imagined diagram, it is possible that two of the visible devices could have connections (for example, Ethernet, or Frame Relay) between them, which would create a device-to-device connector.

One of the devices could have a connection to a device contained in one of the sub-sites, which would require a device-to-site connector. It is also possible that a device contained in the first sub-site could be directly connected to a device in the second sub-site.

In the current view, the diagram would construct a site-to-site connector. Consider also that the devices in the sub-sites may not live at the top of that site level, but be nested in other sub-sites down the hierarchy. Regardless, the same connector would be constructed.

Finally, a device in the current diagram or contained in one of the sub-sites, could be directly connected to a device in a site, in a completely different branch of the site hierarchy, or 'up' the hierarchy. In both of these cases, the terminating device or site would not be visible in the current diagram. In this case, a device-to-off-site, or site-to-off-site connector would be constructed.

Within a site diagram, there are five connector relationships:

### Device-to-Site

Are connections between devices contained in the hierarchy.



### Device-to-Device

Shows connections from one device to another device.



**Device-to-Off-site**

Are connections to devices outside of the site hierarchy. These connections are identified by an off-site icon.

**Site-to-Site**

Shows connections from one site to another site.

**Site-to-Off-site**

Are connections to site levels within the site hierarchy. These connections are identified by an Off-site icon.



**Note** It will take implementing a network site hierarchy to see how the connectors are generated and to understand how the diagramming of connections works within sites. Also note, that the calculation of all the permutations of possible connectors is a tedious process.

Since it is assumed that once a site hierarchy is constructed, there will be few physical changes.

The recalculation of connections in a site hierarchy is completed as a nightly batch process, at approximately 4:00 A.M.

This schedule can be changed, depending on the requirements of your network. As changes are made to networks during regular use, a flag is used to indicate that site diagrams are due for an update. When a site diagram is refreshed, it is transparent to the user. Depending on the number of devices, the refresh may be time consuming.

## Editing the Site Hierarchy

Once created, the site hierarchy can be edited as follows:

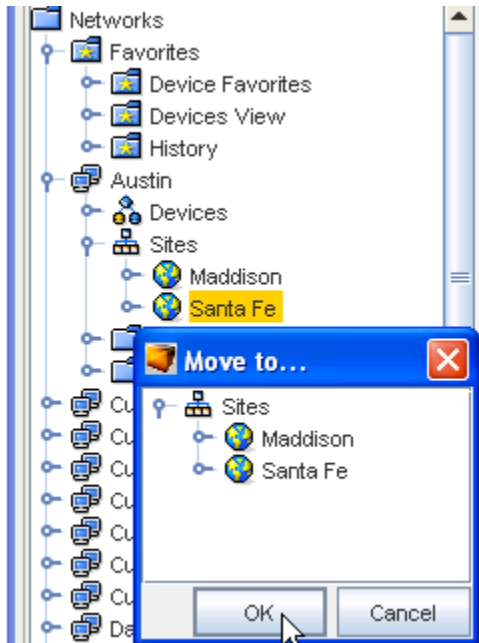
- [Removing a Site Hierarchy level](#)
- Devices can be moved to other site types
- [Sites Hierarchy and Logical Connections](#)
- Site Type properties can be edited

Once a site type has been removed from the site hierarchy, it cannot be retrieved. You must re-enter any information that has been deleted in error.

### Edit Site Hierarchy

To move the site hierarchy,

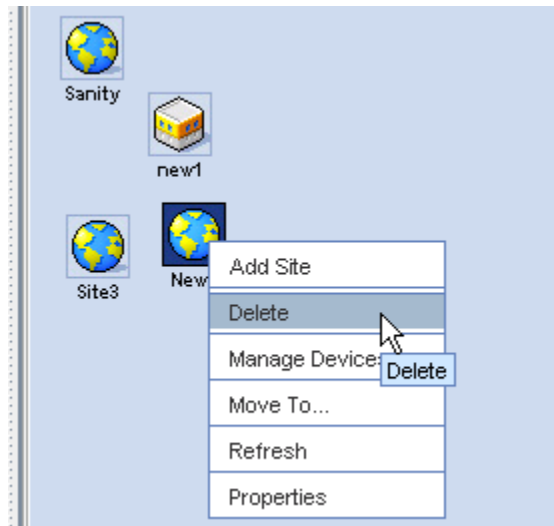
- 1 In the tree menu, expand the **Sites** branch.
- 2 Expand the tree menu, then right-click the appropriate **Site type**.



- 3 From the right-click options, select **Move To....**  
The Move To... window opens.
- 4 Navigate to the site location where the site is being moved.
- 5 Click **OK**. The Move To.... window closes.
- 6 If the window does not automatically refresh, right-click on **Sites**, then select **Refresh**.

## Removing a Site Hierarchy level

- 1 In the tree menu, expand the **Sites** branch.
- 2 Expand the tree menu, then right-click the appropriate **Site type**.
- 3 From the right-click options, select **Delete**.
- 4 The Confirm dialog window asks, "Are you sure?" To delete this single site, click **Yes**. If there are site levels within the site you are deleting, the following Confirm window opens.
- 5 To delete the site levels with the site you are deleting, click **Yes**.
- 6 If the window does not automatically refresh, right-click on **Sites**, then select **Refresh**.



## Permissions and Site Security

Authorizations for the protected device resources in a Site or View are taken from the authorizations granted at the **Network** or **Individual Device** level.

If you have been provided the access or permission (either at the network, or specifically on the device) to update that device and schedule changes for the device to the scheduler, you can complete this task from any Site or View that contains a representation of that device in the network.

To create a Site or View, or to modify its contents, you must be able to [Managing Network Access Permissions](#).

## Sites Filters

To further enhance the information presented within Sites and Views, display filters provide a mechanism for tailoring your display of the network. You can customize the display filters to limit the device types visible in a **Site** or **View** window. In the same way, connection technologies can be filtered between visible devices.

For example, you may have a Site that contains all the devices (72) in the 3rd floor communications closet at the Corporate location. Opening this Site visually displays all 72 routers and switches in that closet. However, at this time, you are only concerned with identifying the Frame Relay routers in the closet. A filter could be quickly constructed within the Site window to only display routers and frame relay connections, greatly speeding the identification of the devices you need.

In addition to displaying filters, Views provide the ability to create dynamic membership filters. Filters are identical to display filter types, but provide a way to automatically assign devices to a View, based on their type or technology.

Each time the view is opened the device membership list is updated with all eligible devices. For example, creating a View with a membership filter is an ideal way to always have a view of every firewall device in your network, which is updated anytime a new firewall is discovered in the network.

For details regarding the Sites window, see [Sites Overview](#) .

## Attributes

Each site type has its own attributes, but as an option, you are able to propagate information to sub-sites that can be inherited or overridden from parent sites. These attributes are used to identify the location of a site, and the devices or other sites contained within it.

In this way, devices and sites placed in a building site construct will inherit the physical address of that site. When changes are made to a higher level site, the overwritten details remains intact.

### Site Attributes include:

- Name
- Type
- Description
- Override (where you can override the initial contact names or description)
- Contact Name
- Contact Phone
- Contact Email
- Address 1
- Address 2
- City
- State/Province
- Zip/Postal Code
- Country

Dynamic inheritance in sites allows lower-order sites to have their site attributes updated when the same information is updated in the parent site. This dynamic inheritance can be overridden at any site.

When the override flag is set for a site, local attributes can be customized, and will not receive dynamic updates from the parent attributes. Un-setting the override flag for a site restores the attribute inheritance from the parent site.

## Creating the Site Hierarchy

Contact information can be provided per Site, or inherited from a parent Site. Once the Site has been created, devices can be associated with the site. Devices associated with the network are listed under the **Devices** branch of the menu tree. The Sites branch remains empty until a site hierarchy is created.

---

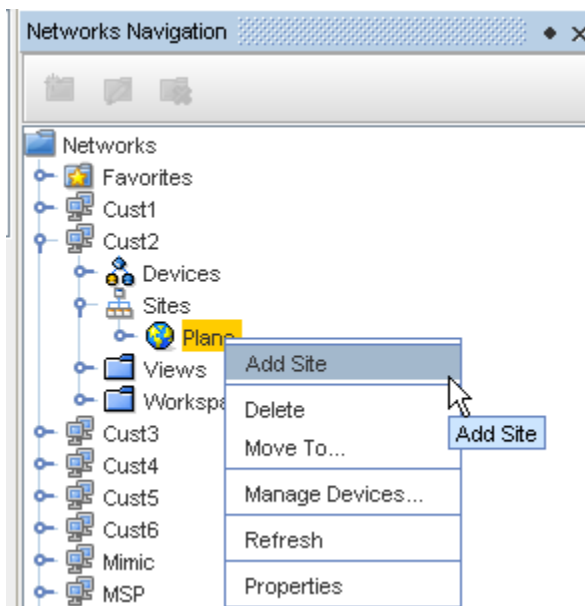
**Important** When creating Sites, you must follow the nesting hierarchy in [Sites Best Practices For more information](#), see [How Sites and Views Work](#).

---

As you are creating the Site hierarchy, devices can be assigned as you go, or the Site hierarchy can be created, and then assigned to the devices within the hierarchy.

To add Site information,

- 1 Select **Site**, then right-click to select **Add Site** from the Navigation pane.



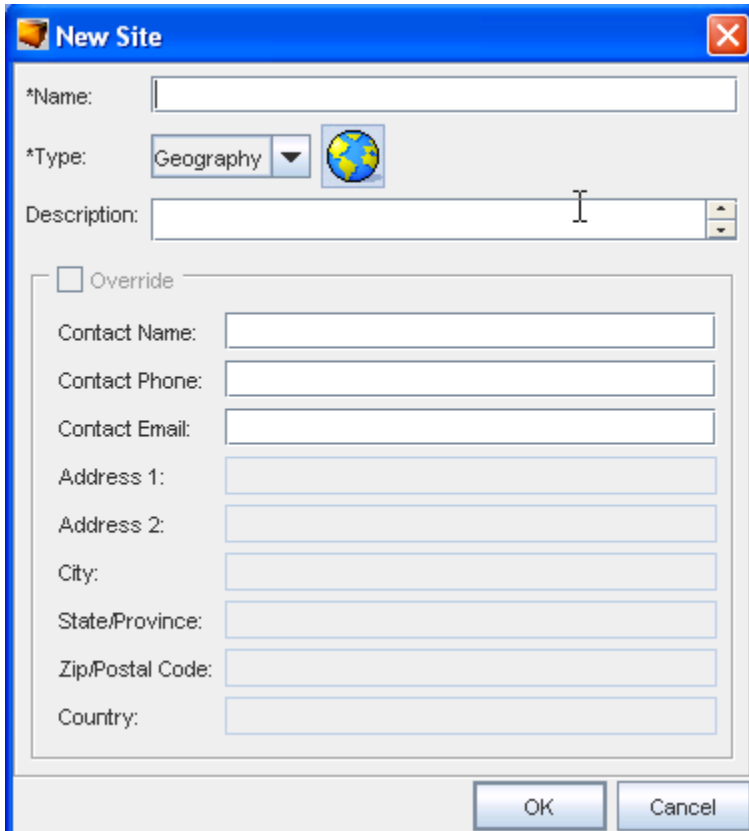
- 2 At the New Site window, enter the information needed.

---

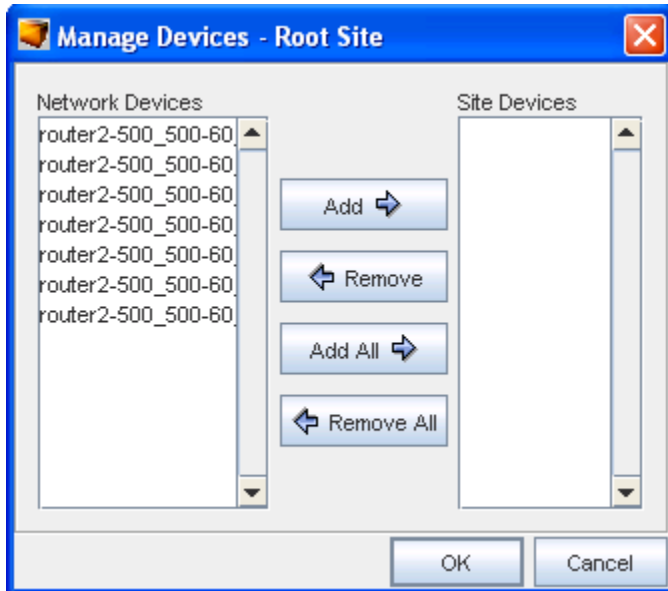
**Note** You can select to Override existing Geography information with this new information if Building, Floor, Room or Rack is selected from the Type drop-down, and Override is checked.

---





- 3 Click **Ok** when you have entered all the information you want visible in the **Site** tab (of the Devices Properties).
- 4 Now, from the Navigation pane, select the site you just created, then right-click to select **Manage Devices** from the Root Site.
- 5 From the Manage Devices - Root Site window, select the devices you want to add to the Site. Use the **Add** or **Add All** arrows.



6 Click **Ok** when you have completed moving devices into the **Site Devices** pane.

When Site types are added to the hierarchy, you need to categorize the networks devices. Once finished, [Assigning Devices to Sites](#) .

## The General Tab - Editing Site Properties

Site properties contain contact and location information for the Site. By default, Sites inherit the properties of the parent Site, unless the Override check box is selected. Devices in Sites inherit Site properties which are displayed in the Site tab of the Device Properties.

Comments and Attachments can be associated with a Site. Site objects also support Data Fields.

The (General) properties of a site are the details entered when the site hierarchy was created. Added to this information are two additional tabs:

- [The Comments Tab](#)
- [Attachments](#)

---

**Important** You must follow the nesting hierarchy [Sites Best Practices](#). For more information, see [How Sites and Views Work](#).

---

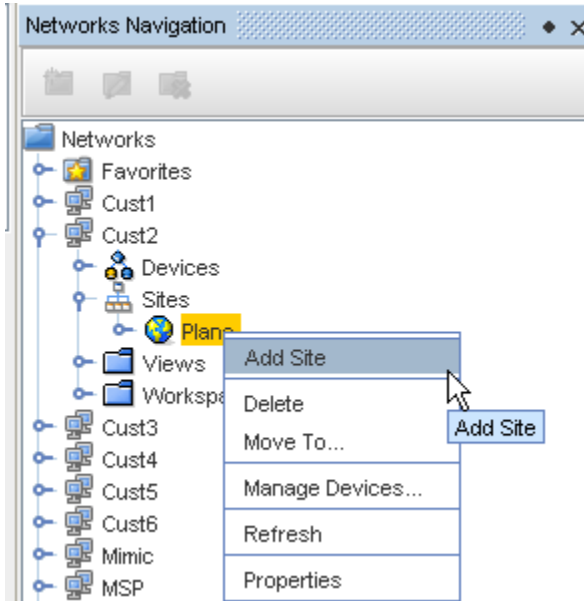
A site type can be edited in two ways:

- [Editing the site type properties](#)
- [Editing Device Associations to Sites](#)

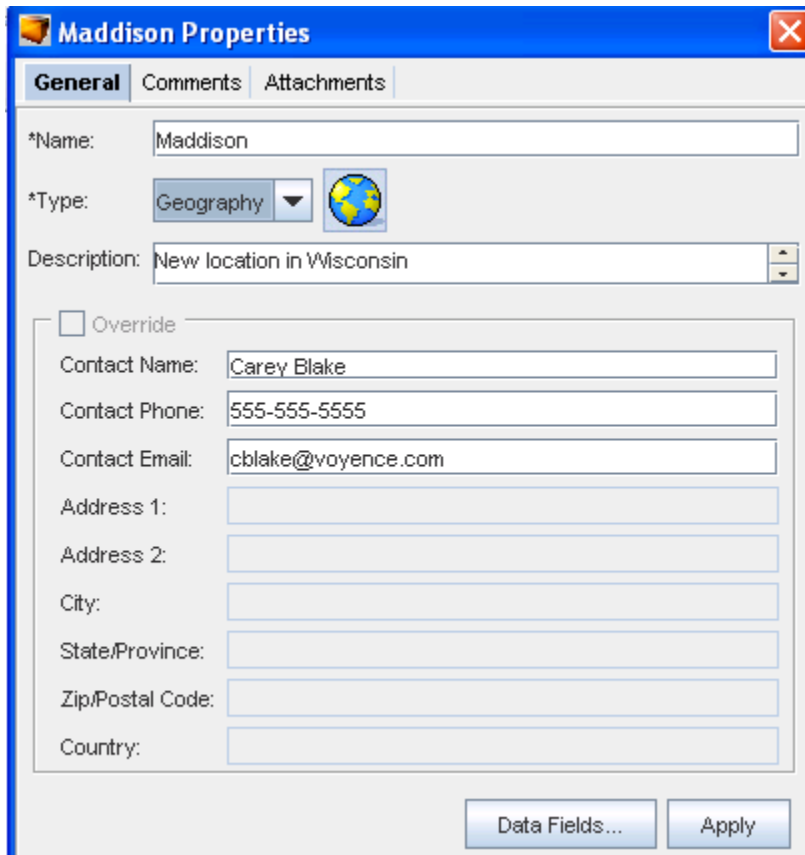
The ability to edit the site type properties allows you to modify the Name, Site Type, Description, and Override information, if needed. This information works hand-in-hand with the ability to edit the devices associated with the site type. Anytime that you edit the site type, you should review the devices associated to the modified site type.

To edit a site types properties,

- 1 In the tree menu, open the **Sites** branch.
- 2 Expand the tree menu, then right-click the appropriate **Site**.



- 3 From the right-click options, select **Properties**. The [Site Name] Properties window opens.



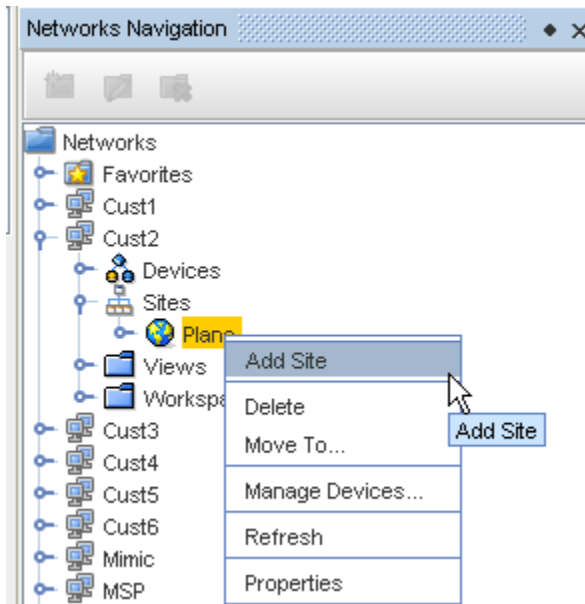
- 4 All fields in the properties window can be edited. **Edit the information** as needed.
- 5 To enter contact information specific to this site (in the **Building, Floor, Room,** and **Rack** types - selected from the Type drop-down) check the **Override** box. The Contact field information window activates allowing you to add additional entries to the previously empty sections.
- 6 When finished, click **Apply**. The [Site Name] Properties window closes.

## Right-click Features

From the Navigation tree you can access other windows to work within sites, and you can complete tasks using the right-click feature.

To use the right-click features in Sites (in the Networks Navigation),

- 1 In the tree menu, right-click **Sites**.



- 2 You can complete the following using the right-click features:
- 3 **Add Site** - this opens the New Site window where you can designate a Site
- 4 **Delete** - this allows you to select a Site, then right-click and select Delete
- 5 **Move to** - this takes you to the Move To window where you can then move the Site within the Network
- 6 **Manage Devices** - this takes you to the Manage Devices window where you can add or remove devices
- 7 **Refresh** - this refreshes your Sites view

- 8 [The General Tab - Editing Site Properties](#) - this takes you to the Properties window where you can enter information pertaining to the Site

## Data Fields in Sites

You can select the appropriate Data Fields within Sites. Data Fields are used to create attributes, and to assign values to devices.

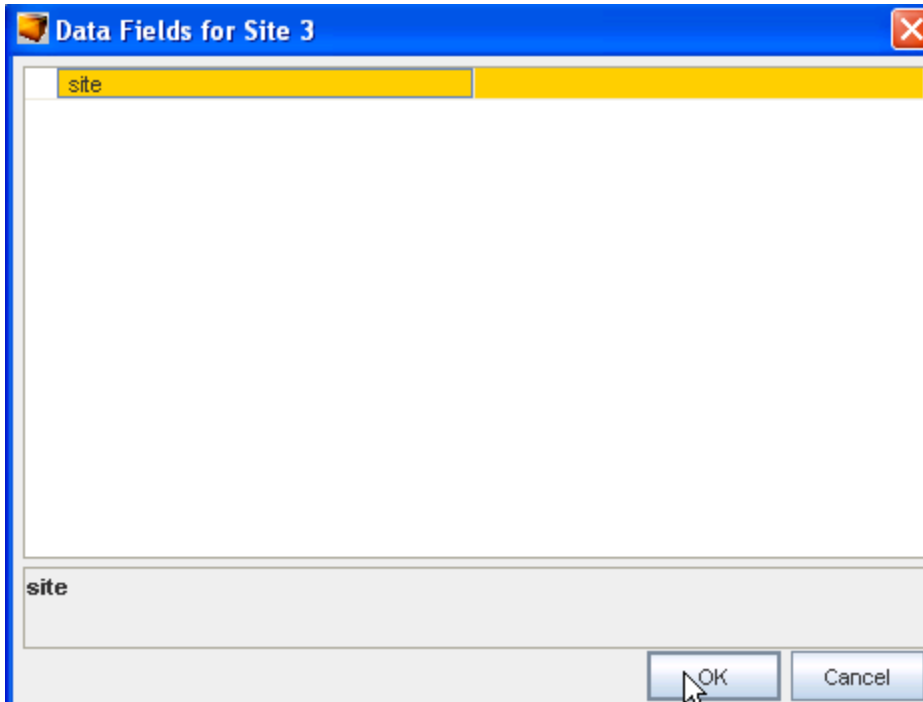
- 1 With the Site Properties window open, click the **Data Fields** selection.

The screenshot shows a window titled "Site 3 Properties" with three tabs: "General", "Comments", and "Attachments". The "General" tab is selected. The form contains the following fields and controls:

- \*Name: Site 3
- \*Type: Geography (with a globe icon)
- Description: New site - associated to New Rack
- Override
- Contact Name: Jamie Dawson
- Contact Phone: 555-555-5555
- Contact Email: jamie@voyence.com
- Address 1: (empty)
- Address 2: (empty)
- City: (empty)
- State/Province: (empty)
- Zip/Postal Code: (empty)
- Country: (empty)

At the bottom of the dialog, there are three buttons: "Data Fields...", "Apply", and "Close".

The available Data Fields will display in the Data Fields for [site name].

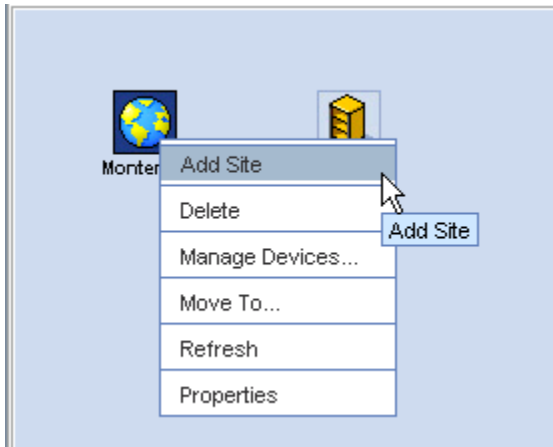


- 2 Select the data field, then click **OK**.

## Right-click Features - Diagram View

To use the right-click features in Sites (in the Sites table or Diagram View),

When you have Sites displayed in the diagram view, you can also use the right-click feature.

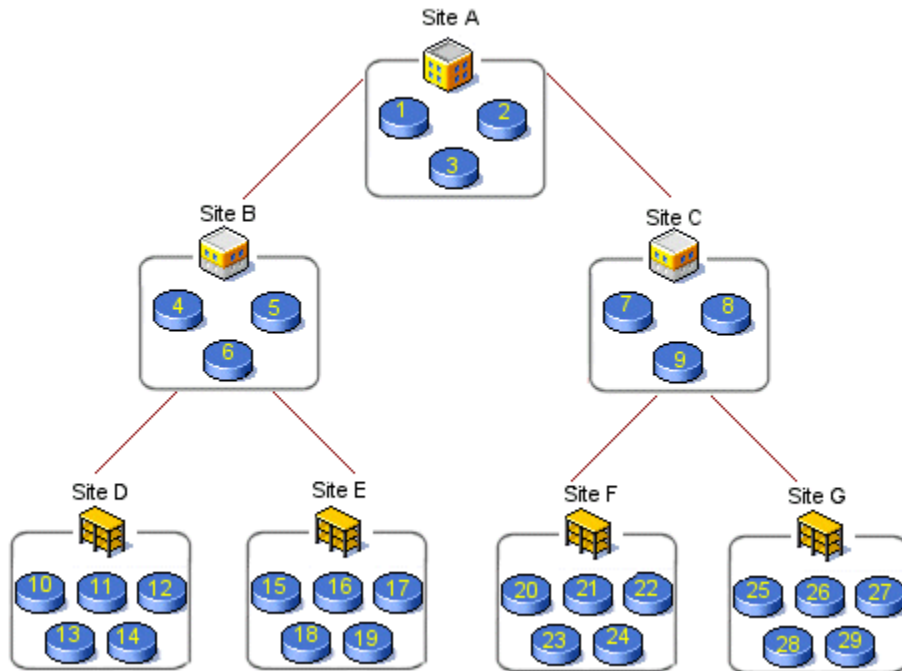


- 1 Right-click the **site** in the table or diagram format.
- 2 Select a **task** from the menu to work with.

## Assigning Devices to Sites

When creating a Site, you can develop a multi-tiered hierarchy that segments the network as deeply as needed. Each Site can contain not only devices, but also other sites .

In the following example, there are seven Sites. Each Site contains not only its own devices, but Sites **B** and **C** serve as both parent and child.



The above graphic indicates:

**Site A** - Site B and Site C and Devices 1,2,3

**Site B** - Site D and Site E and Devices 4,5,6

When creating a site hierarchy, you do not have to consider the devices associated within each Site. From a physical standpoint, Site A has a direct relationship to Site B.

The site hierarchy is a flexible structure. As you are creating the site hierarchy, devices can also be assigned, or the site hierarchy can be created, and then assigned the devices within the hierarchy.

**Note:** When creating a hierarchy for a large network, it is strongly recommended that you build the site hierarchy starting at the bottom-most tier.

To Manage Devices in Site Hierarchy,

- 1 Once the site Type is [Creating the Site Hierarchy](#), right-click on the **type name**.
- 2 In the right-click menu, select **Manage Devices**. The Manage Devices window opens. The list of network devices displays. Devices already associated with the site type are listed in the Site Devices column.
- 3 In the **Network Devices** column, select the devices that will be associated with the site type.

**Note:** A string of devices can be selected by holding down the Shift-key, while selecting the devices. Or, select multiple, non-sequential devices by holding the Ctrl key down, while selecting the devices.

- 4 Click **Add**. The selected devices move to the Site Devices column. Or, to move all devices to the **Site Device** column, click **Add All**.
- 5 To remove devices from the Site Devices column, select the devices to be moved.
- 6 Click **Remove**. The selected devices are moved from the Site Devices column into the Network Devices column. Or, to remove all devices from the Site Devices column, click **Remove All**. The devices that remain in the Site Devices Column are assigned to the site type.
- 7 When you are finished selecting devices to be managed under the current site type, click **OK**. The Managed Devices window closes.

---

**Note** If the tree menu does not immediately refresh to display the devices, right-click on the Site type, and select **Refresh**.

---

## Editing Device Associations to Sites

The location of network devices can change. This could be something as simple as moving a rack of devices to another room, or as complicated as relocating devices from one geographical location to another. Regardless of the level of difficulty, Network Configuration Manager handles the changes with ease.

A Site Type can be edited in two ways by:

- [The General Tab - Editing Site Properties](#)
- Editing the network devices associated with a site type

Assigning devices to a site type in the hierarchy function can be done, but you can also move devices from one site to another site using the drag and drop action.

There are three ways to move devices site-to-site:

- Using the same method used to [Assigning Devices to Sites](#) when it was created
- Dragging and dropping devices into sites
- Moving devices in the tree menu

To drag and drop devices in a site hierarchy,

---

**Note** The drag and drop feature works only in the diagram view.

---

- 1 Open the site type where the devices currently reside.
- 2 Double-click on the site **type**. The Network Configuration Manager [Network Name] > Site Type window opens. All devices and child site types display in the right pane.
- 3 **Click (and hold)** the devices to be moved.



In the table view, a string of devices can be selected by holding down the Shift key while selecting devices. Or, select multiple, non-sequential devices can be selected by holding the Ctrl key while selecting devices. In the diagram view, hold the Shift-key while making selections.

- 4 Drag the selected device to the **child site**. If the tree menu does not immediately refresh to display the devices, right-click on the site type, and select **Refresh**.

To move devices in the tree menu,

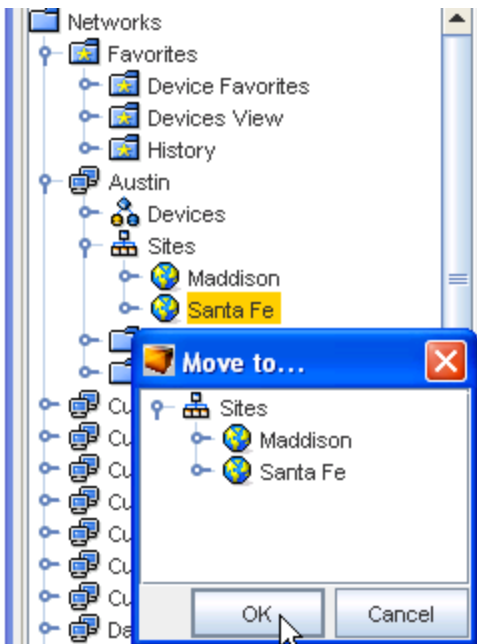
- 1 In the tree menu, select the **devices**.

---

**Note** A string of devices can be selected by holding down the Shift-key, while selecting devices. Or, select multiple, non-sequential devices can be selected by holding down the Ctrl key, while selecting the devices.

---

- 2 After all the devices are selected, right-click on one of the **selected devices** . The Move To... window opens.



- 3 Expand the Sites tree menu until the site where the devices will be moved is displayed.
- 4 Select the **Site**.
- 5 Click **OK**. The window closes. If the tree menu does not immediately refresh to display the devices, right-click on the site type and select **Refresh**.

## Symbolic Device Links in Sites

Due to the physical nature of Sites, devices may exist in only one network and one site. This is logical, considering that a switch or router can physically exist in only one rack, in one room, on one floor, in one building, and in one geography at any time. However, symbolic links for any device can be placed in other sites or networks. This allows connected neighboring devices (that may exist in other networks or sites) to be accessible in the local site, for management convenience.

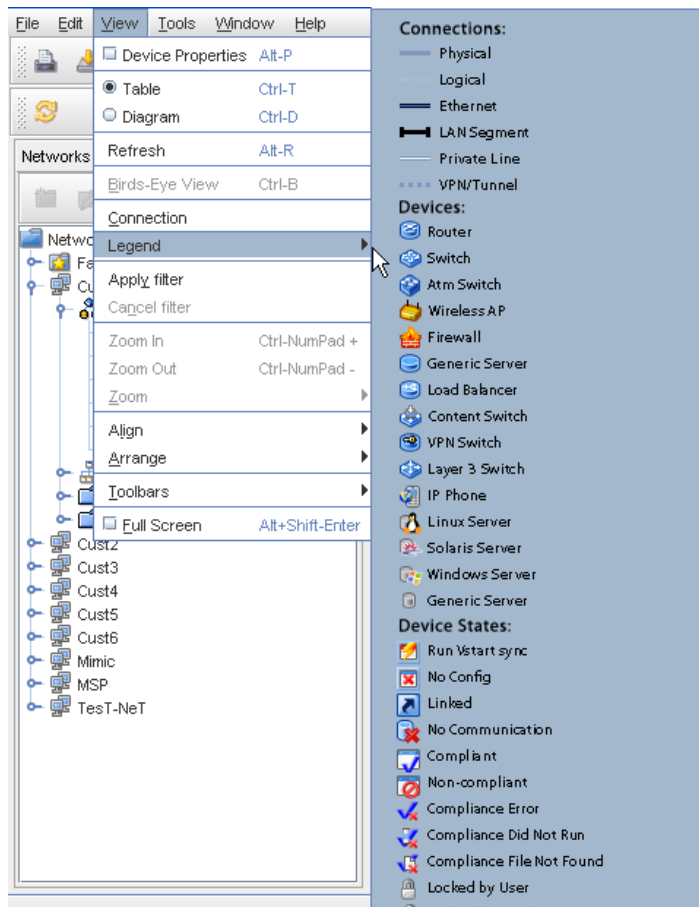
Security for managing symbolically-linked devices comes from the original device, or its primary network. Therefore, a user with no permissions to a device or its primary network, would visually see that device symbolically-linked in another network site, but they will not be able to view or manage that device.

See [Setting Network Permissions](#) for more information on device security.

## Sites - Legends

### Using the Legend

The Legend is part of the Diagram menu bar, and will only be available when using the Diagram layout to view your sites. Review the following legend information to discover the meaning of each icon when viewing your sites.



1 From the Menu bar, select **View**.

2 Next, select **Legend** from the options to view the legend details.

## Sites Property Tabs

### The General Tab - Editing Site Properties

Site properties contain contact and location information for the Site. By default, Sites inherit the properties of the parent Site, unless the Override check box is selected. Devices in Sites inherit Site properties which are displayed in the Site tab of the Device Properties.

Comments and Attachments can be associated with a Site. Site objects also support Data Fields.

The (General) properties of a site are the details entered when the site hierarchy was created. Added to this information are two additional tabs:

- [The Comments Tab](#)
- Attachments

---

**Important** You must follow the nesting hierarchy [Sites Best Practices](#). For more information, see [How Sites and Views Work](#).

---

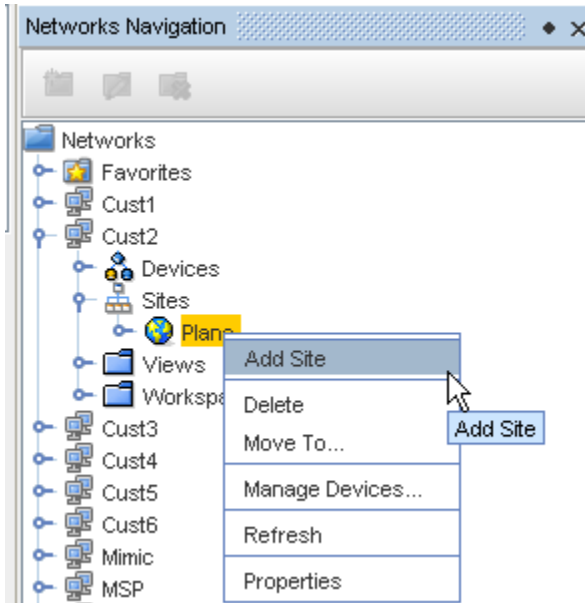
A site type can be edited in two ways:

- Editing the site type properties
- [Editing Device Associations to Sites](#)

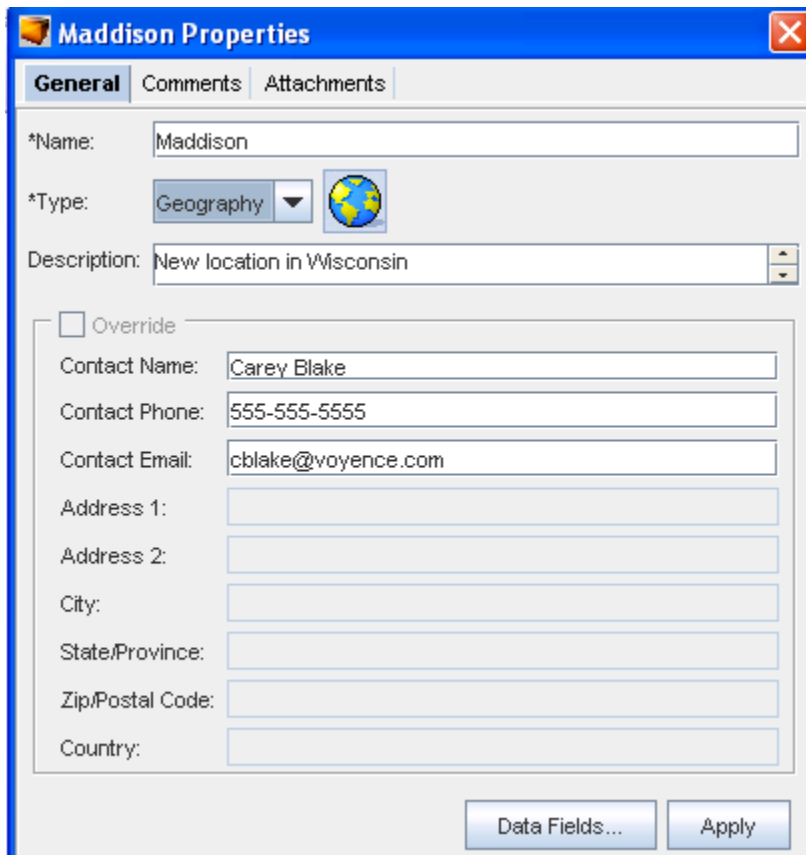
The ability to edit the site type properties allows you to modify the Name, Site Type, Description, and Override information, if needed. This information works hand-in-hand with the ability to edit the devices associated with the site type. Anytime that you edit the site type, you should review the devices associated to the modified site type.

To edit a site types properties,

- 1 In the tree menu, open the **Sites** branch.
- 2 Expand the tree menu, then right-click the appropriate **Site**.



- From the right-click options, select **Properties**. The [Site Name] Properties window opens.

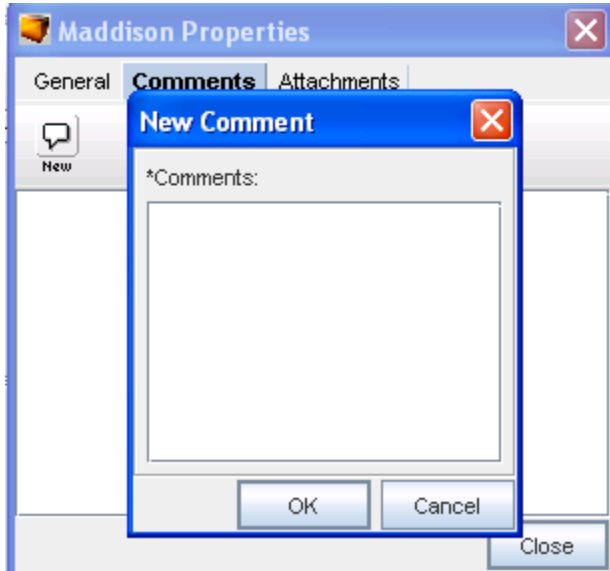


- All fields in the properties window can be edited. **Edit the information** as needed.

- 5 To enter contact information specific to this site (in the **Building**, **Floor**, **Room**, and **Rack** types - selected from the Type drop-down) check the **Override** box. The Contact field information window activates allowing you to add additional entries to the previously empty sections.
- 6 When finished, click **Apply**. The [Site Name] Properties window closes.

## The Sites Comments Tab

The **Comments** tab contains a running list of comments, related to the site.



The comments are logged as they are entered. Each comment identifies who created the comment, and when. A broken line indicates the end of each comment.

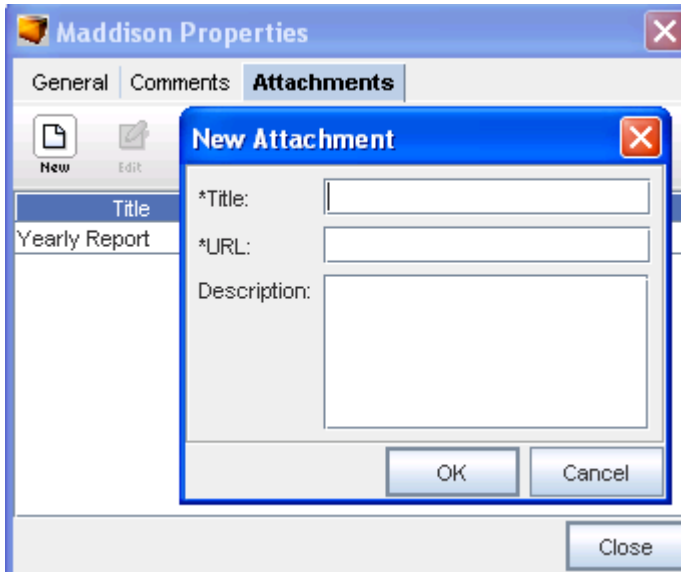
To create a new comment,

- 1 On the Comments tab, click the **New Comment icon**. The New Comments dialog window opens.
- 2 Enter your **comments**. The Enter key can be used to create paragraph breaks in the comments.
- 3 Click **OK**. The New Comments window closes. Each new comment is added to the top.
- 4 For each new comment, repeat **steps 1-3**.

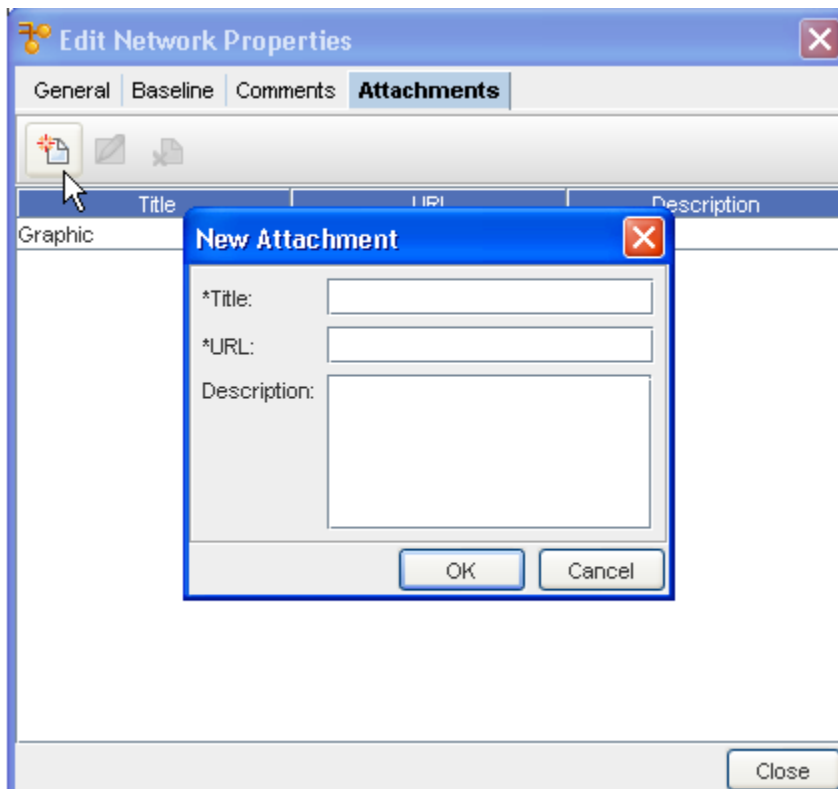
## The Sites Attachments Tab

The **Attachments** tab allows you to associate an external file to the site. This can include worksheets, documents, or .html files. Any document that can be opened in a web browser can be mapped as an attachment.

Multiple attachments can be added to each site.



### Adding an Attachment



To add an attachment,

- 1 On the **Attachments** tab, click the **New icon**. The New Attachments dialog window opens.
- 2 Enter a title **for the attachment** .
- 3 Enter a **URL**. Remember, the document must be saved in a format that will open in a browser.
- 4 If needed, enter a **description**.

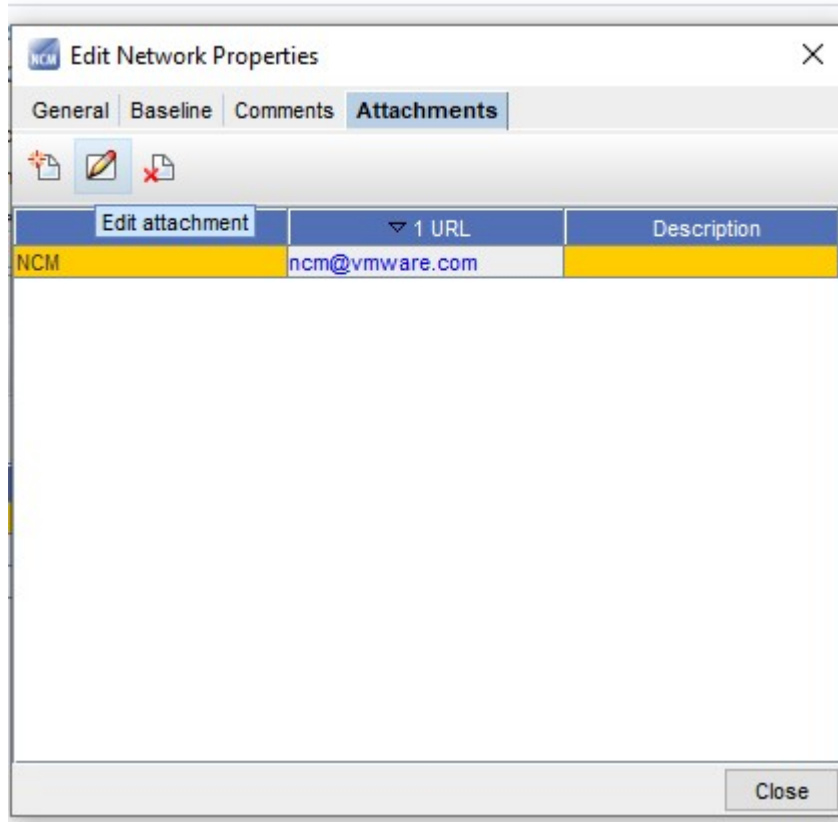
- 5 Click **OK**. The New Attachments window closes.
- 6 For each new attachment, repeat **steps 1-5**.
- 7 Click **Close** when you are finished adding attachments.

---

**Note** The Edit and Delete icons are only active when one or more attachments have previously been created.

---

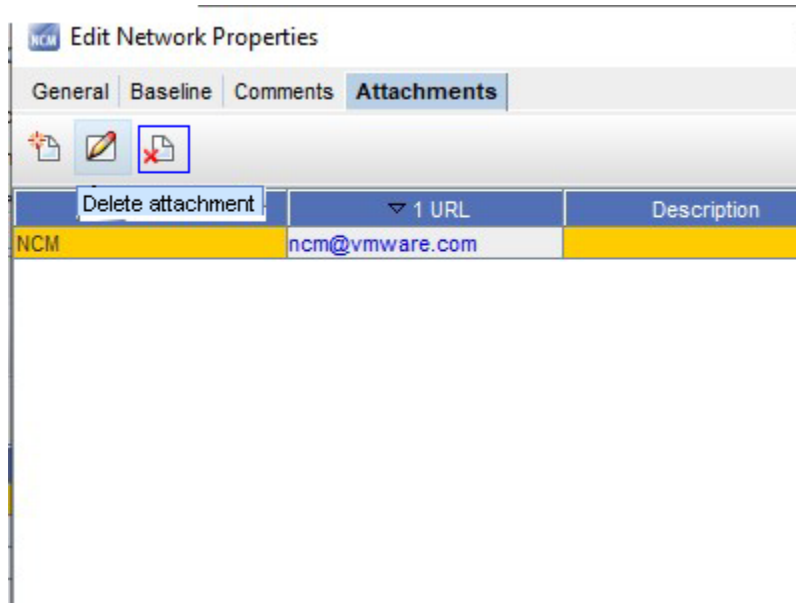
## Editing an Attachment



- 1 First, select an attachment from the listing of attachments.
- 2 On the Attachments tab, click the **Edit** icon. The Edit Attachments dialog window opens.
- 3 The Title, URL and Description fields can all be edited. Make any changes as needed.
- 4 Click **OK**. The Edit Attachments window closes. The attachment row updates with the edited details.
- 5 Click **Close** to close the Edit Network Properties window.

## Deleting an Attachment

When deleting an attachment, the actual document that you are referring to is **not** deleted. You are removing its linked reference from Network Configuration Manager.



- 1 First, select an attachment from the list of attachments.
- 2 On the Attachments tab, click the **Delete** icon. The Confirm dialog window opens asking, "Are you sure?".
- 3 To delete, click **Yes**.
- 4 Click **OK**. The Confirm window closes. The Attachment tab refreshes.
- 5 Click **Close** when you are finished deleting attachments from the list.

## Working with Views

### Views Overview

---

#### **Note** Views have no relationship with Sites!

---

Each network in Network Configuration Manager contains a single view folder construction, which is created at the same time as the network. There is no requirement to create and manage views within each network.

If your organization prefers to manage network resources using sites to create a geographical relationship, there may be no benefit to organizing your devices logically in Views. By default, the views folder is empty. However, a separate view, called the All Devices view is provided and populated with every device discovered in the network.



As there is no need for a relationship to existing between devices in a view, there are no predefined view types. And unlike Sites, devices can display in as many Views as needed, eliminating the need to support symbolic-linked devices in Views. Views are simply logical collectors for devices, and as such have no attributes except for having a name.

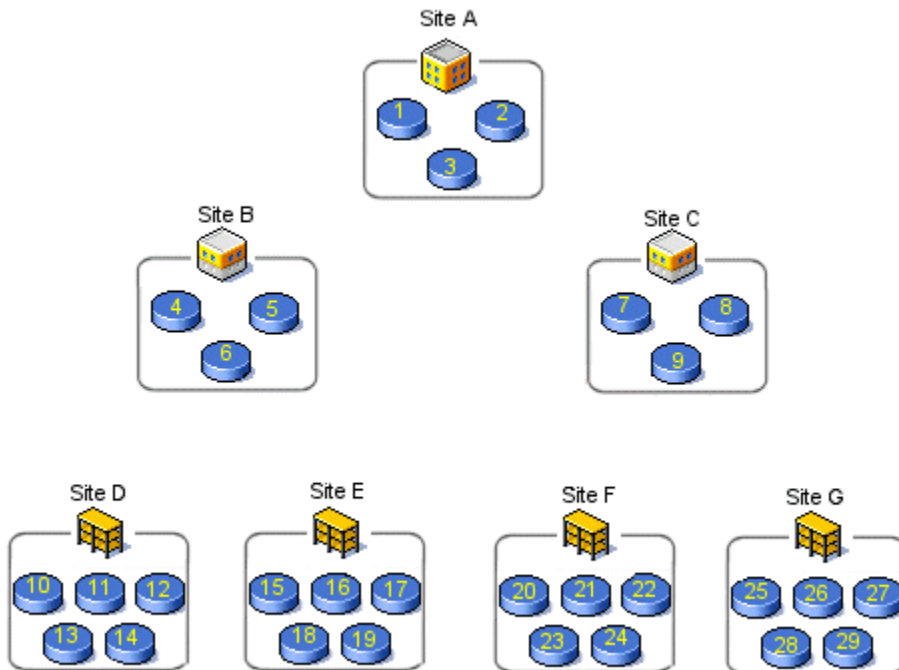
Views and their folder structure can be completely customized to fit your organizational needs.

- One sub-set of folders could be dedicated to Views of devices organized by vendor and model.
- Another sub-set could be dedicated to devices sorted by connection type.
- A third could be grouped by organizational responsibilities. In effect, you can slice and dice your devices any way you choose in Views.

Views enables you to create and organize collections of the devices in a network. When creating a view of a device, there is not a dependency on site type, logical connections, or physical location. A view allows you to select devices and group them together.

As an example, the following is a collection of devices in a network. Using the devices in the collection, you could make the following Views. Since devices in a view do not require a relationship, physical relationships, or logical connections, the Views are random groupings of devices of your choosing.

View 1	View 2	View 3	View 4	View 5
Contains Devices: 1, 7, 20, 21, 24	Contains Devices: 4, 9, 12, 18, 23	Contains Devices: 3, 10, 11, 14,	Contains Devices: 5, 6, 13	Contains Devices: 25, 26, 27, 28, 29



**Note** The examples are not the only view scenarios that can be extracted from the graphic.

## View Memberships

Views offer a unique feature that allows you to automatically assign devices to a view through the use of memberships. Memberships provide a dynamic network filter capability in a view. You do not need to manually assign devices to a view with a membership filter.

Memberships are based on the same pre-defined attributes, providing the ability to create device types or technology type memberships, or any combination of the two. For example, to see a view that contains all routers in your network that have Frame Relay connections.

You could easily create a new, empty view named "Frame Routers" and set the membership of that view to include device type 'router', and technology type 'frame relay'. At that point, the view would be populated with all Frame Relay routers. Additionally, the view will dynamically update each time it is opened with any new frame routers that have been discovered into the network, and delete any that have been removed from the network.

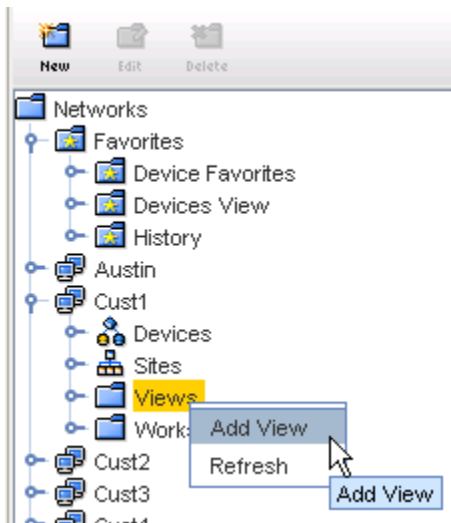
View memberships provide a quick and flexible way to logically segment your network by device and/or technology.

See: [How Sites and Views Work](#) for more information.

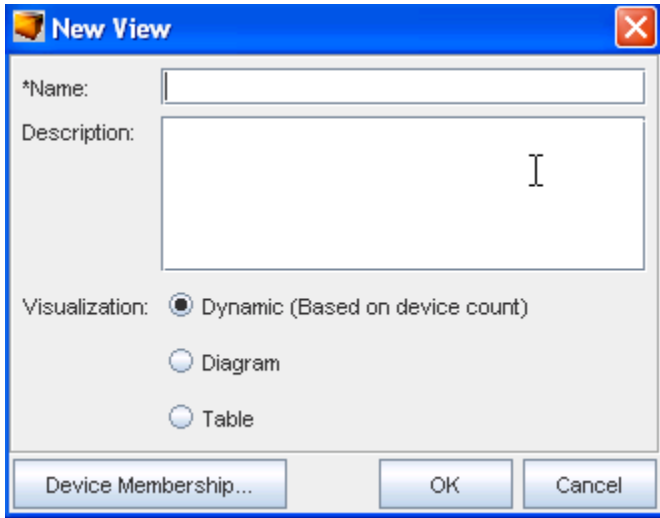
## Creating Views

To create a view:

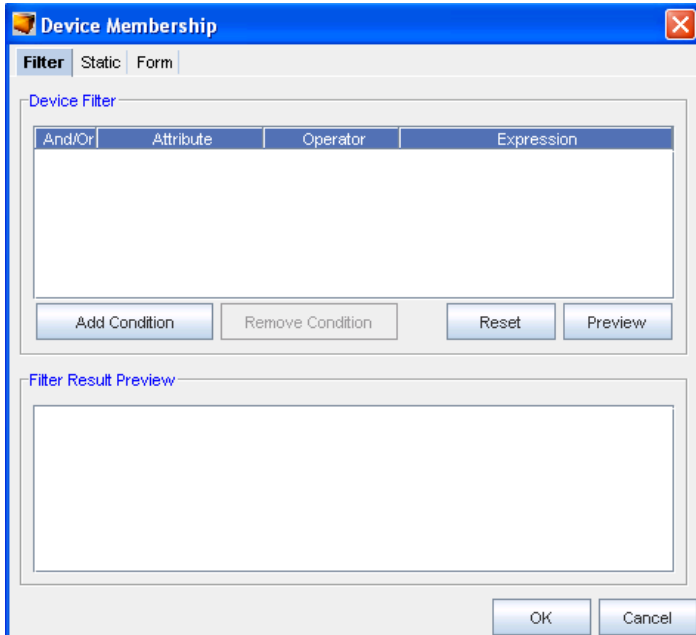
- 1 In the Networks navigation tree, right-click **Views**.
- 2 From the menu options, select **Add View**.



The **New View** window opens.



- 3 In the New View window, enter the **view name**. There are three options for how the view will display when opened.
  - **Dynamic** - (based on the device count. This will open in either the diagram or table view, depending on the device count). Note that this is the default.
  - **Diagram** - layout using device icons
  - **Table** - layout of device properties in table format
- 4 To change the default setting, select a new **visualization** (view) option.
- 5 To add devices to the view, click **Device Membership**. The Device Membership window opens.



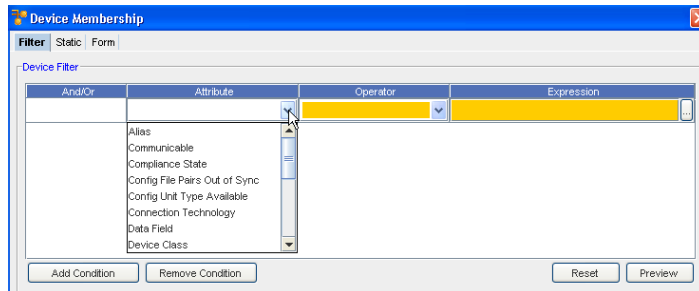
The Device Membership window contains three tabs:

**Filter** Allows you to filter devices by setting conditions based on the device type, name, vendor, or model, or other criteria, and then save the filter settings

**Static** Allows you to select from a list of all the available network devices

**Form** Allows you to select from a list of queries

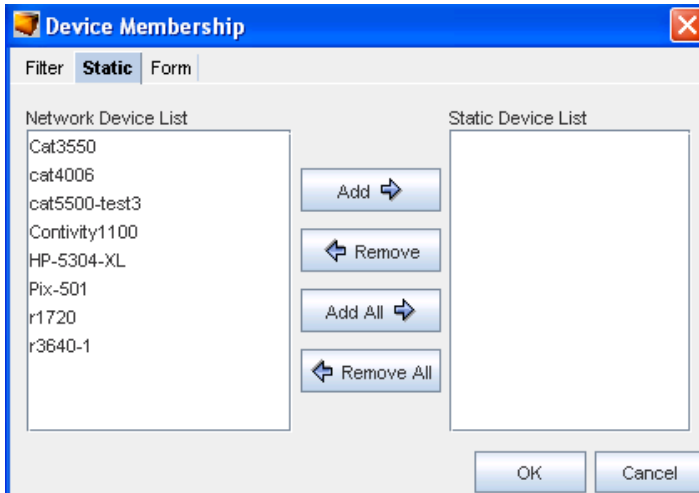
To filter devices:



- 1 Click **Add Condition**. A row is added in the Device Filter section. Determine if you want to use the **And/ Or** for the filter, then select accordingly.
- 2 Click once inside the Attributes column, the attributes the devices can be defined by are displayed.
- 3 Select an **Attribute** from the list.
- 4 Click once inside the **Operator** column. Select an **Operator** from the list.
- 5 Double-click once inside the **Expression** column. Select from the available options (if provided), or enter an expression. Enter the **Expression** that defines the attribute.
- 6 If entering more than one filter, click **Add Condition**. A new row is added to the Device Filter section.
- 7 To add additional filters, repeat **steps 1-6**.
- 8 When the filters are set, click **Preview**. A preview of the filtered results displays in the Filter Result Preview window.
- 9 When finished setting the filter, click **OK**. The Device Membership window closes. The filter devices display in the selected view.

To select from a static list of network devices:

- 1 In the Device Membership window, select the **Static tab**.



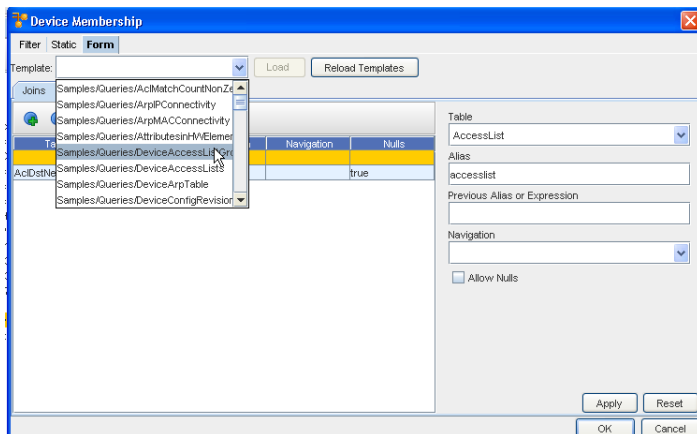
The Static tab contains two columns:

- 2 Using the **Add** and **Remove** buttons, create a list of static devices from the selections in each list.
- 3 When finished, click **OK**. The Membership Device window closes.
- 4 On the New View window, click **OK**. The New View window closes, and the created view opens, allowing you to review the configuration.

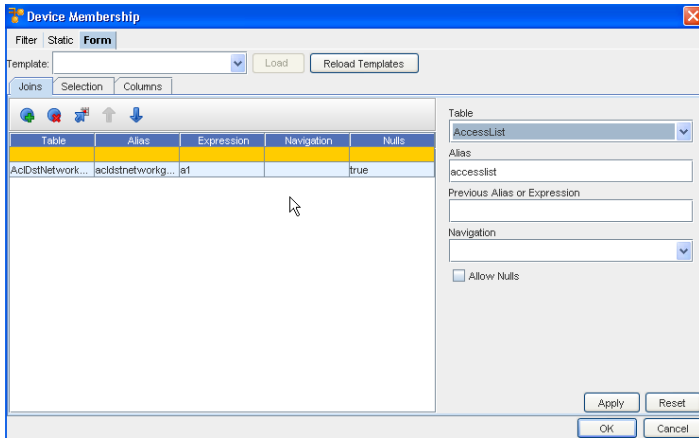
**Network Device List** Here are the devices that are associated with your network. These devices are available even if they are not set up in a site hierarchy.

**Static Device List** These are the devices that are used in a defined view.

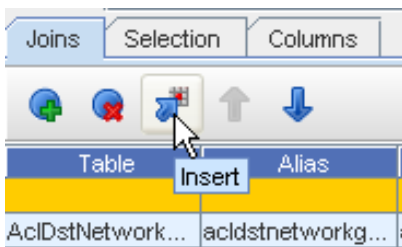
To use the Form tab:



- 1 From this tab, first click the **Template** drop-down, and then select a template from the list.
- 2 If you are not using a pre-defined template, make selections from the **Table** drop-down.



3 Click the **Insert** icon to insert a table.



4 Add an **Alias**, and also a **Previous Alias or Expression** .

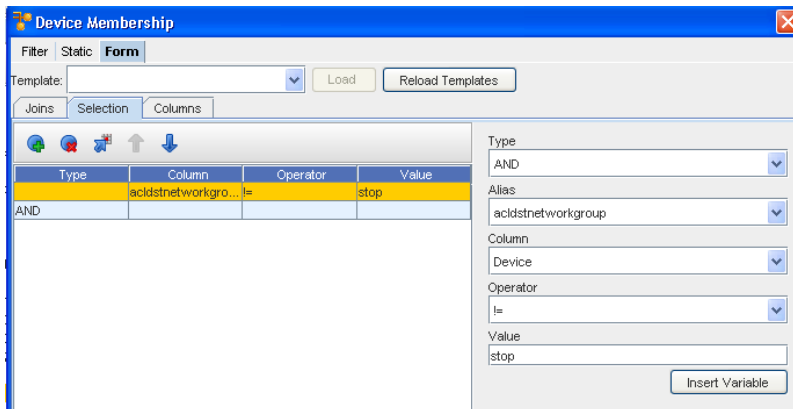
5 Select a **Navigation**.

6 Check to **Allow Nults** if needed.

To complete the Selection section:

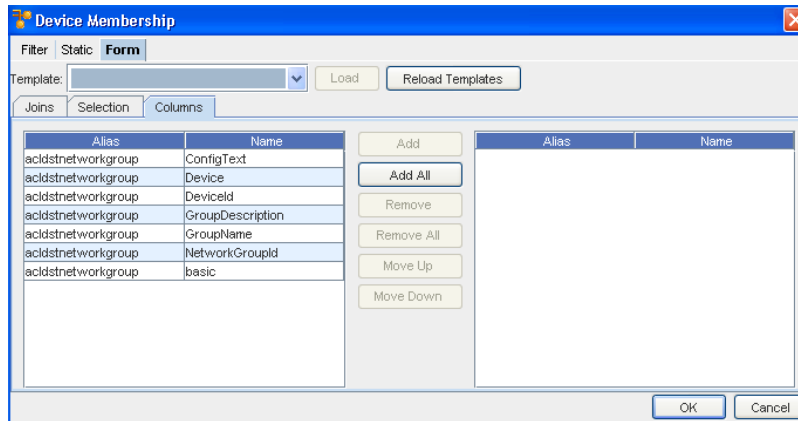
1 Insert a line, then select a **Type**, **Alias**, **Column** and **Operator** from the drop-down arrow menus.

2 Enter a **Value**, then click **Ok**.



**Important** Ensure you note the red warning signs and information. You must make sure those errors are gone before clicking OK to continue.

To complete the Columns section:



- 1 First determine the **columns** you wanted added, then select them from the listing.
- 2 Next, use the **Add** or **Add All** to move the selected columns into the right pane.
- 3 Click **Ok**.
- 4 Now, back at the **Filter** tab, click **Apply**.

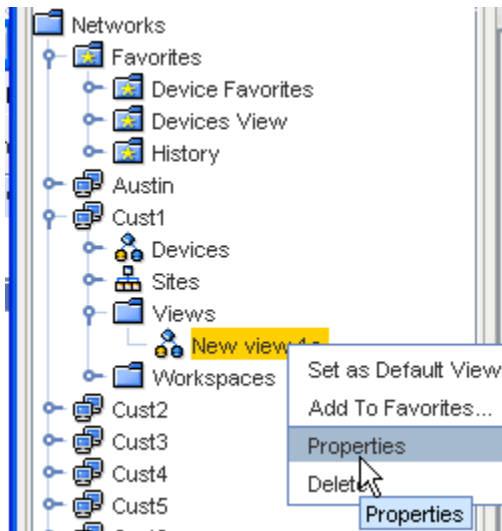
## Editing Views

There are two ways to edit a view:

- Editing the general properties of the view
- Editing the devices within the view

To edit the view properties,

- 1 In the navigation pane, select the **Network**, then **Views**.
- 2 Right-click on the **View**.



- 3 In the right-click menu, select **Properties**. The [View Name] Properties window opens. All text fields are editable. Make changes as needed.
- 4 When finished, click **OK**. The [View Name] Properties window closes.

---

**Note** You can select this view as your **Default View**, and you can also Add this View to your **Favorites**.

---

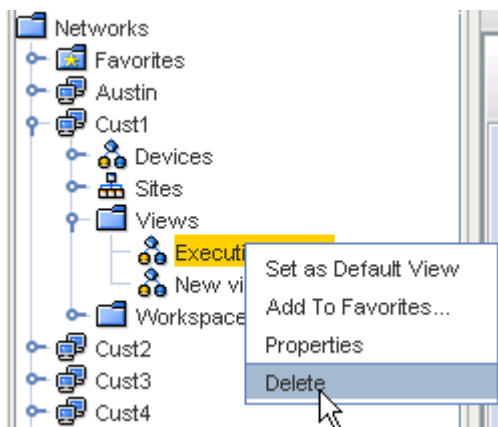
To edit devices within a view,

- 1 In the navigation pane, select the **Network**, then **Views**.
- 2 Right-click on the **view**.
- 3 In the right-click menu, select **Properties**. The [View Name] Properties window opens.
- 4 Click **Device Membership...** The Device Membership window opens.
- 5 You have three options:
  - On the **Filter** tab, use device filters to locate devices
  - On the **Static** tab, select from a list of network devices
  - On the **Form** tab, make your edit changes in the Joins, Selection, and Columns tabs
- 6 When finished, click **OK**. The [View Name] Properties window closes.

## Deleting Views

To delete an existing view,

- 1 In the navigation pane, select the **Network**, then **Views**.
- 2 Right-click on the **View**.
- 3 In the right-click menu, select **Delete**.



The Confirm window opens asking: Are you sure?

- 4 If okay, click **Yes**. The confirm window closes.



- If the navigation pane does not automatically refresh, right-click on the Network's View folder and click **Refresh**.

## Working with Tools

### Network Configuration Manager Tools Overview

Network Configuration Manager offers you quick access to the tools you need to complete tasks using dynamic features and robust functionality. For example, while you are in the Launch Window, you can click **Tools** in the menu bar to go to the listing of available Tools, and then select the tool you want to work with to complete any number of tasks.

This tools selection list is where you begin working through most of your tasks and procedures within Network Configuration Manager.

There are **two separate Tools options** available:

- Tools link from the Launch window.
- Tools link when viewing Devices, Sites, Views and Workspaces.

The following information details the selections available when you select **Tools** from each instance.

Tools	Window	Help
Networks Navigation	F6	
Dashboard	F8	
Automation Library	F3	
Schedule Manager	F7	
QS Inventory	F9	
Event Manager	F11	
Data Field Manager		
Metadata	F12	
System Administration	F4	
EMC M&R		
Change Audit	Ctrl-U	
Global Device Search	Ctrl-S	
Single Device Auto Discovery		
Template Merge		
Change Password		
Change RSA Tokens PIN		

Depending on what tasks you want to complete, or what information you want to view, make your selections from this **Tools** list.

- Networks Navigation
- The Dashboard
- Working in the Automation Library
- Schedule Manager Overview

- [OS Image Inventory Manager Overview](#)
- [Event Manager Overview](#)
- [Introducing the Data Field Manager](#)
- [Metadata Information](#)
- [Getting Started - System Administration Overview](#)
- [EMC M&R](#)
- [Working with Change Audit](#)
- [Global Device Search Overview](#)
- [Single Device Auto Discovery](#)
- [Template Merging](#)
- [Changing Your Password](#)
- [Changing Token Pins](#)

## Working with the Schedule Manager

### Schedule Manager Overview

The Schedule Manager provides a view into **all jobs scheduled** , and their **job status** within Network Configuration Manager.

When any changes have been made to the Schedule Manager, such as Jobs Added, Jobs Changed, or Jobs Removed, the Schedule Manager view is automatically refreshed (updated) to reflect these change.

You can access the Schedule Manger from the **Tools** option in the menu bar.

---

**Note** Security Permissions apply, so you cannot view jobs you do not already have permission to view.

---

Tools Window Help	
Networks Navigation	F6
Dashboard	F8
Automation Library	F3
Schedule Manager	F7
QS Inventory	F9
Event Manager	F11
Data Field Manager	
Metadata	F12
System Administration	F4
EMC M&R	
Change Audit	Ctrl-U
Global Device Search	Ctrl-S
Single Device Auto Discovery	
Template Merge	
Change Password	
Change RSA Tokens PIN	

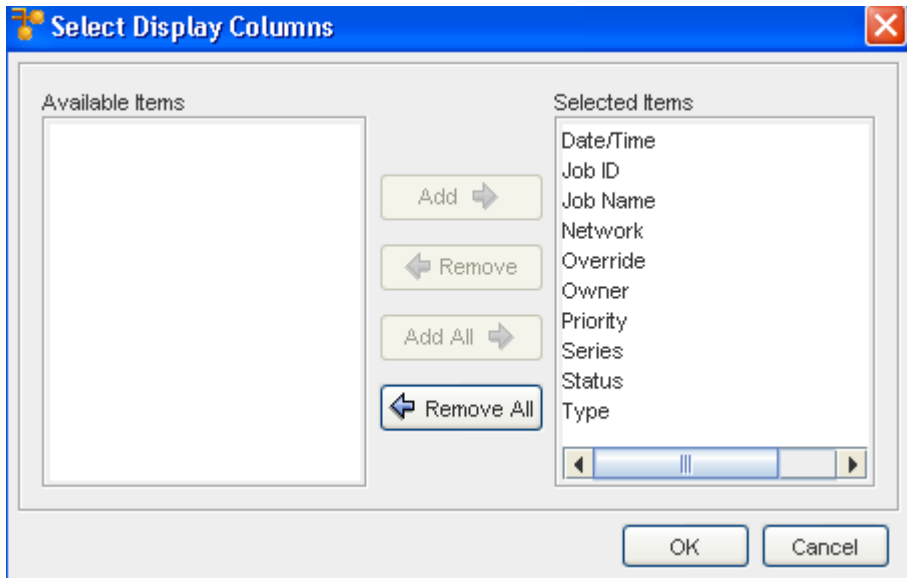
The Scheduler Manager has separate sections detailing information pertaining to various jobs. These include the **Job View** and the **Recurring Series**. The Recurring Series tab displays primary information for recurring jobs.

The screenshot shows the 'Schedule Manager' window with the 'Job View' tab selected. Below the toolbar, there is a 'Quick Filter' section with a dropdown menu set to 'Default Job' and a 'Delete' button. A filter expression is displayed: '(Date >= 02/02/2009) And (Date <= 03/04/2009) Or (Date is Not Defined) Or (Status = Running)'. Below this is a table with the following data:

Series	Status	Job Name	Netw...	Job ID	Date/Time	Owner	Overrid
	Pending	polycypull	Cust1	100110	Run upon app...	sysadmin	

Within the **Job View** tab contents, the first section of the Schedule Manager details each job's information. The various columns give you specific job information.

- 1 To view even more job information, right-click on any column heading to see the available column options in the **Select Display Columns** window. Move column headings between the **Available Items** and **Selected Items** to view more or less job information displayed within the Schedule Manager.
- 2 After making your selections, click **OK**.



**Note** If you have previously defined filters, use the Quick Filter drop-down arrow to see the selections of filters, then make a selection from the list. To designate a new filter, click the Apply icon, and then define your filter criteria.

This **Status** tab displays the current status of each job. Jobs fall into the following categories:


- Completed
- Approved
- Rejected
- Running
- Failed
- Pending
- Completed/Warning
- Cancelled
- Partially Completed
- Hold



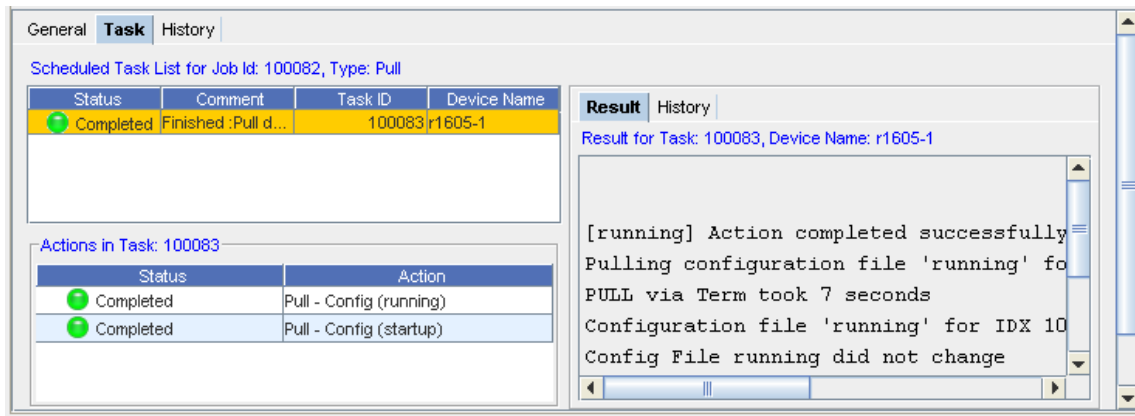
**Note** The tool bars displayed in Job View and Recurring Series include some different icons. To review the icons in the Recurring Series that differ from those in the Job View see: [Recurring Series](#).

Once a job displays in the Schedule Manager, the following tasks can be completed:

- Printing a copy of a Job
- Exporting a Job (copy)
- Filtering the Job Listing
- Quick Filter
- To Save the Current Filter
- Executing a Job
- Canceling a job
- Copying a Job
- Copying a Job
- Adding a Data Field
- Deleting a Job
- Changing the Job Status
- Schedule Manager (Override) Update Credentials
- Job Details
- Reviewing Job/Status Summary
- Refreshing a Job List

- 3 Within the **Job View** tab, view more information by clicking the **Details**  icon. The bottom section of the Schedule Manager displays the **details** of a job, including the **General** and **Task** information for the job selected from the list.

### Schedule Manager tool bar options



The screenshot shows the 'Task' tab of the Schedule Manager. It displays a 'Scheduled Task List for Job Id: 100082, Type: Pull' with one task completed. Below this, it shows 'Actions in Task: 100083' with two completed actions. On the right, a 'Result' window shows the execution details for task 100083 on device r1605-1, indicating a successful pull of a configuration file.

Status	Comment	Task ID	Device Name
Completed	Finished :Pull d...	100083	r1605-1

Status	Action
Completed	Pull - Config (running)
Completed	Pull - Config (startup)

```

[running] Action completed successfully
Pulling configuration file 'running' fo
PULL via Term took 7 seconds
Configuration file 'running' for IDX 10
Config File running did not change
    
```

## Recurring Series

There are two tabs located within the Schedule Manager.

- The **Job View** is just that, a listing of the current jobs that have been scheduled to run, along with information pertaining to each job.
- The second tab at the top of the Schedule Manager is the **Recurring Series** tab. If there have been any jobs scheduled to run on a **Recurring Series**, those jobs are listed within this tab. The Recurring Series tab displays primary information for recurring jobs.





This tab is much like the Job View tab, giving you access to details, and providing the same information on each job through the General and Task tabs.

Notice that the tool bar options within the Recurring tab are more limited than those options on the Job View tab. This is because the recurring jobs are very specific. For example, you **cannot Execute or Cancel a recurring job**.

Note the following icons:

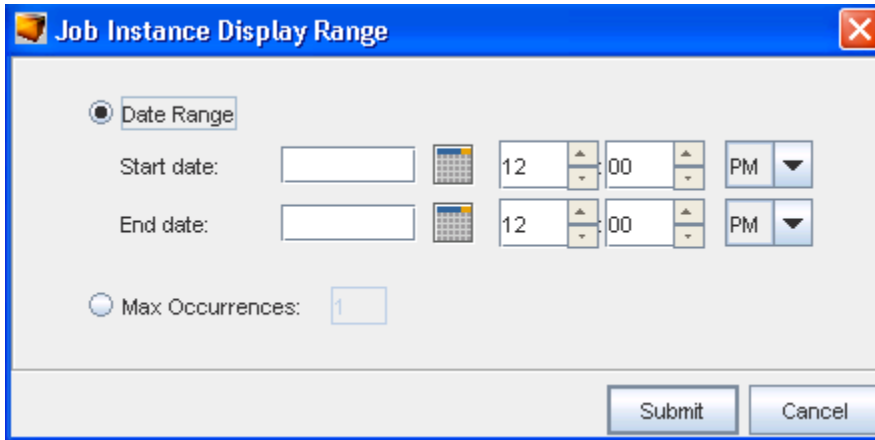


When the recurring **Series**  icon is selected, the original or primary recurring jobs are listed. These are the jobs that were originally created to run specifically at set intervals.

The **Instances**  icon, when selected, allows you to make changes in the "instances" you want to run **from** the originally scheduled job. Each time a scheduled recurring job runs, it creates an instance.

When the Instances icon is selected, the **Job Instant Display Range** window opens. From here, you can make changes to an "instance". For example, if you want the **Max Occurrences** to be 10, click the radio button, and insert the number **10**. Click **Submit** when you have made selections from this window. This tells the application that you want the original recurring job to run 10 instances.

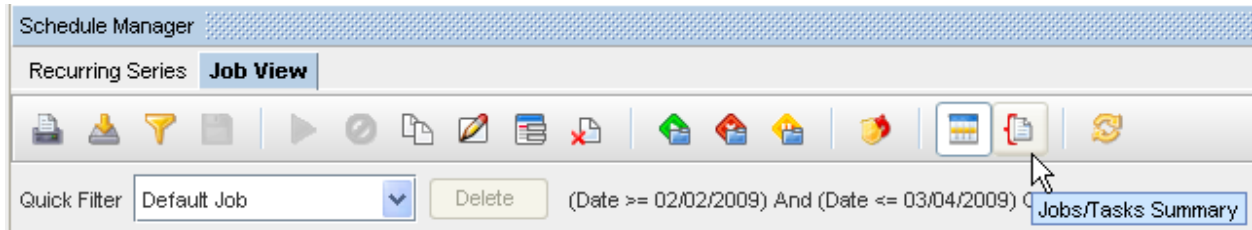
You can also alter the **Date Range** of the "instance" by first clicking the Date Range radio button, then entering the day and the time for both the Start and End dates.



## Viewing a Scheduled Job Summary

When viewing the Schedule Manager, keep in mind that it now automatically refreshes when new jobs are added, or when there is a change in a job status. You will always get the latest, real time view of the Schedule Manager.


To view a summary of the scheduled jobs and their current status, select the **Summaries** icon on the tool bar bar.

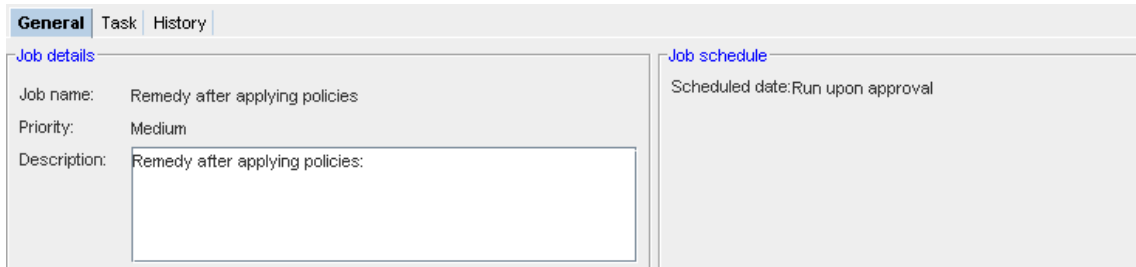


The Summary of jobs is displayed to the left of the listing of jobs. Notice that the summary includes the total count of the jobs, divided into status categories.

## General Tab

### Job View

- 1 With the **Details** icon  clicked and the details displayed on the Schedule Manager window, select the **General** tab.
- 2 You can view the information contained within the General tab for any job you have selected from the list.

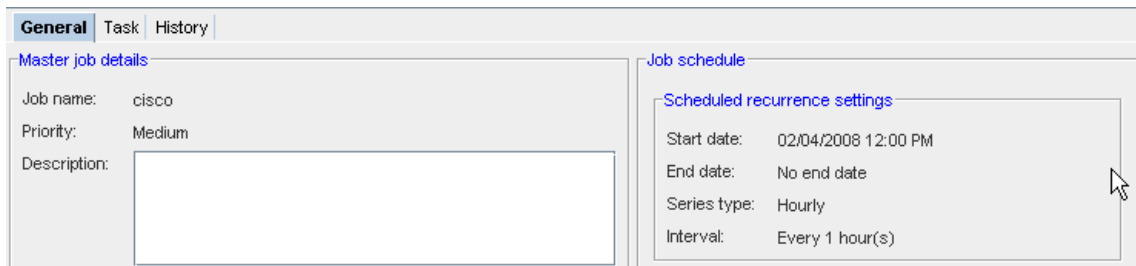


3 Switch to the **Task** tab, or the **History** tab for more detailed information.

### Recurring Series



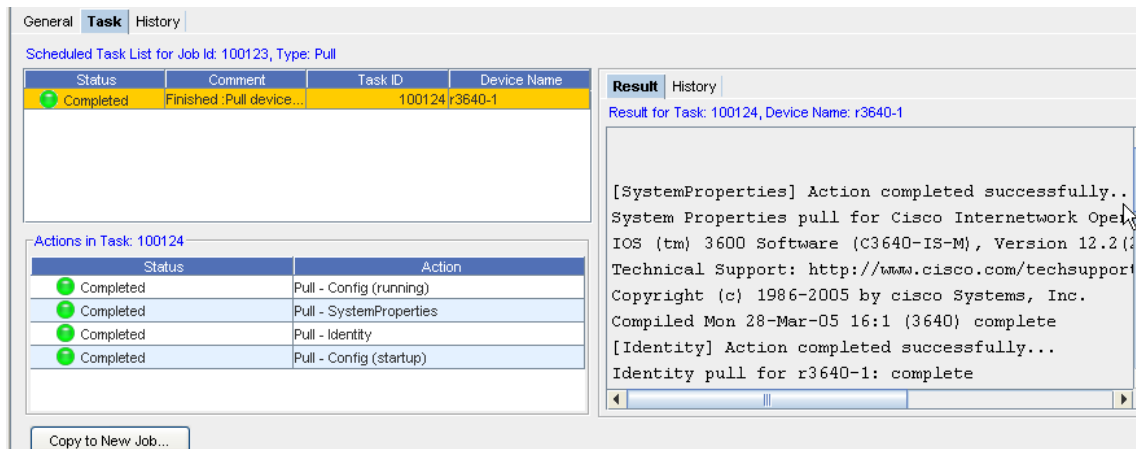
- 1 With the **Details** icon clicked and the details displayed on the Schedule Manager window, select the **General** tab.
- 2 You can view the information contained within the General tab for any job you have selected from the list.



3 Switch to the **Task** tab, or the **History** tab for more detailed information.

### Task Tab

- 1 To view more details concerning any job that has been scheduled, first select a job from the listing. In this example, **Job ID 100083** has been selected from the list.





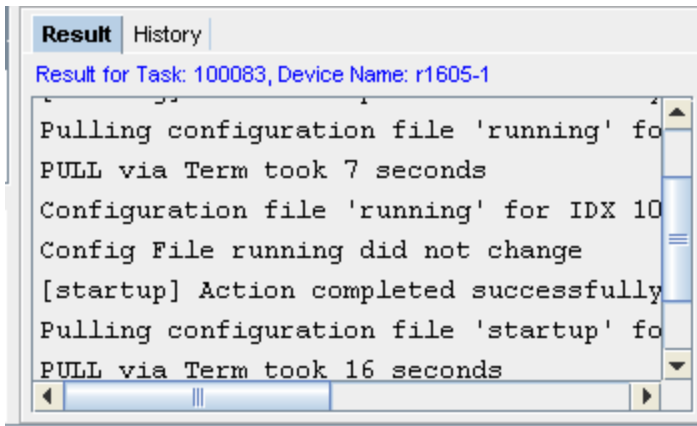
- 2 Within the **Task** tab, the **Scheduled Task List for Job Id:100083, Type: Pull** is displayed. This indicates that a Network push was requested. This push entails that all devices within that specific network are affected.
- 3 As you can now complete multi-config pushes, the **Actions in Task:** section details the results of each action associated to each task . View the **Result** tab to see the results for each action associated with the Network Push task.

---

**Note** The Actions in Task number will always be one number higher than the Job ID number.

---

- 4 The **Result** section details the results for the Task (shown here at 100057), and the Device as Router. Scroll through this section to view the actions results. The **Results** tab shows information **associated to the Action**.




---

**Note** **E rrors and warning** from Device Services (detailed in the Schedule Manager) are **color coded**. Errors are displayed in **red**, while warnings are in **orange**.

---

Within the contents of the Results tab, there may be symbols accompanying the contents.

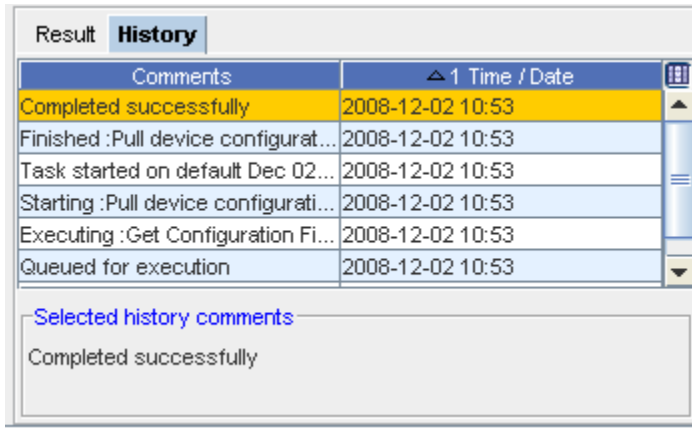
The following symbols are used to help define the contents.

- 5 Next, click the **History** tab to view the history details of the task. The **History** tab displays information **associated to the Task** .

Result tab,

Symbol	Description
>>>	Indicates information is included
!!!	Indicates here is a warning
---	Indicates negative information
===	Indicates information set on device

History tab,



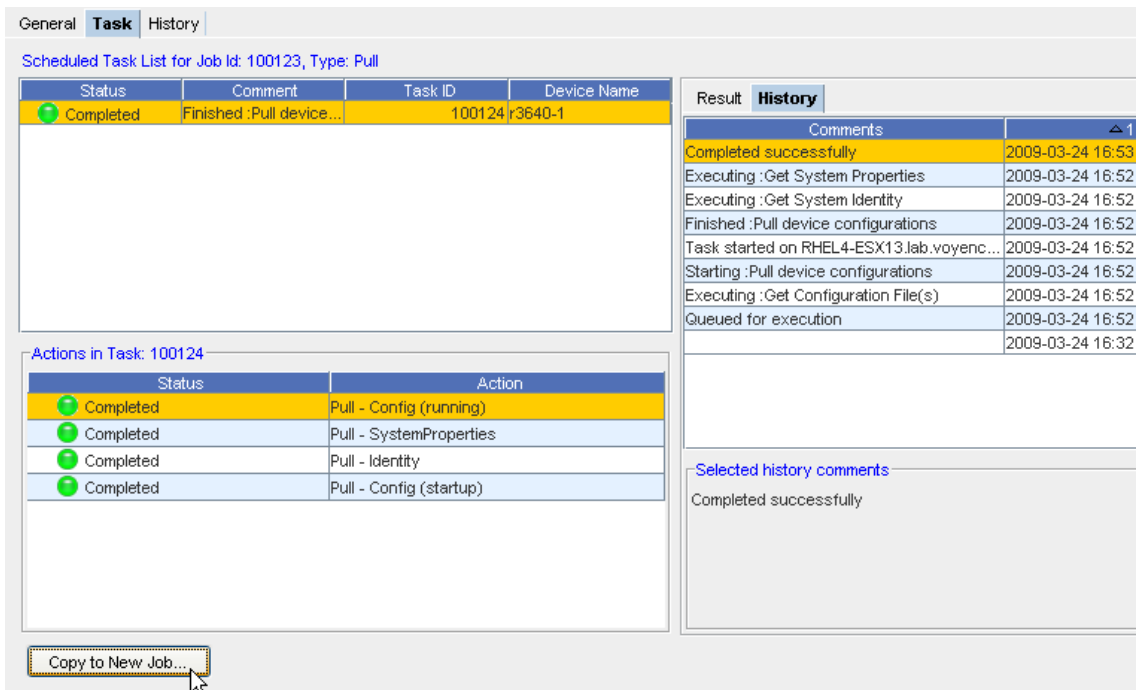
Selected task comments,

From this section, you can view the **Selected History Comments** on the each task. Scroll to view all comments.

**Note** View the **Task** tab in the **Recurring Series** section as well to get additional job information for specific Recurring jobs.

## Additional Task

From the **Task** tab you can access an additional Task. For example, with the **Job View** displayed, and the **Task** tab selected, you can access the following task - **Copy to New Job** - for **Pull Only** jobs.




This takes you to the Schedule Copy Pull job window.

## Printing a copy of a Job

From the Schedule Manager window, you can access the icon to **Print a copy** of the job displayed.



- 1 Select the Job from the listing of jobs displayed.
- 2 Click the **Print** icon  to use your browser's print facility. The printed copy contains the Status, Network, Job ID, and more.

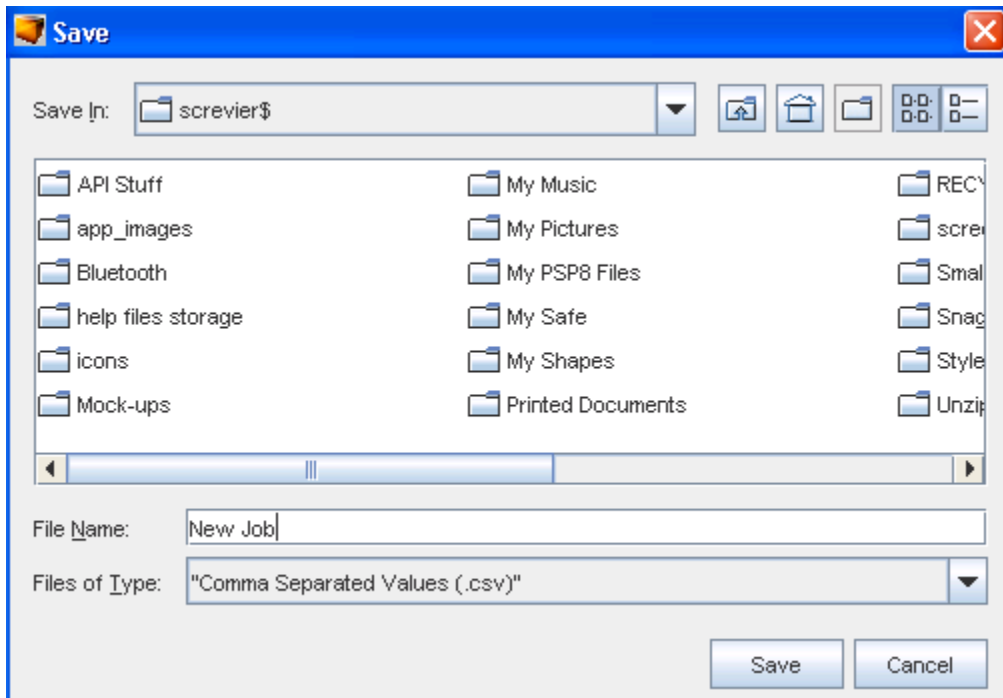
## Exporting a Job (copy)

From the Schedule Manager window, you can access the icon to **Export a copy** of the job displayed.



- 1 With the list of jobs displayed, click the **Export** icon .


The Save Job window opens.



- 2 Determine **where** you want to export this job to, and the **File Name**, then click **Save** after making your selections.
- 3 You can also change the File Name, as well as designate the File Type when exporting a job. A copy of the job you exported is now stored in the format (Files of Type) you selected.

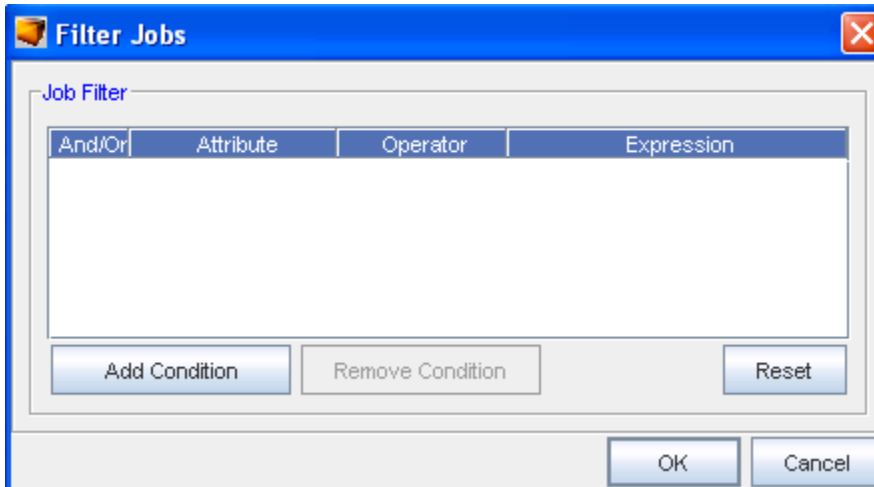
## Filtering the Job Listing

From the Schedule Manager window, you can access the icon to **Filter the list of jobs** displayed.

- 1 With the list of jobs displayed, select the Filter **Apply** icon  on the Schedule Manager window.



The Filter Jobs window displays.



- From here, use the **Add Condition** button to add another filter. Remember, you must have an Expression for each Attribute.

---

**Important** Click **Reset** to remove any existing filters.

---

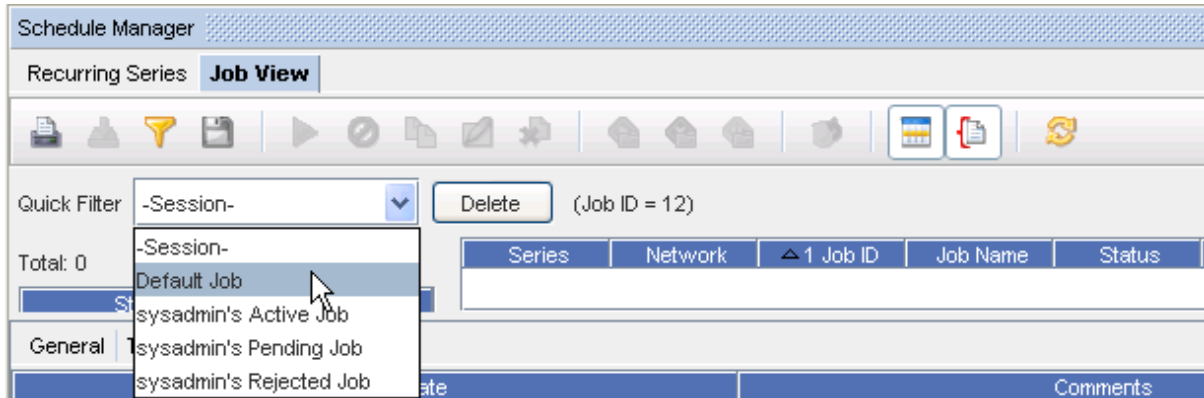
- You can also use the **Remove Condition** to have an existing conditional filter removed.
- Click **Ok** when you have made your filtering selections.
- You can Save the current Filters using the **Save** icon.

### To Save the Current Filter

If you have changed filters, (see the Filter Job window above) and used the **Apply** icon, you can now **Save** that new filter.



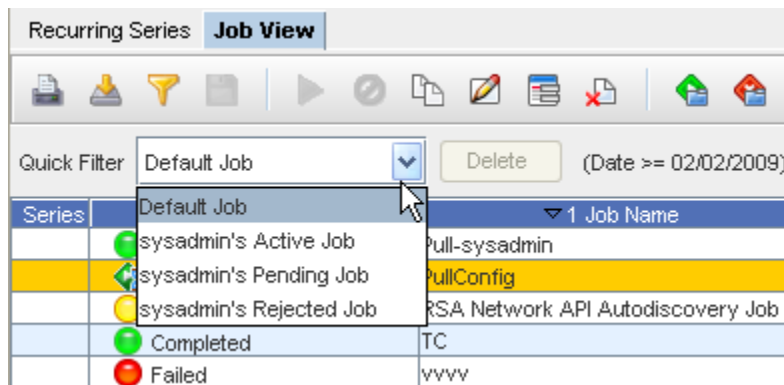
- Click the **Save Filter** icon, to name and save that filter,.
- The next time you want to select a filter, using the Quick Filter drop-down selections. The newly save filter is now in the listing, and can easily be selected.



- Using the Quick Filter drop-downs, you can also Delete a filter you have saved. Select a filter name from the list, then click **Delete**.

## Quick Filter

From the Schedule Manager, you can use the **Quick Filter** drop-down arrow options to determine what jobs you want displayed, by filtering.



You can use the Default to view all the Jobs in the Schedule Manager. You can also select from the following filters:

- Active
- pending
- Rejected

---

**Note** The Default is to show all jobs.

If you have perviously defined your own filters, you can use the **Delete** button to delete any selected user-defined filters from the Quick Filter drop-down options.

---

**Note** You cannot delete the system filters.

## Executing a Job

Use the **Execute** icon (where appropriate) to execute an existing job in the Schedule Manager listing. The job must have already been **scheduled and approved** , and you must have adequate permissions to complete this task.

- 1 Select the **job you want to Execute** from the listing of jobs.
- 2 Next, click the **Execute** icon.
- 3 Click **Ok** at the confirmation message.

## Canceling a job

Use the **Cancel** icon (where appropriate) to cancel a job in the Schedule Manager listing. You must have permission to cancel a job that has not yet run.



- 1 Select the **job you want to cancel** from the listing of jobs. Only Running jobs can be cancelled.
- 2 Next, click the **Cancel** icon.
- 3 Click **Ok** at the confirmation message.

## Copying a Job

Instead of recreating a job and tasks, an existing scheduled job can be copied, edited, and then scheduled as new.

Using the Schedule Manager, the following tasks can be completed:

- Copy an existing job, edit, and reschedule
- Edit an existing recurring job
- Delete an existing recurring job
- Filter the list to display specific job types
- Approve or reject recurring jobs
- Review the details of a recurring job

To copy a scheduled job,

- 1 From the menu bar, select **Tools - > Schedule Manager**.
- 2 On either the Job View or the Recurring Series tab, select a **job**. The grayed out icons in the toolbar now activate.

- Click the  **Copy icon** . The Schedule Copy Pull Job window opens.



The **Copied Job ID** number indicates that this job is a copy of an existing job.

- After you have entered the **new Job Name**, then go to the **Schedule Job** section of the window to Submit this job.

The 'Schedule Job' window is divided into two main sections: 'Job details' and 'Schedule job'.

**Job details:**

- Copied job ID: 100060
- \*Job Name: [Empty text box]
- Job owner: sysadmin
- Job description: [Empty text area]
- \*Priority: Low (dropdown menu)

**Schedule job:**

- Run in next maintenance window:
- Run upon approval:
- Run upon operator initiation:
- Run at scheduled date/time: [Empty] [Calendar icon] 12 [Up/Down] 00 [Up/Down] PM [Down]
- Run as recurring series:
  - Hourly: 
    - Start time: [Empty] [Calendar icon] 12 [Up/Down] 00 [Up/Down] PM [Down] [GMT-06:00] America/Chicago [Down]
    - End Time:
      - Never Ends:
      - Ends after [Empty] occurrences:
      - Ends on this date/time [Empty] [Calendar icon] 12 [Up/Down] 00 [Up/Down] PM [Down]:
    - Interval:
      - Every: 1 hour(s): [Input field]
  - Weekly:
  - Monthly:

Buttons at the bottom: Approve & Submit, Submit, Cancel



- 5 If needed, click the [Using the Notification Tab to Send an Email](#) and add users, add email addresses, and select the notification states for users who need to be notified of the new job.

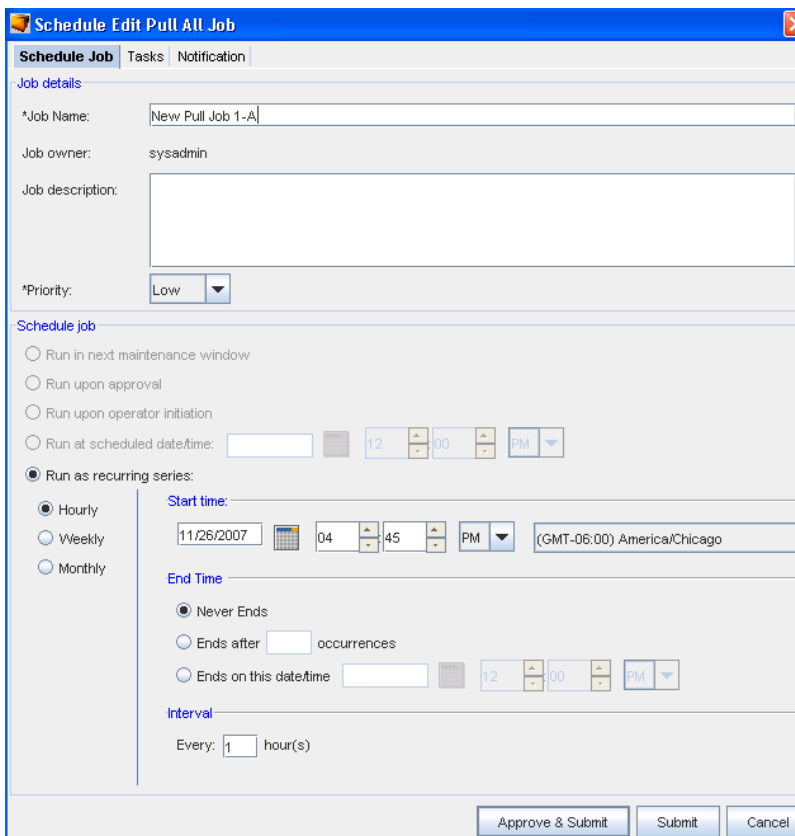
## Editing a Job

To edit a scheduled job,

- 1 From the menu bar, select **Tools** - > **Schedule Manager**.
- 2 On either the **Job** or the **Recurring Series** tab, select a **job**. The grayed out icons in the toolbar now activate. The job must be in a Hold, Pending, or Approved Status for you to complete an edit.



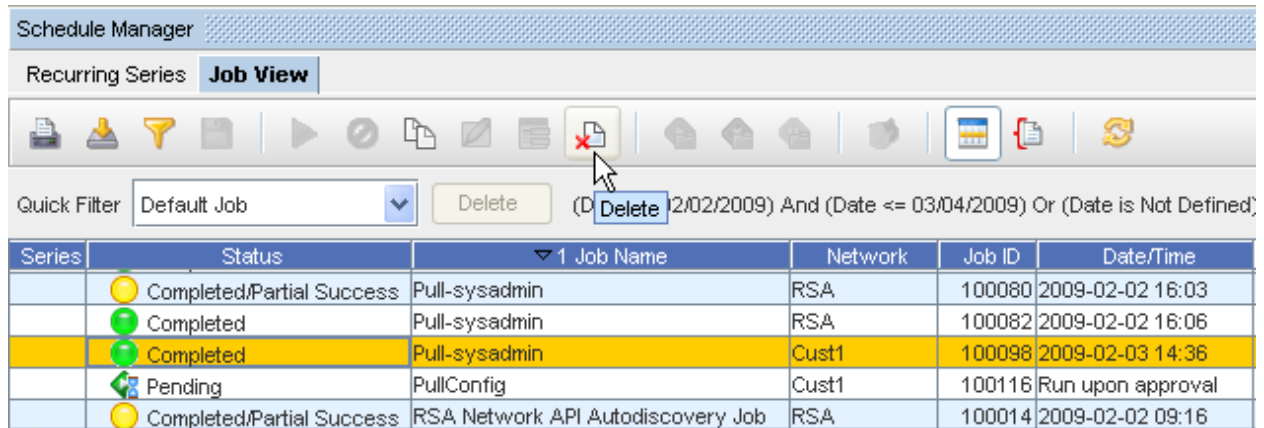
- 3 Click the **Edit**  icon. The **Schedule Edit** (for the job you selected) window opens.



- 4 At the Schedule Edit window, make any needed changes to the existing information, then at the **Schedule Job** portion of the window, make your selections for Submitting this job.
- 5 Click **Submit** when you have made your changes. You can click **Approve & Submit** if you have those permissions.

## Deleting a Job

Use the **Delete** icon (where applicable) to delete a job permanently from the Jobs list displayed in the Schedule Manager. You must have the correct permissions to complete a delete activity.



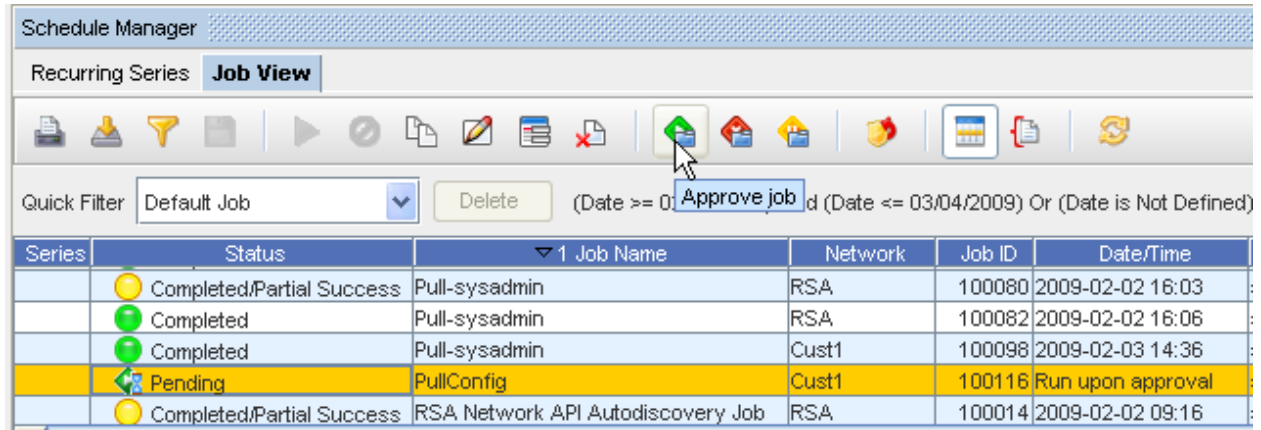
- 1 From the listing, **select the job** you want to delete.
- 2 Select the **Delete** icon from the tool bar.
- 3 Click **Ok** at the confirmation message.

## Changing the Job Status

If granted the appropriate permissions, you can change the status of an existing job.

- Review the listing of jobs within the Schedule Manager, and locate a job that is in **Hold or Pending status**.
- Highlight the job, then change the current status by selecting one of the options on the Schedule Manager tool bar. You can select:
  - Approve
  - Reject
  - Hold

### Approve



Reject



Hold



**Note** Note that the Schedule Manager automatically refreshes whenever there is a change to a job.


## Jobs in the Hold Status

For jobs that are in the **Pending** or **Hold** status, you have several features available to assist you in getting these job details. You can select to Approve those jobs if you have the appropriate permissions, or reject those jobs.

## Schedule Manager (Override) Update Credentials


With this option, you have the ability to override the existing credentials for a job or other non-scheduled operations. Only those users with the **Override Credential** permissions are allowed to override the credentials.



- 1 From the listing, **select the job** you want to override and Update the Credentials on.
- 2 Select the  **Update Credentials** icon from the tool bar.
- 3 At the **Job Credentials Input** window, you must enter the appropriate information needed to update (override) the credential.
- 4 Click **Ok** when you have completed updating the credential.

**Note** Note that the Schedule Manager automatically refreshes whenever there is a change to a job.

## Job Details


- 1 From the Schedule Manager tool bar, use the **Details**  icon to show or hide the **Job details** section of the Schedule Manager window. Once clicked, the General and Task tabs display in the lower portion of the work area, along with the Result, History, and Content tabs offering even more job information on the job and tasks.

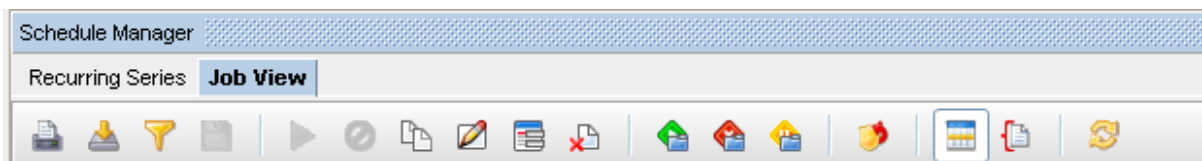


- 2 Clicked the icon once again, and the tabs (containing the job detail tabs) are no longer displayed.

## Reviewing Job/Status Summary

With the Schedule Manager displayed, you can select to review a Job/Status summary.

- 1 Select the **Summaries**  icon. The Job/Status summary information is presented in the left portion of the Schedule Manager window. This summary displays the total number of jobs, as well as the job count per status.



- 2 Click the **Summaries** icon again, to close this Job/Summary window.

## Refreshing a Job List

Once you have made changes to the existing list of jobs displayed in the Schedule Manager (for example, if you deleted jobs from the list), note that the Schedule Manager **automatically refreshes** whenever there is a change to a job.

You can also use the **Refresh**  icon to refresh the Schedule Manager.



## Displaying Columns in the Schedule Manager

Use this icon to select columns you want to display within the Schedule Manager.

- 1 Right-click any **column heading** to see the Select Display Columns window. The Select Display Columns window opens.
- 2 Using the **Add** or **Remove** arrows, make your selections on what you would like to have displayed as a column on the Schedule Manager window. Move the **Available Items** into the **Selected Items** pane, or remove items in the Selected Items column. You can use the Add All or Remove All buttons as well.
- 3 Click **Ok** when you have made your additions or removed existing columns.

## Scheduling Jobs

### Using the Scheduler

When viewing the Schedule Manager, keep in mind that it now automatically refreshes when new jobs are added, or when there is a change in a job status. You always get the latest, real time view of the Schedule Manager.

When a configuration change is ready to be scheduled to one or more devices in the Network, typically on completion of an Editor session, the scheduler is opened. The scheduler allows you to define when a job is run, and enforces workflow approvals.

The Scheduler allows you to designate when jobs are **pushed** to the network. Access to the Schedule option is available at the bottom of each editor window.

The Scheduler allows you to complete the following tasks:

- Set the Priority of a Job
- Set Run Times for all Jobs
- Set Recurring Job Schedules
- Approve Scheduled Jobs (user-permissions required)
- Submit Jobs for Approval
- Send Notifications to Other Users Regarding Job
- Review Job Tasks
- View Data Fields

When opened, the Schedule Job window contains three tabs:

<b>Schedule Job</b>	Contains general job tasks details and date configuration settings
<b>Tasks</b>	Contains the task details of the job. Including the content of the <b>push</b> and the devices that are affected. Depending on how this is accessed, this tab may not be available on each Schedule Job window.
<b>Notification</b>	Contains settings and selections for who, when, and why notifications are sent while the job is processing
<b>Data Fields</b>	Contains the Data Fields for this selected device

For a job to be scheduled, details on the Schedule Job tab must be completed. Details on the Tasks and Notification tabs need not be completed to submit the job.

## Scheduling a Run Time

Regardless of how the Schedule Job window is accessed, the method of scheduling jobs is exactly the same. All required fields must be populated. Any required fields not populated will generate errors.

For more information on the various settings, see [Using the Scheduler](#).

**Schedule Job**

**Schedule Job** | Tasks | Notification | Data Fields

**Job details**

\*Job Name:

Job owner: sysadmin

Job description:

\*Priority: Medium

**Schedule job**

Run in next maintenance window

Run upon approval

Run upon operator initiation

Run at scheduled date/time:       PM

Run as recurring series:

Hourly

Weekly

Monthly

**Start time:**       PM (GMT-06:00) America/Cr

**End Time**

Never Ends

Ends after  occurrences

Ends on this date/time       PM

**Interval**

Approve & Submit | Submit | Cancel

In the Job details section of the Schedule Job tab,

- 1 Enter the **Job Name** .
- 2 You can also enter a job **Description**.
- 3 From the **\*Priority** drop-down list, select a **Priority level** .

This level determines the execution priority of your job in the Device Server. For most jobs, select the Medium priority. (This is the default.) This will run on a normal schedule. For jobs such as Cut-Through, you should select High as the priority as this task is completed in real time and needs the highest priority. A Low priority can also be selected if you have numerous jobs to run.

Scheduling a job,

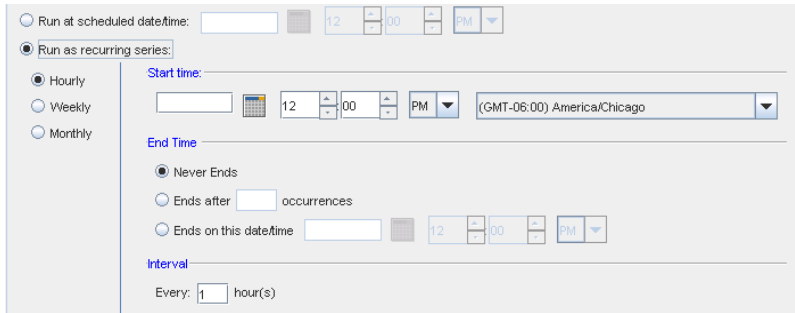
- 1 At the Schedule job section, by default, all jobs are scheduled to **Run upon approval** . All selections in the following example are displayed as being active in the schedule for viewing purposes only. With adequate permission, you can click the Submit button located at the bottom of the window.
- 2 Note that you can select to have the job **Run in the next maintenance** window.
- 3 If you select the **Run upon operator initiation** option, and Submit the job for approval, this keeps the job in a pending state after approval . After this, any user with Schedule permissions can then execute this job.
- 4 To set a specific time, select **Run at scheduled date/time** . The related date and time fields activate.
- 5 Enter a **date**. For assistance, use the Calendar icon to open a monthly calendar.
- 6 Select the time. The hour, minute, and AM/PM settings must be designated.
- 7 If this option is okay, click **Submit**.
- 8 To set a recurring schedule, select **Run as recurring series** . The recurring setting options activate.

---

**Important** When the **recurring schedule** is selected, the new time zone drop-down options are available. Make your selection from the drop-down options. The time zone you select must be the **client's time zone**. The new time zone field will be propagated with the client time zone automatically when creating a new Maintenance Window or recurring scheduled job.

---





9 Set the recurring options: Frequency, Start and End Times, and Time Interval.

10 If this option is okay, click **Submit**. The job is sent to the Schedule Manager and the Schedule Job window closes.

The **Cancel** button takes you out of this window, and back to the previous window you opened.

To review the process of a job, see the [Schedule Manager Overview](#)

## Using the Schedule Tab

The Schedule Job tab is divided into two sections:

- Job Details
- Schedule Job

The following fields are available used when scheduling a job. Required fields are identified by an asterisk.

Job Details,

- Enter the **Job Name** . The job name is how you will refer to the job in the job history. The Job Owner is System generated from the user creating the job.
- enter a **Job Description** . Add any comments in this area for outlining job significance and additional details that other users would find helpful during a review of job history and tasks.
- Select a **Priority Setting** . This allows the job to run ahead of other scheduled jobs, depending on the priority setting. Priority settings are: Low, Medium and High

Schedule Job,

---

**Note** The following graphic has been edited so that all options are active. When viewing the actual application, only the selected option is available.

---

The following fields are available used when scheduling a job. Required fields are identified by an asterisk.

Scheduling a job,

- 1 At the Schedule job section, by default, all jobs are scheduled to **Run upon approval** . All selections in the following example are displayed as being active in the schedule for viewing purposes only. With adequate permission, you can click the Submit button located at the bottom of the window.
- 2 Note that you can select to have the job **Run in the next maintenance** window.
- 3 If you select the **Run upon operator initiation** option, and Submit for approval, this keeps the job in a pending state after approval. After this, any user, with Schedule permissions, can then execute this job.
- 4 To set a specific time, select **Run at scheduled date/time** . The related date and time fields activate.
- 5 Enter a **date**. For assistance, use the Calendar icon to open a monthly calendar.
- 6 Select the time. The hour, minute and AM/PM setting must be designated.
- 7 If this option is okay, click **Submit**.
- 8 To set a recurring schedule, select **Run as recurring series** . The recurring setting options activate.
- 9 Set the recurring options: Frequency, Start and End Times, and Time Interval.

---

**Note** When the **recurring schedule** is selected, the new time zone drop-down options are available. Make your selection from the drop-down options. The time zone you select must be the **client's time zone**. The new time zone field will be propagated with the client time zone automatically when creating a new Maintenance Window or recurring scheduled job.

---

10 If this option is okay, click **Submit**. The job is sent to the Schedule Manager and the Schedule Job window closes.

The **Cancel** button takes you out of this window, and back to the previous window you opened.

## Reviewing Job Tasks

The Schedule Job Tasks tab allows you to review the job that is scheduled for **push or pull**. See: [Using the Scheduler](#).

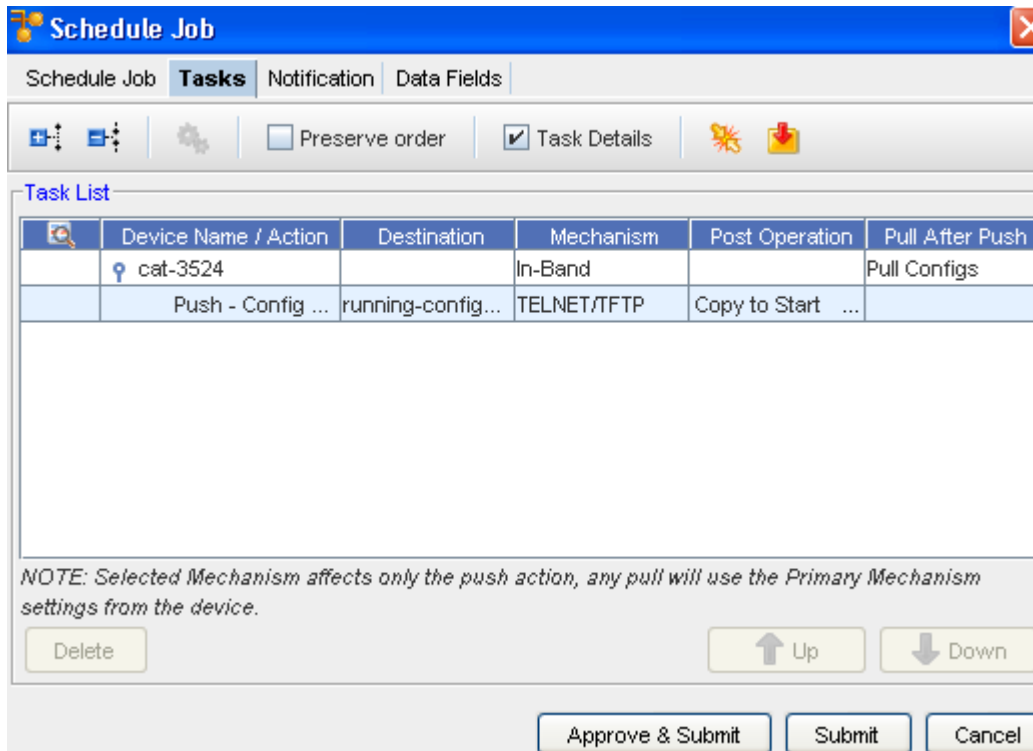
---

**Note** Depending on the module where the Schedule Job window is accessed, the Tasks tab may not be available.

---

The **Tasks tab** allows you to complete the following:

- Set a device order
- Designate a Run Type
- Identify Conflicting Scheduled Pushes or Pulls
- Insert a Command on-the-fly, into the content area of the scheduled job (Configlet, Config, Command or Interface)
- Complete a Modem Push
- Remove any Device from the Scheduled Update List



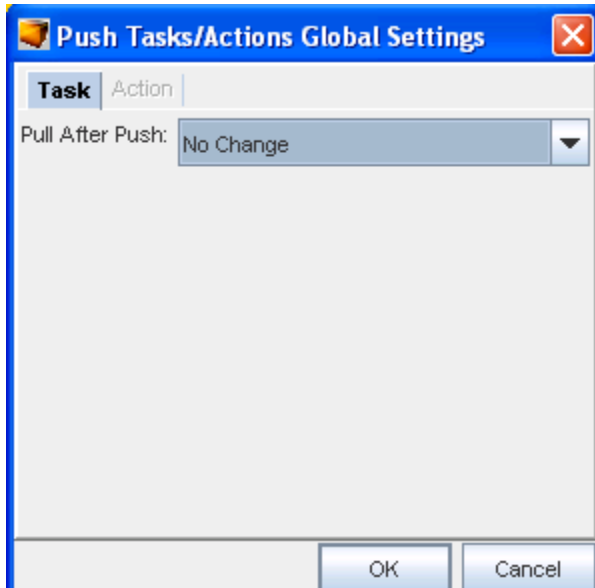
## Feature Toolbar

The first area of the Tasks tab is the toolbar. There are several actions that can be completed:

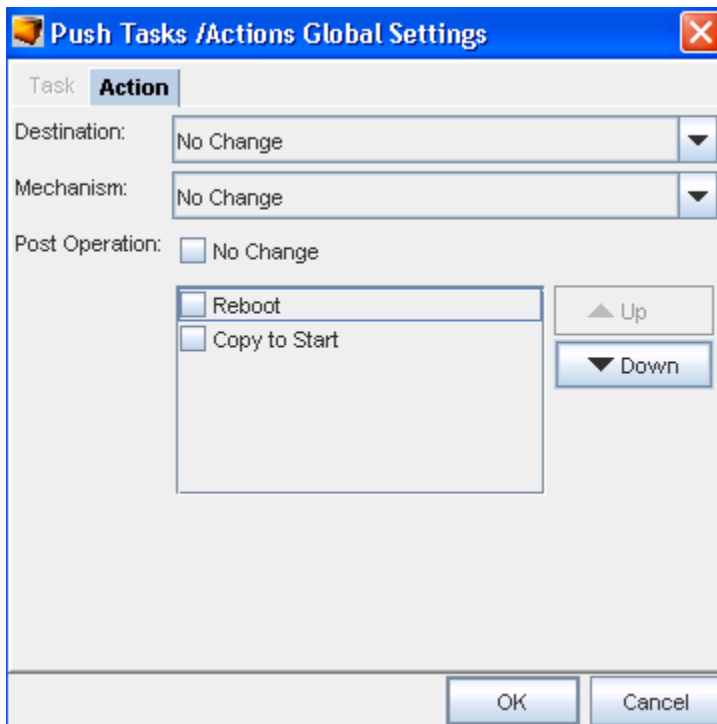
Icon	Description
	Expand the list
	Collapse the list
	Task/Action Global Setting
<input checked="" type="checkbox"/> Preserve order	Used to preserve the listed order
<input checked="" type="checkbox"/> Task Details	When a task is selected (under the Device Name) the task information is displayed. For example is this graphic the check box is checked and the details for that task ( <b>Config for running</b> ) are displayed.
	Prior to submitting any job, you can verify if there are any jobs that conflict with the job you are now scheduling
	Opens the Command Editor allowing you to create and insert a Command on-the-fly, into the scheduled job

## Content Area

The content area contains the body of the file being sent. This is the final opportunity, before push, that you are able to view the contents of the file being pushed.



When viewing the information contained within the Task tab, you can select the Global Settings icon and change the devices mechanism all at one time, rather than clicking each device listed, and changing the mechanism individually.

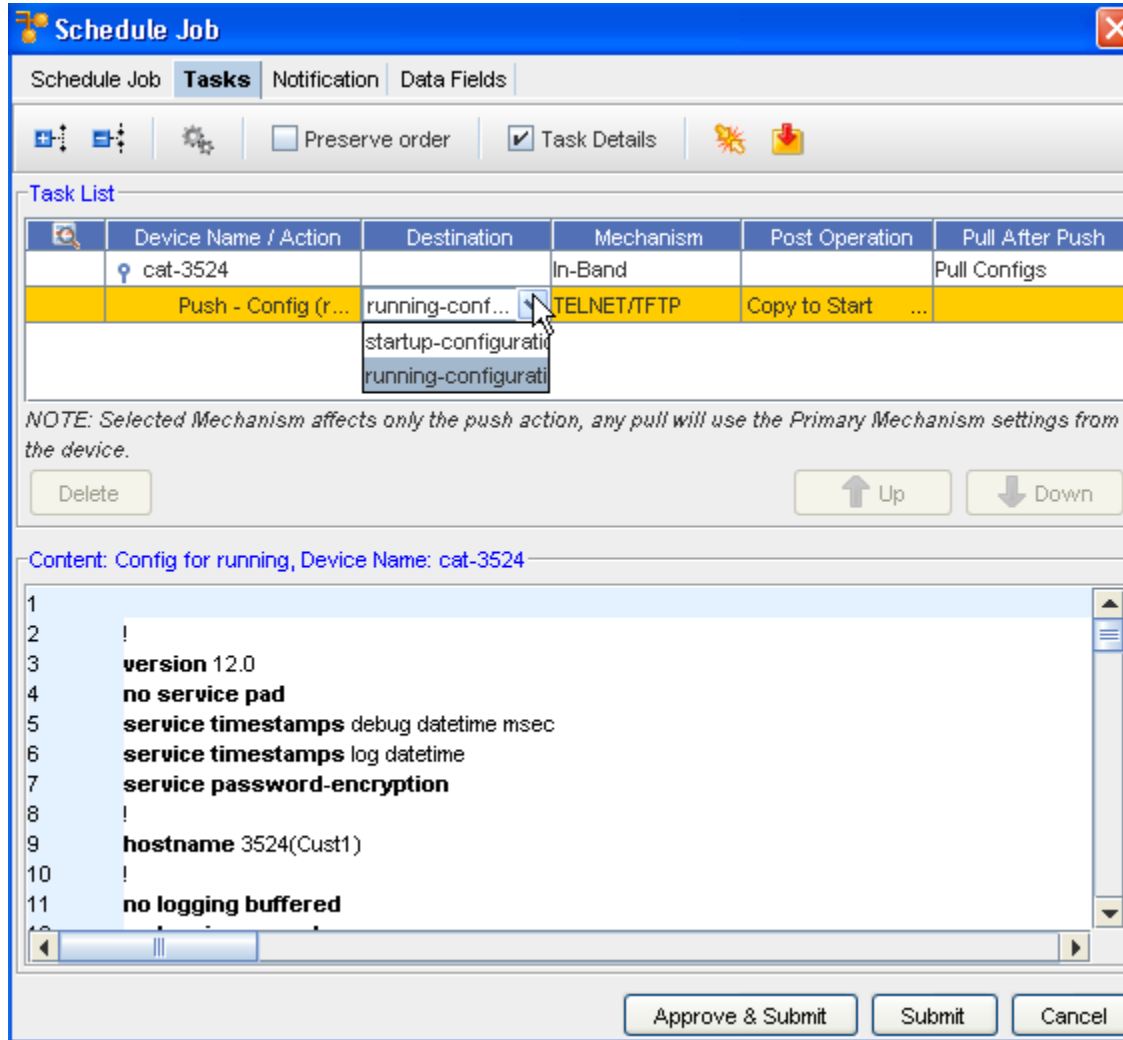


## Using the Task Tab



The Task tab details the actions that are scheduled for each device within a job. The listed devices can be moved to change the order in which each device receives its updates.



The **Tasks** tab on the Schedule Job window is divided into two sections:

- Task List with additional device information
- Content of the configuration for the running device



The first area of the Tasks tab is the toolbar. There are two actions that can be completed:

Icon	Description
	Expand or Collapse the list
	Task / Action Global Setting
<input checked="" type="checkbox"/> Preserve order	Preserve Order of the list
<input checked="" type="checkbox"/> Task Details	When a task is selected (under the Device Name) the task information is displayed. For example is this graphic the check box is checked and the details for that task ( <b>Config for running</b> ) are displayed.

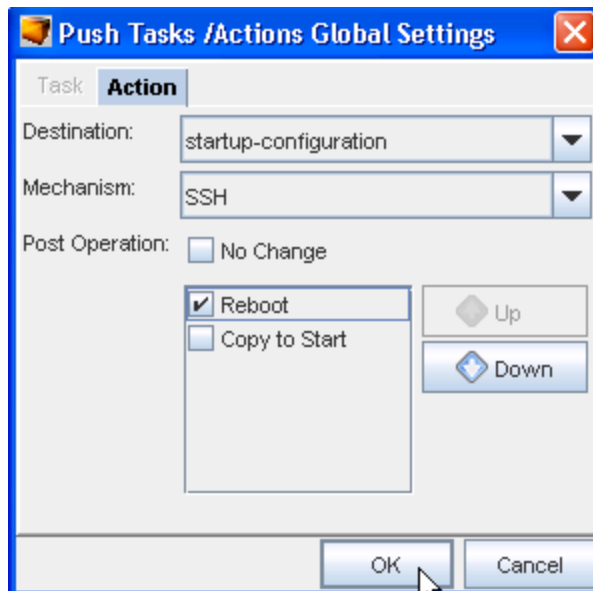
Icon	Description
	Prior to submitting any job, you can verify if there are any jobs that conflict with the job you are now scheduling.
	Opens the Command Editor allowing you to create and insert a Command on-the-fly, into the scheduled job

### Expand or Collapse

Use these icons to expand or collapse the task list.

### Task/Action Global Setting

When this is selected, the Push Task/Action Global Setting window opens, and allows you to make selections on Destination, Mechanism, and Post Operation settings.



### Preserve Order

Click this check box to preserve the order of the tasks list.

### Task Details

Click this check box to view additional details on the tasks.

### Conflict Resolution

- Before submitting a job, any job can be checked for Conflicts.
- A Conflict can occur if a previous job had been scheduled, but not yet executed for a device in the current job. Conflicts should be resolved before scheduling to ensure overwrites of changes do not occur.

### Commands

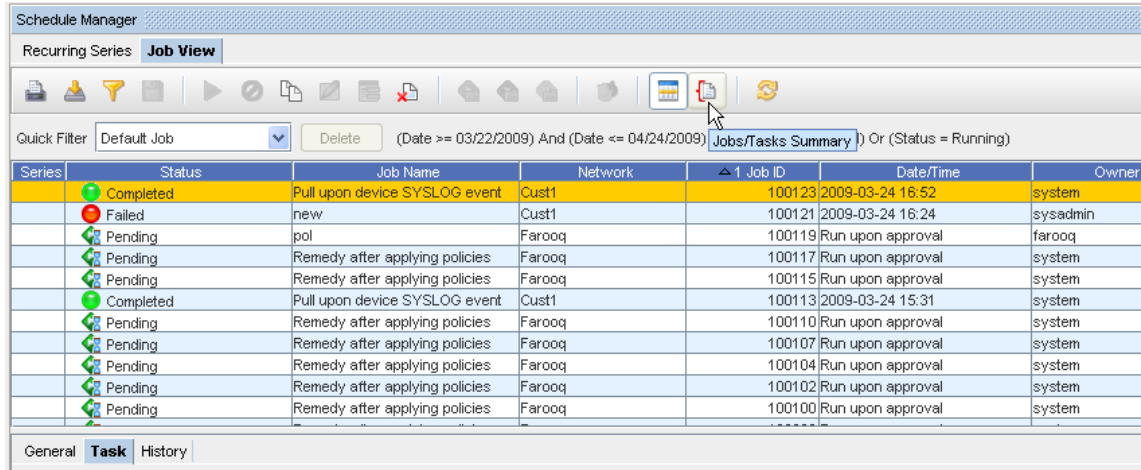
- Commands can be inserted into any scheduled job (via the Command Editor), and executed before or after configlet or config tasks.




- Commands help to validate the state of the device during job execution.
- The Command icon opens the Command Editor. Duplicate Commands are created for each device in the job.

## Reviewing Job/Status Summary

With the Schedule Manager displayed, you can select to review a Job/Status summary.



- 1 Select a **job** from the list, and then select the **Jobs/Tasks Summary**  icon.
- 2 The Job/Status summary information is presented in the left portion of the Schedule Manager window.
- 3 Click again on the Summary icon to close this Job/Summary window.

## Using the Notification Tab to Send an Email

The **Notification tab** allows you to select users or groups within your network, and users that are external to the application. You can then send email's regarding the state (status) of the job as it is processed. By default, all users and groups that have access to the Network are listed here. They do not receive email unless they are added to the Notification State column.

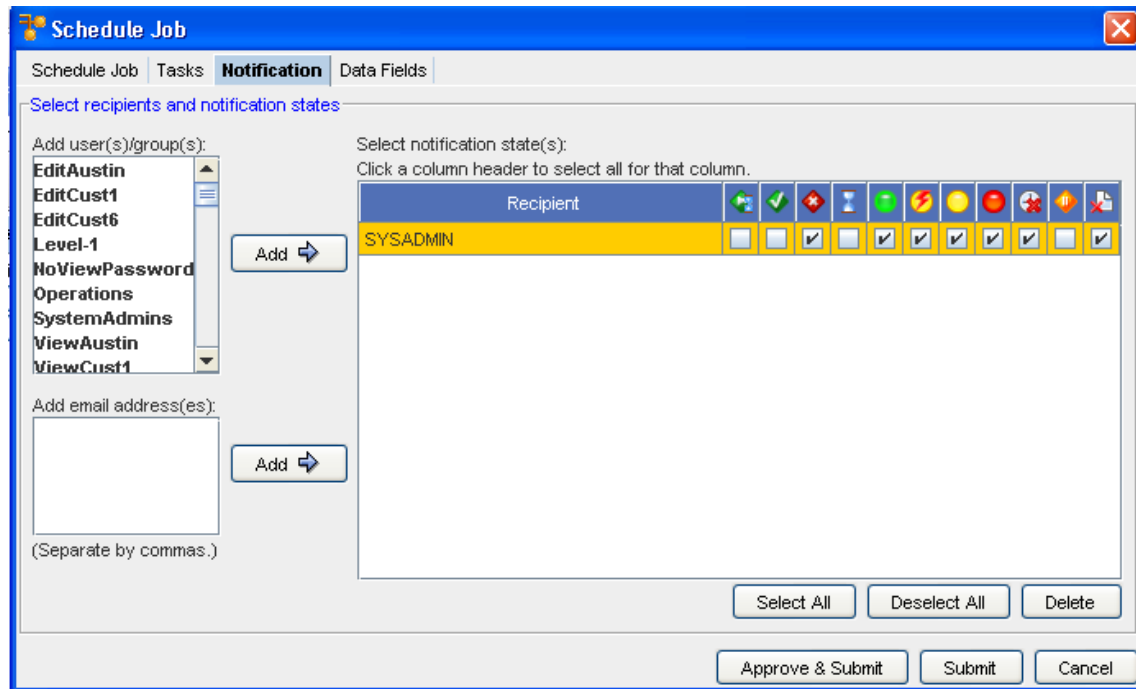
Any external email addresses can be added by entering names in the Add Email Address field, and adding these names to the Notification list.

---

**Important** You must add at least one email address to the Notification tab while scheduling a Report.

---

As jobs are being pushed to the network they have various states. Depending on the success of the push, the states (or status) the device goes through vary.



The Notification tab contains three sections.

- Add users/groups
- Add email Addresses
- Select Notification States

**Note** The Select All, De-select All, and Delete buttons can be used in the Notification States section to work with the list of recipients.

## Add users/groups

The Add user/group section allows you to select users or groups from all the available Network Configuration Manager users.

## Add email addresses

The Add email addresses section allows you to enter a comma delimited list of external user's email addresses.

## Notification States

When users are added (using one of the methods listed above) each job state is available for selection for each user. Depending on the user or group, the check boxes allow you to select notification status, based on the user or group's needs.

To send an email notification to users and/or groups,

- 1 On the Notification tab, select the **users** from the Add user/group column. Or if you are adding external email addresses, enter the email addresses in the Add email addresses text field. A comma ( , ) must be used to separate each email address.
- 2 In the Notification State section, select the **job states** for each user/group, for which an email will be sent. At the bottom of the window is the option to **Select All** job states. This option checks all the check boxes, for all the listed users/groups. Or, to reset all users/groups, click **Deselect All**.
- 3 When finished with the job details, click **Submit**. for the job to be submitted to the Schedule Manager. Or, if you have been granted adequate permissions, click **Approve & Submit**. The job will be scheduled to run based on the settings that were defined in the [Using the Scheduler](#).

## Working with the Event Manager

### Event Manager Overview

Due to the large number of events that may have transpired, the Event Manager may take a lengthy time to open. To enhance the opening of the Event Manager, you must periodically Archive and Purge the events. It is recommended that you archive all events that are older than 30 days, then purge these events. See the *Network Configuration Manager Installation Guides* for information on using the Archive and Purge Utility.

---

**Note** When viewing the Event Manager, keep in mind that it now **automatically refreshes** the view whenever new events occur.

---

The Event Manager feature allows you to view and manage **activities that have transpired** on the network. For example, you can access the log and view the Event, the Owner (or user), the Network that was accessed, the Date/Time the event was logged, and more!

---

**Important** You must have Network Administration or System Administration permission to access the Event Manager.

---

Events can be related to Device events, System events, and Security events.

This feature is designed to assist you in maintaining security, as well as auditing and following the activities of events and users.

### Accessing the Event Manager

You can access the Event Manager from the following system locations:

- From the menu bar, select **Tools**, then **Event Manager** .

Tools Window Help	
Networks Navigation	F6
Dashboard	F8
Automation Library	F3
Schedule Manager	F7
QS Inventory	F9
Event Manager	F11
Data Field Manager	
Metadata	F12
System Administration	F4
EMC M&R	
Change Audit	Ctrl-U
Global Device Search	Ctrl-S
Single Device Auto Discovery	
Template Merge	
Change Password	
Change RSA Tokens PIN	

- From the **Devices view**, select a device, then select **Properties**. The **General** tab contains access to the **Event Manager**.

The screenshot shows the 'Event Manager' window with the 'Device' tab selected. The window contains a toolbar with icons for print, refresh, filter, and search. Below the toolbar, there are settings for 'Page Size: 500' and a checked 'Auto Resize' option. The main area displays a table of events with the following columns: Date/Time, Event, Type, Owner, Network, Device Name, and Severity. The table contains 8 rows of event data.

Date/Time	Event	Type	Owner	Network	Device Name	Severity
12/02/2008 10:54 AM	Failed to Communica...	Device	system	Cust4	r2501-2	Warning
12/02/2008 10:54 AM	Task Run	System	system		r2501-2	Info
12/02/2008 10:54 AM	Job Run	System	sysadmin	Cust4		Info
12/02/2008 10:54 AM	Job Scheduled	System	sysadmin	Cust4		Info
12/02/2008 10:54 AM	Job Approved	System	sysadmin	Cust4		Info
12/02/2008 10:53 AM	Job Complete	System	system	Cust4		Info
12/02/2008 10:53 AM	Task Complete	System	system		r1605-1	Info
12/02/2008 10:53 AM	Device Pull	Device	system	Cust4	r1605-1	Info

Rows: 20 Page 1 of 1

More about Event Manager,

You can complete the following tasks within the Event Manager:

- Print
- Export
- Filter
- Refresh
- Select the columns you want displayed in the Event Manager. See [Displaying Columns](#) to review the list of columns available for you to display on each tab.

- Sort

---

**Note** If the Event Manager is accessed from Network Properties, only the events for that Network are displayed. If the Event Manager is accessed from the Device Properties, only the events for that Device are displayed.

---

- If an object (such as a network or a device) is deleted from the system, the event remains in the log.
- You can click within the **Auto Resize** check box to resize the width of the columns .
- To view more or less Events per page, select a number from the **Page Size** drop-down arrow. After selecting the pages you want to view, click **Refresh** to refresh the log screen. This page sizing allows you to maneuver between pages.
- The events that are logged are grouped into the following categories. You can select any one of these tabs when the Event Manager is displayed. Events differ for each category.
  - **All Events**
  - **System Events**
  - **Security Events**
  - **Device Events**

## All Events Log

When viewing the Event Manager, keep in mind that it now automatically refreshes the view when new events occur.

To view all the events from the Event Manager,



- 1 Access the **Event Manager** using one of the following methods:
  - From the **Tools** menu bar
  - From the **General** tab in Device Properties

Date/Time	Event	Type	Owner	Network	Device Name	Severity
12/02/2008 10:54 AM	Failed to Communicate...	Device	system	Cust4	r2501-2	Warning
12/02/2008 10:54 AM	Task Run	System	system		r2501-2	Info
12/02/2008 10:54 AM	Job Run	System	sysadmin	Cust4		Info
12/02/2008 10:54 AM	Job Scheduled	System	sysadmin	Cust4		Info
12/02/2008 10:54 AM	Job Approved	System	sysadmin	Cust4		Info
12/02/2008 10:53 AM	Job Complete	System	system	Cust4		Info
12/02/2008 10:53 AM	Task Complete	System	system		r1605-1	Info
12/02/2008 10:53 AM	Device Pull	Device	system	Cust4	r1605-1	Info

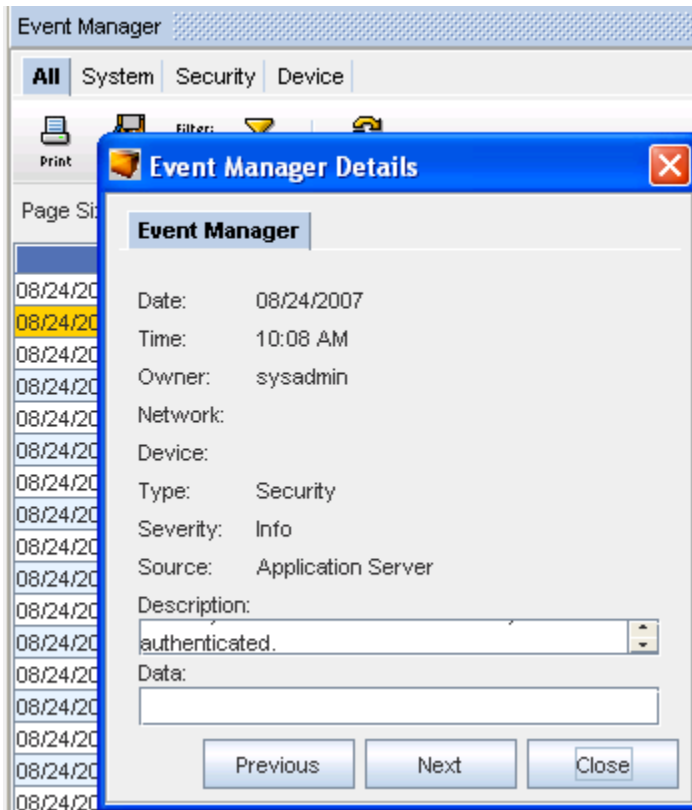
Page Size: 500  Auto Resize (Type = Device,Security,System) (Date/Time >= 11/30/2008)

Rows: 20 Page 1 of 1

**Important** To view more or less Events per page, select a number from the **Page Size** drop-down arrow.

- After selecting the pages you want to view, click **Refresh**  to refresh the log screen. This page sizing allows you to maneuver between pages.
  - There is also an **Auto Rest Settings**  when changes have been made to the settings.
  - You can also use the **Page box** at the bottom of the screen to go to any available page in the Events view.
- 2 With the **All** tab selected, you can view the information for all the events that have occurred, including System Events, Security Events, and Device Events. You can also select each tab to see the events specific to that tab.
  - 3 Double-click on any item in the **Event** column to display the event details. For example, by double-clicking on the User Log On event (from the above illustration), the following **Event Manager Details** window is displayed containing the event information. Click **Close** after viewing the event details.

**Important** From the Event Manager Details window, you can use the **Previous** and **Next** buttons to go through the listing of Events. Use **Close** when you are finished reviewing the event details.



- 4 You can [Printing Event Logs](#) or [Exporting Event Logs](#) the Event Manager by accessing the Print or Export icons. You can also [Refresh](#) the view, and click within the **Auto Resize** check box to resize the width of the columns.

## System Events Log

When viewing the Event Manager, keep in mind that it now automatically refreshes the view when new events occur.

To view System events from the Event Manager,

- 1 Access the **Event Manager** using one of the following methods:
  - From the **Tools** menu bar
  - From the **General** tab in Device Properties

Event Manager

All **System** Security Device

Page Size: 500  Auto Resize (Type = System) (Date/Time >= 11/30/2008)

Date/Time	Event	Owner	Network	Device Name	Severity
12/02/2008 10:55 AM	Job Failed	system	Cust4		Info
12/02/2008 10:55 AM	Task Failed	system		r2501-2	Info
12/02/2008 10:54 AM	Task Run	system		r2501-2	Info
12/02/2008 10:54 AM	Job Run	sysadmin	Cust4		Info
12/02/2008 10:54 AM	Job Scheduled	sysadmin	Cust4		Info
12/02/2008 10:54 AM	Job Approved	sysadmin	Cust4		Info
12/02/2008 10:53 AM	Job Complete	system	Cust4		Info
12/02/2008 10:53 AM	Task Complete	system		r1605-1	Info

Rows: 12 Page 1 of 1

- 2 With the **System** tab selected, you can view the information for all the System Events that have occurred. Notice that along with the Event, the event specifics are displayed, including Date/Time, Owner, Network, Device, and Severity. See [Displaying Columns](#) to review the list of columns available for you to display on each tab.

**Important** To view more or less Events per page, select a number from the **Page Size** drop-down arrow. After selecting the pages you want to view, click **Refresh** to refresh the log screen. This page sizing allows you to maneuver between pages.

You can also use the **Page box** at the bottom of the screen to go to any available page in the Events view.

#### The System tab includes the following System Events:

- Device Managed State Changed
- Device Server - Config Change Trap Received
- Device Server - Task Queued
- Device Server - Task Run
- Scheduler Events - Jobs Deleted/Jobs Held/Jobs Modified/Jobs Approved
- Scheduler Event - Jobs Run - both the job available and the job run time
- SNMP Trap Received
- Syslog Message Received



- Task Create from Workplace (such as push, synch)

**Important** You can [Printing Event Logs](#) or [Exporting Event Logs](#) the Event Manager by accessing the Print or Export icon. You can also [Refresh](#) the log view, and click within the **Auto Resize** check box to resize the width of the columns.

## Security Events Log

When viewing the Event Manager, keep in mind that it now automatically refreshes the view when new events occur.

To view Security events from the Event Manager Log,

- 1 Access the **Event Manager** using one of the following methods:
  - From the **Tools** menu bar
  - From the **General** tab in Device Properties

Date/Time	Event	Owner	Network	Device Name	Severity
12/02/2008 10:52 AM	View Access	sysadmin	Cust2		Info
12/02/2008 10:52 AM	View Access	sysadmin	Cust6		Info
12/02/2008 10:51 AM	View Access	sysadmin	RSA		Info
12/02/2008 10:49 AM	View Access	sysadmin	Cust5		Info
12/02/2008 10:49 AM	View Access	sysadmin	Cust4		Info
12/02/2008 10:15 AM	User Log On	sysadmin			Info

- 2 With the **Security** tab selected, you can view the information for all the Security Events that have occurred. Notice that along with the Event, the event specifics are displayed, including Date/Time, Owner, Network, Device, and Severity. See [Displaying Columns](#) to review the list of columns available for you to display on each tab.

**Important** To view more or less Events per page, select a number from the **Page Size** drop-down arrow. After selecting the pages you want to view, click **Refresh** to refresh the log screen. This page sizing allows you to maneuver between pages.

You can also use the **Page box** at the bottom of the screen to go to any available page in the Events view.

**The Security tab includes the following Security Events:**

- Any/all events that go through the Security Proxy
- Authentication Failures
- Auto Discovery Create/Modify
- Auto Discovery Delete
- Config File was Saved to File
- Credentials Create/Modify/Delete
- Device Create/Modify/Access
- Device Delete
- Device Server Create/Modify
- Exports/Imports from Automation Library
- Group Create/Modify
- Group Delete
- Network Create/Modify/Access
- Network Delete
- Policy Create/Modify
- Policy Delete
- Report Create/Modify
- Report Delete
- Run Cut-Through
- Run Proxy Access
- Run Quick Command
- Saved Command Create/Modify
- Saved Delete
- Site Create/Modify/Access
- Site Delete
- Standard Create/Modify/Delete
- Template Create/Modify/Delete
- Test Create/Modify
- Test Delete
- User Create/Modify/Delete
- User Not Authenticated

- User Lockout
- User Log On/Off
- User Login Expired
- View Create/Modify/Access
- Workspace Create/Modify/Access
- Workspace Delete

**Important** You can [Printing Event Logs](#) or [Exporting Event Logs](#) the Event Manager by accessing the Print or Export icon. You can also [Refresh](#) the log view, and click within the **Auto Resize** check box to resize the width of the columns.

## Device Events Log

When viewing the Event Manager, keep in mind that it now automatically refreshes the view when new events occur.

To view Device events from the Event Manager,

1 Access the **Event Manager** using one of the following methods:

- From the **Tools** menu bar
- From the **General** tab in Device Properties

Date/Time	Event	Owner	Network	Device Name	Severity
12/02/2008 10:55 AM	No New Revision After ...	system	Cust4	r2501-2	Warning
12/02/2008 10:55 AM	Communication to Devic...	system	Cust4	r2501-2	Info
12/02/2008 10:55 AM	No New Revision After ...	system	Cust4	r2501-2	Warning
12/02/2008 10:54 AM	Failed to Communicate ...	system	Cust4	r2501-2	Warning
12/02/2008 10:53 AM	Device Pull	system	Cust4	r1605-1	Info
12/02/2008 10:53 AM	No New Revision After ...	system	Cust4	r1605-1	Warning
12/02/2008 10:53 AM	No New Revision After ...	system	Cust4	r1605-1	Warning

Rows:7 Page 1 of 1

- 2 With the **Device** tab selected, you can view the information for all the Device events that have occurred . Notice that along with the Event, the event specifics are displayed, including Date/Time, Owner, Network, Device, and Severity. See [Displaying Columns](#) to review the list of columns available for you to display on each tab.

---

**Important** To view more or less Events per page, select a number from the **Page Size** drop-down arrow. After selecting the pages you want to view, click **Refresh** to refresh the log screen. This page sizing allows you to maneuver between pages.

---

You can also use the **Page box** at the bottom of the screen to go to any available page in the Events view.

### The Device tab includes the following Device Events:

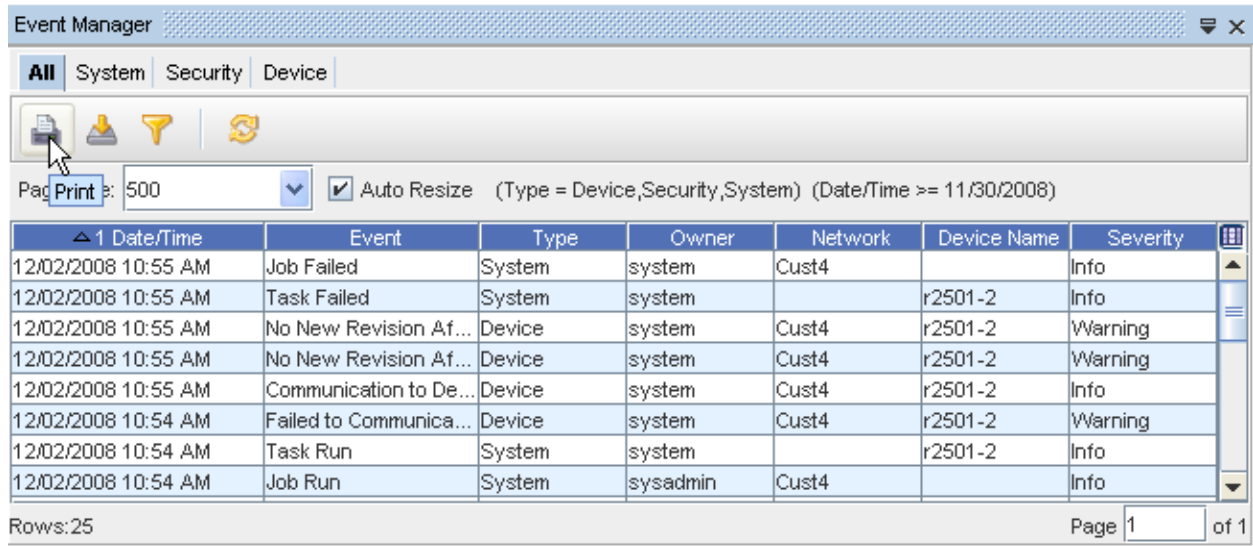
- Config File was Saved to File
- Credential Update
- Cut-Through Performed - descriptions include the keystroke log for the session
- Device Create
- Device Delete
- Device Managed State Changed
- Device Out-of-Sync - and return to sync
- Device Pull
- Device Revision Created (external reason)
- Device Revision Created (internal reason)
- Device Task Complete
- Hardware Pull
- New Configuration Revisions - all revision types
- OS Update Occurred
- Policy Check Failed
- Policy Failures
- Push Completed
- Run Compliance Check
- Run Cut-Through
- Run Quick Command
- Run Report
- SNMP Trap Received - description to include the Trap

- Syslog Message Received - description to include the message

**Important** You can [Printing Event Logs](#) or [Exporting Event Logs](#) the Event Manager Log by accessing the Print or Export icon. You can also [Refresh](#) the log view, and click within the **Auto Resize** check box to resize the width of the columns.

## Printing Event Logs

From the Event Manager window, you can access the icon to **Print** the log information.



The screenshot shows the Event Manager window with a toolbar containing icons for Print, Export, Filter, and Refresh. The 'Print' icon is highlighted. Below the toolbar, there is a 'Page Size' dropdown set to 500 and a checked 'Auto Resize' checkbox. The main area displays a table of event logs with columns for Date/Time, Event, Type, Owner, Network, Device Name, and Severity. The table contains 7 rows of data.

Date/Time	Event	Type	Owner	Network	Device Name	Severity
12/02/2008 10:55 AM	Job Failed	System	system	Cust4		Info
12/02/2008 10:55 AM	Task Failed	System	system		r2501-2	Info
12/02/2008 10:55 AM	No New Revision Af...	Device	system	Cust4	r2501-2	Warning
12/02/2008 10:55 AM	No New Revision Af...	Device	system	Cust4	r2501-2	Warning
12/02/2008 10:55 AM	Communication to De...	Device	system	Cust4	r2501-2	Info
12/02/2008 10:54 AM	Failed to Communica...	Device	system	Cust4	r2501-2	Warning
12/02/2008 10:54 AM	Task Run	System	system		r2501-2	Info
12/02/2008 10:54 AM	Job Run	System	sysadmin	Cust4		Info

Rows: 25 Page 1 of 1

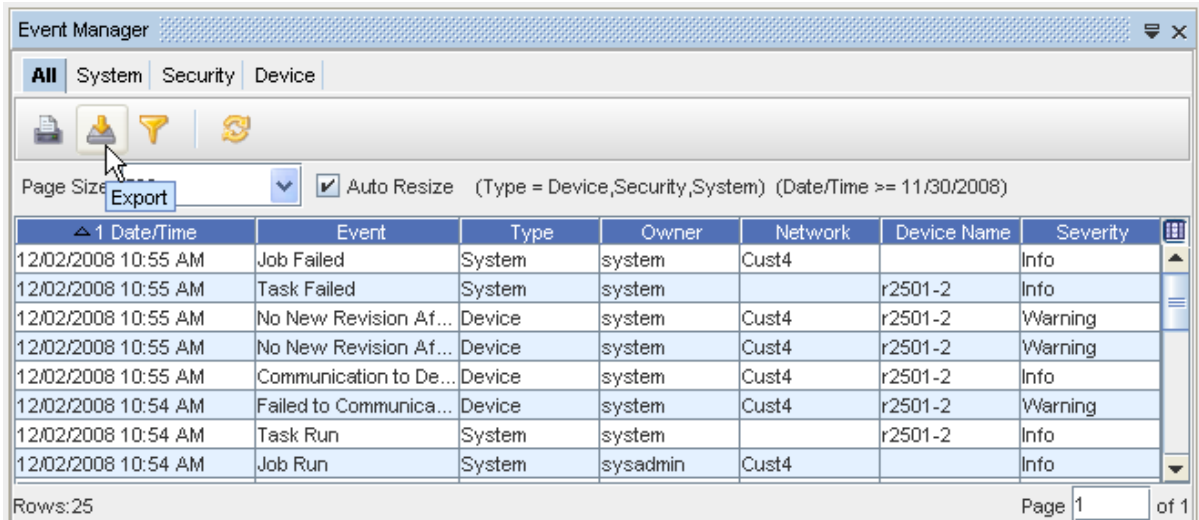
- 1 Access the Event Log, then select an **event** from the appropriate tab listing.
- 2 Click the **Print** icon to use your browser's print facility.

**Important** To view more or less Events per page, select a number from the **Page Size** drop-down arrow. After selecting the pages you want to view, click **Refresh** to refresh the log screen. This allows you to maneuver between pages.

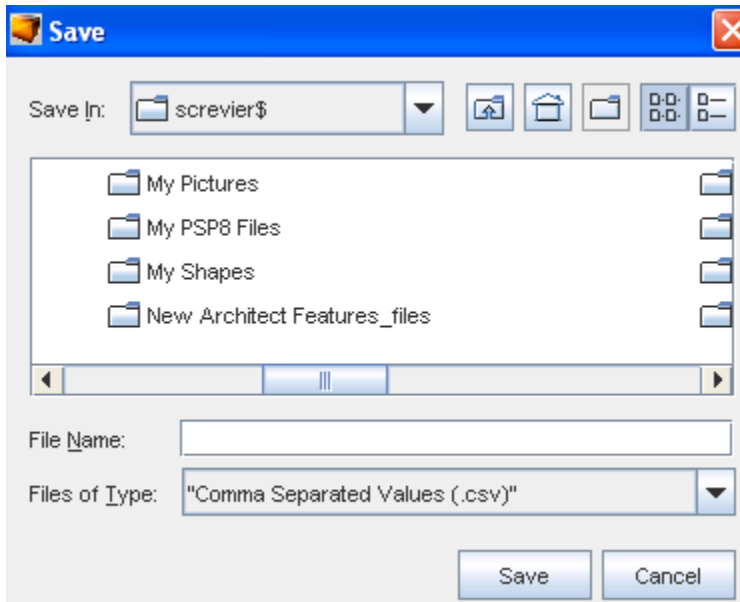
## Exporting Event Logs

From the Event Manager window, you can **Export** a copy of the log displayed.

- 1 With the Event Manager displayed, select an **Event** from the listing, then click the **Export** icon.



The Save window (from your own network) opens.



- Determine where you want to export a copy of the Event Manager to. This includes selecting a **Location**, entering a **File Name**, and selecting a **File Type**.
- Click **Save** after making your selections. Your copy of the Event Manager is now stored in the location you selected, with the file name and file type you also selected.

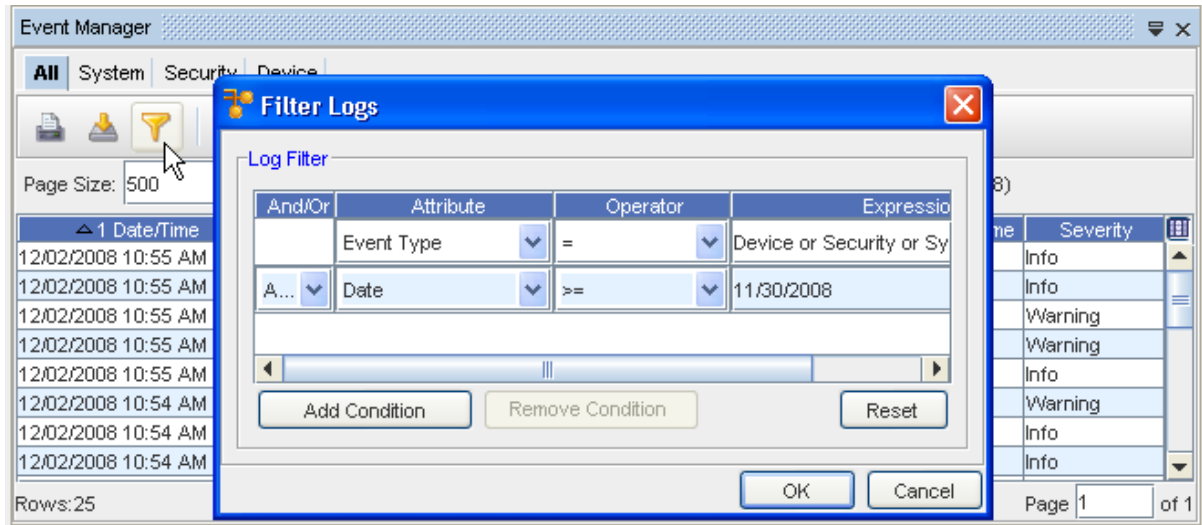
## Filtering the Event Manager Data

When viewing the Event Manager, keep in mind that it now automatically refreshes the view when new events occur.

- Click **Tools** on the menu bar, then select **Event Manager**.

Tools Window Help	
Networks Navigation	F6
Dashboard	F8
Automation Library	F3
Schedule Manager	F7
OS Inventory	F9
Event Manager	F11
Data Field Manager	
Metadata	F12
System Administration	F4
EMC M&R	
Change Audit	Ctrl-U
Global Device Search	Ctrl-S
Single Device Auto Discovery	
Template Merge	
Change Password	
Change RSA Tokens PIN	

2 At the Event Manager window, select the **Filter** icon.



- 3 Click **Add Condition** to select the And/Or, Attribute, Operator, and Expression filter options.
- 4 With the Filter Logs window displayed, make your filter selections.
- 5 Click **OK** when you have created your new conditions.

Note that the Attribute drop-down has included additional **Event Type** filtering selections. You can select from:

- Date
- Description

- Device ID
- Device Name
- Event
- Event Owner
- Network
- Service Name
- Severity
- Source

Note that the Operator drop-down has included additional filtering selections. You can select from the following.



- 6 If you need to start from the beginning and re-select conditions, click the **Reset** button to clear all the fields. Click **Ok** at the Reset confirmation message. After clearing the fields, click **Add Condition**.

---

**Important** You can remove any existing conditions by clicking the **Remove Condition** button. Use this feature on one or more of the existing conditions. You cannot however, remove the default conditions from the filter. These are default conditions for the Event Type and the condition changes, depending on which Event Type tab (All, System, Security or Device) is selected. Default conditions also exist for the Network and Device, and also cannot be removed from these filters.

---

- 7 When you view the Event Manager again, your data is filtered according to your selections.

**Attribute:**

**Operator:**

---

**Note** Filtering the log requires the same steps, regardless of what events (tabs) you are viewing (All, Security, System, or Device).

---

[Event Manager Overview](#)



# Using the Command Line Interface (Bulk Import)

## Using the Command Line Interface

Network Configuration Manager provides an alternative interface (to the user interface), allowing you to complete the following tasks, via the Command Line:

- Importing Credentials
- Importing Users
- Importing Groups
- Importing Sites
- Exporting Credentials
- Decrypting Credential Logs
- Setting the number of Devices
- Auto Discovery
- Importing Devices

The Command Line Interface allows you to use *command line operations* to import and export credentials, and to decrypt Credential Logs generated by password roll outs. It also allows you to import devices and Auto Discover devices.

---

**Note** When using the Command Line Interface (Bulk Import) tool, use the following jar file:

---

```
/usr/jboss/jboss-4.0.2/server/vc-server/deploy/vc.ear  
-rw-rw---- 1 jboss vc 2684634 Feb 23 11:12 voyence.jar
```

### Important Variables Information!

To begin using the Bulk commands, and to set the **\$VOYENCE\_HOME** variable, you must first enter the following command:

```
./etc/voyence.conf
```

After you have entered the above command, you can then use the **\$VOYENCE\_HOME** variable.

### Security Permissions

Ensure you have the following permissions to successfully complete any Command Line Interface tasks.

- To work with *Global credentials*, you must have **System Administrator** security access.

- **Systems Administration functions:** are intended for access by any user that has been given VoyencControl system administrator, network administrator, or user administrator privileges. The system administrator can create or delete networks, manage device servers and devices, create and edit system users, and create authorization policies between users, groups, and networks. System Administrators can see and alter information about any network in the VoyencControl application.
- To work with *Network credentials* , you must have **System Administrator, Network Administrator, and View Device Passwords on Devices** security access.

**Network Administration functions:** are limited to those networks to which you are assigned, or that you create. Network Administrators cannot see or manage any networks that they do not have specific permissions to access; manage users, groups, and network authorizations; or edit system global information.

## Important Syntax Information - for Global Credentials

You must include the syntax **global: in each credential name.**

For example, if you have 2 global credentials, you must use the **global:** for each c\_name. Such as, **global: c\_credentialname1, global: c\_credentialname2.**

## Available Commands

The following is a listing of the available Command Line Interface commands. If you need to review this list from the actual command line, enter **help**, then press **Enter**, and the list displays showing the syntax needed for each of the commands.

```
importCredentials [snmpv3] <scope> <credFile> <update>
exportCredentials [snmpv3] <scope>
seedAD <network name> <device server name> <Discovery type> hostfile <credentials>
importDevices <network name> <device server name> devicesCSVFile <updateFlag>
decryptCredentials <credentialsRollOutLogFileName> <outputFileName>
importUsers inputfile
importGroups inputfile
importSites <network name> inputfile
quit
help <cmd name>
```

## Creating Command Files

To work with these commands, you must first ensure that specific files needed to process these commands have been created. For example, to successfully complete **Importing Credentials** , you must have the **<credFile>** file created to enter the **credFile name** within the syntax of the command.

## Creating a credFile

The following is an example of **credFile content** used to import credentials using the importCredentials command.

```
#CREDENTIAL_NAME,CREDENTIAL_TYPE,COMMUNITY_STRING:RO,COMMUNITY_STRING:RW,ACCOUNT:USERNAME,ACCOUNT:PASSWORD,ACCOUNT:EXTERNAL AUTHENTICATION,ACCOUNT:PRIVILEGE_CREDENTIAL,PRIVILEGE:PASSWORD,UNIQUE,LENGTH,SECURE(PrivPassOnly)
```

#CREDENTIAL_NAME	CREDENTIAL_TYPE	COMMUNITY_STRING:RO	COMMUNITY_STRING:RW	ACCOUNT:USERNAME	ACCOUNT:PASSWORD	ACCOUNT:EXTERNAL AUTHENTICATION	ACCOUNT:PRIVILEGE_CREDENTIAL	PRIVILEGE:PASSWORD	UNIQUE	LENGTH	SECURE(PrivPassOnly)
AdminPP	Privilege							admin	N		Y
CiscoPP	Privilege							cisco	N		Y
AdminAcct	Account			admin	admin	N			N		
CiscoAcct	Account			cisco	cisco	N			N		
MSP-CS	Community	MSP	MSP-RW						N		
AUniqueAccount	Account								Y	10	

## Credfiles Rules

Following is a sample of the information from the various columns (shown in the csv file), that must be provided, based on the credential type. **Column 1** (Credential Name), and **Column 2** (Credential Type) are **mandatory**.

Credential Type	Mandatory Column Names
Privilege	<ul style="list-style-type: none"> <li>■ PRIVILEGE:PASSWORD</li> <li>■ UNIQUE</li> <li>■ SECURE(PrivPassOnly)</li> </ul>
Account	<ul style="list-style-type: none"> <li>■ ACCOUNT:USERNAME</li> <li>■ ACCOUNT:PASSWORD</li> <li>■ ACCOUNT:EXTERNAL AUTHENTICATION</li> <li>■ ACCOUNT:PRIVILEGE_CREDENTIAL</li> </ul> <p>If there is an Associated Privilege Credential, add the following:</p> <ul style="list-style-type: none"> <li>■ PRIVILEGE:PASSWORD</li> <li>■ UNIQUE</li> </ul>

SNMP v1/v2c	<ul style="list-style-type: none"> <li>■ COMMUNITY_STRING:RO</li> <li>■ COMMUNITY_STRING:RW</li> <li>■ UNIQUE</li> </ul>
SNMP v3	<ul style="list-style-type: none"> <li>■ SNMPV3:UserName</li> <li>■ SNMPV3:Security Level 1 -&gt; NoAuthNoPriv 2-&gt; AuthNoPriv 3 -&gt; AuthPriv</li> <li>■ SNMPV3:Authentication Protocol 1 -&gt; NONE 2-&gt; MD5 3 - SHA</li> <li>■ SNMPV3:Privacy Protocol none = 1, des = 2, idea = 9, aes128 = 19, aes192 = 20, aes256 = 21</li> <li>■ SNMPV3:Authentication Password Only needed for AuthNoPriv and AuthPriv security levels</li> <li>■ SNMPV3:Privacy Password Only needed for AuthPriv security level</li> </ul> <p>These parameters are not mandatory</p> <ul style="list-style-type: none"> <li>■ SNMPV3:Context Name</li> <li>■ SNMPV3:Engine Id</li> <li>■ SNMPV3:Group</li> <li>■ SNMPV3:View</li> <li>■ SNMPV3:ViewAccess 1 -&gt; Read Access 2 - Write Access</li> <li>■ SNMPV3:IncMibs - Separate the individual mibs using ""</li> <li>■ SNMPV3:ExcMibs - Separate the individual mibs using ""</li> </ul> <p>Following is an example:</p> <pre>#CREDENTIAL_NAME,SNMPV3:UserName,SNMPV3:SecLevel,SNMPV3:AuthProt,SNMPV3:PrivProt, SNMPV3:AuthPasswd,SNMPV3:PrivPasswd,SNMPV3:CtxName,SNMPV3:EngineId,SNMPV3:Group, SNMPV3:View,SNMPV3:ViewAccess,SNMPV3:IncMibs,SNMPV3:ExcMibs,UNIQUE, LENGTH cnv3-1,test123username,3,2,2,test123,test123,test123Ctx,test123EngineId,test123Group,test123,2, intenet*mib2,internet, N,</pre> <p>Note: Length is the length of the unique credential that is generated by the application.</p>

### Creating a hostfile

You must also ensure the **<hostfile>** file is created to complete both the **Auto Discovery** and **Importing Devices** tasks.

### Creating a SeedAD file <hostfile>

The following is an example of **seedAD content** used for Auto Discovery.

```
172.18.0.1 r3640-1.internal.powerupnetworks.com r3640-1
172.18.0.2 r3640-2.internal.powerupnetworks.com r3640-2
172.18.0.3 r3640-3.internal.powerupnetworks.com r3640-3
```

**Note** This is very similar to the **/etc/hosts file....**

### Examples of files

Examples of the Command Line Interface commands can be found in **examples.tar** in the **\$VOYENCE\_HOME /tools/bulk-import** directory. ( **./etc/voyence.conf**)

The examples.tar contains the following sample files:

- createCred.csv - sample file used in importCredentials command

- hosts - sample file used in seedAD command
- importDevices.csv - sample file used in importDevices command
- exportedCredentials.csv - sample output of exportCredentials command

## Accessing the Command Line Interface

- 1 SSH to the application server machine.
- 2 Enter **cd** to change the directory to **\$VOYENCE\_HOME/tools/bulk-import**, and press **Enter**.
- 3 At the command prompt, enter **runCmd.sh**, then press **Enter**.

---

**Important** For Windows, enter **runCmd.pl**, then press Enter.

---

- At the next command prompt, enter your **User Name** and **Password**. See the following prompts:
- **Enter User Name:** where you then enter the user name
- **Enter Password:** where you enter the password
- After entering the User Name and Password, press **Enter**.

---

**Note** This is the same User Name and Password you use to access the VoyencControl application. The Command Line Interface feature is now started by displaying a command prompt **cmd>**.

---

To work with the Command Line Interface functions, determine the task you want to complete, then go to:

- [Setting the Number of Devices](#)
- [Importing Credentials](#)
- [Importing Users](#)
- [Importing Groups](#)
- [Importing Sites](#)
- [Exporting Credentials](#)
- [Decrypting Credentials Log](#)
- [Auto Discovery](#)
- [Importing Devices](#)

## Setting the Number of Devices

You can set the number of devices you want to work with using the Command Line Interface feature.

## Accessing the Command Line Interface

- SSH to the application server machine.
- Enter `cd` to change the directory to `$VOYENCE_HOME/tools/bulk-import`, and press **Enter**.
- At the command prompt, enter `runCmd.sh`, then press **Enter**.
- At the next command prompt, enter your **User Name** and **Password**. See the following prompts:
  - **Enter User Name:** where you enter the user name.
  - **Enter Password:** where you enter the password.
- After entering the User Name and Password, press **Enter**.

---

**Note** This is the same User Name and Password you use to access the Network Configuration Manager application. The Command Line Interface feature is now started by displaying a command prompt `cmd>`.

---

### Determining the Number of Devices (per Transaction)

You can change the number (the value) of devices that can be handled during a single transaction.

- 1 First, you must access the `runCmd.sh` file. (See steps 1 through 3 in **Accessing the Command Line Interface** procedures detailed above.)
- 2 Determine if your system has a high load of activity during the Importing process. If so, you should tailor the number of devices you want to import accordingly.
- 3 Change the number in the `-DdevicesPerTransaction=1000` parameter, to the number of devices you want to import.

---

**Important** The default is currently set for **1000**, meaning that one transaction completes for a maximum of 1,000 devices. You can set the parameter for any number you choose. For example, if you change the number in `-DdevicesPerTransaction=5000`, the system accepts this 5000 number. However, the transaction is completed on only 1000 devices at one time. You would then actually have 5 transactions completed. The transactions **always take place for 1000 devices at one time**, but completes as many times as needed to meet the number of devices you entered in the parameter.

---

## Importing Credentials

Use the Command Line Interface feature to **Import Credentials**.

To import credentials (except for SNMPv3),

- 1 Go to [Using the Command Line Interface](#) if you have not already done so. At the command line, you must enter the command to `import credentials`. For example: `importCredentials [snmpv3] <scope> <credFile> <update>`

- Now, enter the appropriate command to **import** credentials. Make sure the format and syntax is **exactly** as shown in the following example.

```
<cmd> importCredentials global credentials.csv false
```

#### NOTES:

<scope> can be one of the following:

- global - which is the exact string
- Network name - which is the same network name in Network Configuration Manager

If the **network name** contains any spaces or other special characters, you must enclose the name using double quotes ( "). For example, if the network name is Network A, then the network name would appear as "**Network A**".

If the **file name** contains special characters (including slashes and spaces) the file name must be enclosed within double quotes. For example, if the file name is Creds/new, then the file name would appear as "**Creds/New**".csv.

The input file names should be quoted only if the file name has special characters - this applies to various commands.

---

**Note** You must enter the Credential Name or the Device Name using double quotes inside the file. The different values need only to be separated by a comma.

---

<Update> can be one of the following:

- false - to create new credentials
- true - to update existing credentials

- Press **Enter**. The credential file provides the details in the following comma-separated values (csv) format.

```
CREDENTIAL_NAME,CREDENTIAL_TYPE,COMMUNITY_STRING:RO,COMMUNITY_STRING:RW
,ACCOUNT:USERNAME,ACCOUNT:PASSWORD,ACCOUNT:EXTERNAL AUTHENTICATION,
ACCOUNT:PRIVILEGE_CREDENTIAL,PRIVILEGE:PASSWORD,UNIQUE,LENGTH,SECURE(priv.
pass only)
```

Here is the **output** you will see on executing this command:

```
Creating Community String:CS
```

```
Creating Account:Acct-1
```

```
Creating Privilege Password:PrivPass
```

- 4 In a separate telnet window, verify your command results entering change directory ( **cd** ) to **\$VOYENCE\_HOME /logs**, then pressing **Enter**. The log file to review is **commandLineUtil.log**. You can also go to the System Administrator **Credential** screen (in Network Configuration Manager) to verify that the credentials have been imported.
- 5 If you have completed importing credentials, and no further actions are needed, enter **quit** at the command line, then press **Enter**. You are now logged off of Network Configuration Manager.

### To import SNMPV3 credentials

- 1 Go to [Using the Command Line Interface](#) if you have not already done so. At the command line, you must enter the command to *import credentials*. For example:  
importCredentials[snmpv3]<scope> <credFile> <update>
- 2 Now, enter the appropriate command to **import** credentials. Make sure the format and syntax is **exactly** as shown in the following example.

```
cmd > importCredentials snmpv3 global credentials.csv false
```

#### NOTES:

<scope> can be one of the following:

- global - which is the exact string
- Network name - which is the same network name in Network Configuration Manager

If the **network name** contains any spaces or other special characters, you must enclose the name using double quotes ( " ). For example, if the network name is Network A, then the network name would appear as "**Network A**".

If the **file name** contains special characters (including slashes and spaces) the file name must be enclosed within double quotes. For example, if the file name is Creds/new, then the file name would appear as "**Creds/New**".csv.

#### Important Information!:

- You must enter the Credential Name or the Device Name using double quotes inside the file. The different values need only to be separated by a comma.
- To import SNMPv3 credentials, this must be specified in the command. For example,

```
importCredentials snmpv3 global credentials.csv false
```

- SNMPv3 Credentials are imported using their own csv, and are not available as a part of the existing csv. This is because the SNMPv3 Credentials have a large set of parameters.

<Update> can be one of the following:

- false - to create new credentials
- true - to update existing credentials

Press **Enter**. The credential file provides the details in the following comma-separated values (csv) format. **Example:**



Format of v3 csv (not mibs need to be separated by delimiter '\*' ):

```
#CREDENTIAL_NAME,SNMPV3:UserName,SNMPV3:SecLevel,SNMPV3:AuthProt,SNMPV3:PrivProt,
SNMPV3:AuthPasswd,SNMPV3:PrivPasswd,SNMPV3:CtxName,SNMPV3:EngineId,
SNMPV3:Group,SNMPV3:View,SNMPV3:ViewAccess,SNMPV3:IncMibs,SNMPV3:ExcMibs,
UNIQUE,LENGTH
testuser2,testuser,3,2,2,testuser,testuser,Test,Test,View,Group,2,abc*internet*internet,
,N,privuser3,privuser,3,2,2,privuser,privuser,null,null,null,null,3,,,N,
testuser,testuser,3,2,2,testuser,testuser,,,GroupName,ViewName,2,
internet*internet,,N,
```

- 3 In a separate telnet window, verify your command results entering change directory ( **cd** ) to **\$VOYENCE\_HOME /logs**, then pressing **Enter**. The log file to review is **commandLineUtil.log**. You can also go to the System Administrator **Credential** screen (in Network Configuration Manager) to verify that the credentials have been imported.
- 4 If you have completed importing credentials, and no further actions are needed, enter **quit** at the command line, then press **Enter**. You are now logged off of Network Configuration Manager.

## Importing Users

Use the Command Line Interface feature to **Import Users** .

To import Users,

- 1 Go to [Using the Command Line Interface](#) if you have not already done so. At the command line, you must enter the command to *import users*. For example: importUsers inputfile
- 2 Now, enter the appropriate command to **import** Users. Make sure the format and syntax is **exactly** as shown in the following example.

```
cmd > importUsers inputfile
```

Notes:

- The input file names should be quoted only if the file name has special characters - this applies to various commands.
- First Parameter: **inputFile** It is a comma separated file. The table below describes a sample content.
- The \* indicates this is a mandatory field and must be completed.
- Notice groups and subgroups have the syntax shown in row1 and row 2. The subgroup is delimited by a % character.

- The groups are assumed to be present in Network Configuration Manager when assigning users to it. They are be created as a part of this command.

Please use the horizontal scroll bar to view all the columns within the table.

*#User Name	First Name	Last Name	*Email Address	Phone	*Authentication_Type	*User_Password
GUEST	guestname		guest@voyence.com	5555555555	DB_AUTHENTICATION	Guest
admin	adminuser	adminuser	admin@voyence.com	5555555555	RADIUS_AUTHENTICATION	Admin
user	user		user@voyence.com		DB_AUTHENTICATION	user
adminldap			adminldap@voyence.com		LDAP_AUTHENTICATION	
admintacacs			admintacacs@voyence.com		TACACS_AUTHENTICATION	

**\*User Password** is Required for DB\_AUTHENTICATION and RADIUS\_AUTHENTICATION Types of authentication. In the case of Radius, this field is treaded as the radius realm name.

In case of errors, the logs to be inspected are **commandLineUtil.log** and **bulkuser.log** in directory **INSTALLATION\_DIR/logs**.

### Sample File Content for Import Users

```
#USER_NAME,FIRST_NAME,LAST_NAME,EMAIL_ADDRESS,PHONE,AUTHENTICATION_TYPE,
USER_PASSWORD,LOCK,GROUPS%GROUPS
GUEST,guestname,,guest@voyence.com,1298654575,DB_AUTHENTICATION,guest,1,Everyone
admin,adminuser,adminuser,admin@voyence.com,42343244343,RADIUS_AUTHENTICATION,
admin,0,EveryOne%Qualityuser,user,,user@voyence.com,,DB_AUTHENTICATION,user,0,
Everyone%Managementadminldap,,,adminldap@voyence.com,,
LDAP_AUTHENTICATION,,1,Everyone%Quality
```

### Importing Groups

Use the Command Line Interface feature to **Import Groups** .

To import Groups,

- 1 Go to [Using the Command Line Interface](#) if you have not already done so. At the command line, you must enter the command to *import groups*. For example: `importGroups inputfile`
- 2 Now, enter the appropriate command to **import** Groups. Make sure the format and syntax is **exactly** as shown in the following example.

```
cmd > importGroups inputfile
```

**Notes:**

- The input file names should be quoted only if the file name has special characters - this applies to various commands.
- First Parameter: **inputFile** – It is a comma separated file. The table below describes a sample content.
- The \* indicates this is a mandatory field and must be completed.
- You can create a group under a group (a subgroup) by using the syntax shown in row 3 of the sample below. Use the 3rd column to define the containing group or the hierarchy by using a % sign between each level of group.

*GROUP_NAME	GROUP_DESCRIPTION	GROUPS#GROUPS
Quality	Quality	
Management	Management	
Sales	All Sales	Quality%NoGroup
Marketing	Marketing	Quality%Management
Everyone		Management

In case of errors, the logs to be inspected are **commandLineUtil.log** and **bulkgroup.log** in directory **INSTALLATION\_DIR/logs**.

### Sample File Content for Import Groups

GROUP\_NAME,GROUP\_DESCRIPTION,GROUPS#GROUPS

Quality,Quality

Management,Management

Sales,All Sales,Quality%NoGroup

Marketing,Marketing,Quality%Management

Everyone,,Management

### Importing Sites

Use the Command Line Interface feature to **Import Sites** .

To import Sites,

- 1 Go to [Using the Command Line Interface](#) if you have not already done so. At the command line, you must enter the command to *import sites*. For example: `importSites <network name> inputfile`
- 2 Now, enter the appropriate command to **import** Sites. Make sure the format and syntax is **exactly** as shown in the following example.

**cmd >importSites <network name> inputfile**

Notes:

- First parameter: **<network name>** is a valid network name already existing in VoyencControl NG. If the **network name** contains any spaces or other special characters, you must enclose the name using double quotes ( "). For example, if the network name is Network A, then the network name would appear as **"Network A"**.
- The input file names should be quoted only if the file name has special characters - this applies to various commands.
- Second Parameter : **inputfile** is a comma separated file. The following table describes sample content.
- The first two columns (designated with an \*) are mandatory.
- The third example below, shows a way to create a sub-site. If you already had a site named Site A, you can add sub sites using this syntax SiteA%SiteB, where SiteB is the sub-site

\*Use the horizontal scroll bar to view all the columns within the table.

SITE_NAMES	SITE_TYPES	SITE_DESCRIPTION	CONTACT_NAME	CONTACT_PHONE	CONTACT_EMAIL	ADDRESS1	ADDRESS2
TestGeo	Geographic	VC Created This	VC	972-759-4000	info@vc.com	1801	N.
SiteA	Building	VC Created This	VC	972-759-4000	info@vc.com	Glenville	
SiteA%SiteB	Room	Building Site	VC	972-759-4000		1801	N.
		VC Created This				Glenville	
		Building Site					
SiteA%SiteB%SiteC	Rack	VC Created This	VC	972-759-4000	info@vc.com	1801	N.
		Building Site				Glenville	

In case of errors, the logs to be inspected are **commandLineUtil.log** and **bulksite.log** in directory **INSTALLATION\_DIR/logs**.

**Sample File Content for Import Sites**

SITE\_NAME,SITE\_TYPE,SITE\_DESCRIPTION,CONTACT\_NAME,CONTACT\_PHONE,  
CONTACT\_EMAIL,ADDRESS1,ADDRESS2,CITY,STATE,ZIP,COUNTRY

TestGeo,Geographic,VC Created This,VC,972-759-4000,,,,,,,,

SiteA,Building,VC Created This Building Site,VC,972-759-4000,info@vc.com,  
1801 N.Glenville St.,Richardson,TX,75081,USA

If you already had a site named Site A, you can add sub sites using this syntax:

SiteA%SiteB,Room,VC Created This Building Site,VC,972-759-4000,info@vc.com,  
1801 N.Glenville St.,Richardson,TX,75081,USA

SiteA%SiteB%SiteC,Rack,VC Created This Building Site,VC,972-759-4000,info@vc.com,1801 N.Glenville St.,Richardson,TX,75081,USA

### Additional Information:

When importing Sites, any **contact information** appears grayed out (not accessible). If you are loading contact information with your Sites, you must go into the application and manually click the **Override** button for those sites. This then allows you to select or change the contact information.

## Exporting Credentials

Use the Command Line Interface feature to **Export Credentials** .


To export credentials (except SNMPv3),

- 1 Go to [Using the Command Line Interface](#) if you have not already done so. At the command line, enter the command to **export** credentials. Here is the command you need to enter.

```
exportCredentials [snmpv3] <scope>
```

- 2 Make sure the format and syntax is **exactly** as shown in the following example.

```
cmd > exportCredentials global
```

 When entering this command, <scope> can be either:

- global
  - network name. If the **network name** contains any spaces or other special characters, you must enclose the name using double quotes ("). For example, if the network name is Network A, then the network name would appear as "**Network A**".
  - The input file names should be quoted only if the file name has got special characters - this applies to various commands. (only Export Credentials cmd have a file name parameter).
- 3 Press **Enter**. The **global.csv** is now written in the directory (\$VOYENCE\_HOME/tools/bulk-import). If the network name is used as scope, a (networkname.csv) is created.
  - 4 In a separate telnet window, verify your command results by entering change directory (**cd**) to **\$VOYENCE\_HOME/logs**, then pressing **Enter**. The log file to review is **commandLineUtil.log**. You can also go to the System Administrator **Credential** screen (in Network Configuration Manager) to verify that the credentials seen here have been exported.
  - 5 If you have completed exporting credentials, and no further actions are needed, enter **quit** at the command line, then press **Enter**. You are now logged off of Network Configuration Manager.


To export SNMPv3 credentials,

- 1 Go to [Using the Command Line Interface](#) if you have not already done so. At the command line, enter the command to **export** credentials. Here is the command you need to enter.

```
exportCredentials [snmpv3]<scope>
```

- 2 Make sure the format and syntax is **exactly** as shown in the following example.

```
cmd > exportCredentials snmpv3 global
```

 When entering this command, <scope> can be either:

- global
  - network name. If the **network name** contains any spaces or other special characters, you must enclose the name using double quotes ("). For example, if the network name is Network A, then the network name would appear as "**Network A**".
- 3 Press **Enter**. The **snmpv3 global.csv** is now written in the directory (\$VOYENCE\_HOME/tools/bulk-import). If the network name is used as scope, a (networkname-snmpv3.csv) is created.
  - 4 In a separate telnet window, verify your command results by entering change directory (cd) to **\$VOYENCE\_HOME /logs**, then pressing **Enter**. The log file to review is **commandLineUtil.log**. You can also go to the System Administrator **Credential** screen (in Network Configuration Manager) to verify that the credentials seen here have been exported.
  - 5 If you have completed exporting credentials, and no further actions are needed, enter **quit** at the command line, then press **Enter**. You are now logged off of Network Configuration Manager.

## Auto Discovery

Use the Command Line Interface feature to **seed Auto Discovery** .

To complete command line Auto Discovery,

- 1 Go to [Using the Command Line Interface](#) if you have not already done so.
- 2 Here is the *auto discovery* Command you need to enter: seedAD <network name> <device server name> <Discovery type> hostfile <credentials>
- 3 Make sure the format and syntax is **exactly** as shown in the following example.

```
cmd > seedAD Cust-1 devserver1 ping-sweep hosts "global:Acct-1,ppwd"
```

### NOTES:

- **Discovery type** can be one of the following:
  - ping-sweep
  - snmp-sweep
- **Hostfile** is a tab separated format, similar to **/etc/hosts**. See **examples.tar** in the **\$VOYENCE\_HOME/tools/bulk-import** directory to see examples.
- **Credentials** can be either global/network credentials.
  - global - global credentials have a **global:** prefix.

- Network - network credentials are those that belong to the network provided in the command

If the credential names (in **either global or network** ) contains any spaces or other special characters, you must enclose the name using double quotes ( "). For example, if the global name is **global: cred name , cred name2** , then the name would be entered as:

**"global:cred name,cred name2"**.

- 4 Press **Enter**.

Here is the **output** you will see on executing this command: Added the CS:MSP-CSto AD

Added the Account:Account 1to AD

\*\*\*\*\*AD Entry Details\*\*\*\*\*

NameAUTODISC-CMDLINE-Tue Sep 28 11:32:20 CDT 2004

Account Identities[Account 1]

CS Identities[MSP-CS]

\*\*\*\*\*AD Entry Details\*\*\*\*\*

- 5 In a separate telnet window, verify your command results by entering change directory ( **cd** ) to **\$VOYENCE\_HOME/logs**, then pressing **Enter**. The log file review is **commandLineUtil.log**. You can also go to the System Administrator screens (in Network Configuration Manager) to verify Auto Discovery.
- 6 If you have completed command line auto discovery and no further actions are needed, enter **quit** at the command line, then press **Enter**. You are now logged off of Network Configuration Manager.

## Importing Devices

Use the Command Line feature to **Import Devices** .

See [Setting the Number of Devices](#) before you begin this task.

To import devices,

- 1 Go to [Using the Command Line Interface](#) if you have not already done so.
- 2 Here is the *import devices command* format you need to enter. importDevices <network name> <device server name> devicesCSVFile <updateFlag>
- 3 Make sure the format and syntax is entered at the **cmd >** prompt, **exactly** as shown in the example.

```
cmd> importDevices Network1 DeviceServer1 devices.csv false
```

The input file names should be quoted only if the file name contains special characters - this applies to various commands.

---

**Note** You do not have to enter the Credential Name or the Device Name using double quotes inside the file. The different values need only to be separated by a comma.

---

NOTES:

- **hostfile** names
- The hostfile format is the following:

(Single-Level Mode)

```
#IP Address, HostName, DeviceAlias, DevicePkg, InMech, InAcct, In-Snmp, In-CTMech, InCutCre, OOBMech, OOBCre, OOBCTMec, OOBCTCre, OOBDS, OOBP, PP Field, PP Field, PP Field, PP Field
```

```
172.18.20.3, Test1-Device1, TestAliasName, 1, SNMP / TFTP, global:Cisco-Account, global:Cust1, Telnet, global:Cisco-Account, global:r2511, global:Cisco-Account, global:rlocal, global:Cisco-Account, 972, 1112, PPIBP:global:ciscop, PPIBC:global:level14, PPOBP:global:level11, PPOBC:global:level12, SNMPV2:global:Cust1, SNMPV3:global:testuser, SNMPPORT:162, ACTIVESNMPVERSI  
ON:v1
```

Notice PP information has been added after the 15th column and has to be qualified with either (in Normal Mode : 4 new entries):

```
[PPIBP|PPIBC|PPOBP|PPOBC]::<global/network>:<pp cred>
```

---

**Note** Privilege Password values.

---

The last 4 fields in the CSV are for Priv Pass credentials. They each require a prefix to define which Priv Pass you are setting. The prefixes are:

- "PPIBP:" aka. Priv Pass In-Band Primary management
- "PPIBC:" aka. Priv Pass In-Band Cut-thru
- "PPOBP:" aka. Priv Pass Out-of-Band Primary management
- "PPOBC:" aka. Priv Pass Out-of-Band Cut-thru

**(Multi-Level Mode)** - (requires each priv pass to be appended with @<level> : up to 15 new privlevel entries)

```
#IPAddress, HostName, DeviceAlias, DevicePkg, InMech, InAcct, In-Snmp, In-CTMech, InCutCre, OOBMech, OOBCre, OOBCTMec, OOBCTCre, OOBDS, OOBP, PP Field, PP Field, PP Field, PP Field
```



```
172.18.20.3,Test1-Device1,TestAliasName,1,SNMP / TFTP,global:Cisco-
Account,global:Cust1,Telnet,global:Cisco-Account,global:r2511,global:Cisco-
Account,global:rlocal,global:Cisco-
Account,972,1112,PPLEV:global:ciscop@15,PPLEV:global:level14@14,PPLEV:global:level11@11,PP
LEV:global:level12@11,
SNMPV2:global:Cust1,SNMPV3:global:testuser,SNMPPORT:162,ACTIVESNMPVERSI
ON:v1
```

**Notice format : PPLEV:<global>:<ppcred>@<level>**

**Note:** For SNMPv3 Credentials there is no change in command but the .csv format should indicate v2 ,v3 ,snmpport , snmpactiveversion params with qualifiers in the above example. These parameters must be added to the end of the .csv record for the specific device.

- These field names are mandatory in the input deviceCSVfile.
- IP Address
- HostName
- DevicePkg
- A combination of ip address and hostname is used to check for uniqueness.
- All the field names can be updated except "Hostname" as it is the key in the CSV data input file for updates.
- The remaining are optional. These include, InMech,InAcct,In-Snmp,In-CTMech,InCutCre,OOBMech,OOBCre,OOBCTMec,OOBCTCre,OOBDS,OOBP
- UpdateFlag
- false - to create new devices
- true - to update existing credentials

What each column represents:

Valid Package Numbers are:

- 4 Press **Enter**.
- 5 In a separate telnet window, verify your command results by entering change directory (cd) to **\$VOYENCE\_HOME /logs**, then pressing **Enter**. The log file to review is **commandLineUtil.log**. You can also go to the System Administration screens (in Network Configuration Manager) to verify that the devices have been imported.
- 6 If you have completed importing devices, and no further actions are needed, enter **quit** at the command line, then press **Enter**. You are now logged off of Network Configuration Manager.

Column Number	Field Name	Required/ Optional	Valid Values
1	<b>IP Address</b> - The IP Address of the Device	Required	

2	<b>HostName</b> - The Hostname of the Device	Required	
3	<b>DeviceAlias</b> - The Device Alias name	Optional	
4	<b>DevicePkg</b> - The name of the Device Package	Required	Valid Package Number
5	<b>InMech</b> - The In-Band Management Mechanism (Telnet/SSH for example)	Optional	SNMP/TFTP, TELNET, SSH, TELNET/TFTP, SSH/SCP
6	<b>InAcct</b> - The In-Band Account Credential name	Optional	Valid Account Name
7	<b>In-Snmp</b> - The In-Band SNMP Credential name	Optional	Valid SNMP Credential Name
8	<b>In-CTMech</b> - The In-Band Cut-Through Mechanism (Telnet/SSH for example)-	Optional	SSH, TELNET
9	<b>In-CutCre</b> - The In-Band Cut-Through Credential name	Optional	Valid Account Credential
10	<b>OOBMECH</b> - The Out-of-Band Management Mechanism	Optional	Out-of-Band Server Name
11	<b>OOB CRED</b> - The Out-of-Band Management Credential	Optional	Valid Account Credential
12	<b>OOBCTMec</b> - The Out-of-Band Cut-Through Mechanism name	Optional	Out-of-Band Server Name
13	<b>OOBCTCRre</b> - The Out-of-Band Cut-Through Credential name	Optional	Valid Account Credential
14	<b>OOBDS</b> - The Out-of-Band Dial String name	Optional	Any String
15	<b>OOBP</b> - The Out-of-Band Port name	Optional	Number
16	<b>PP Field</b> In-band Management	Optional	Privilege Password Name
17	PP Field – In-band cut-thro - Privilege Password field In-Band Cut-thro	Optional	Privilege Password Name
18	PP Field – OOB Mgmt - Privilege Password field Out-of-Band Management	Optional	Privilege Password Name
19	<b>PP Field – OOB</b> Cut-thro - Privilege Password Filed - Out-of-Band Cut-through	Optional	Privilege Password Name

Package ID	Package Name
1220	3Comm NetBuilder II
19	Adtran NetVanta
18	Adtran NetVanta Switch
1007	Airespace Wireless Switch
14	Alcatel OmniCore 5000

45	Nortel Alteon
42	Nortel Router
25	Aruba Wireless Switch
40	Nortel Baystack
41	Nortel BPS2000
15	Cisco Aironet AP
16	Cisco Aironet AP CXWorks
17	Cisco Aironet Bridge
2	Cisco CATOS Switch
1004	Cisco Content Switch
24	Cisco ISO Layer 3 Switch
1	Cisco ISO Router
2	Cisco IOS Switch
4	Cisco Lightstream ATM Switch
10	Cisco PIX
11	Cisco VPN Concentrator 3000
1000	Checkpoint Firewall
1203	Ericsson MSED
13	Extreme Switch
1006	F5 Load Balancer Rev
1001	F5 Load Balancer
1008	Foundry
2000	Generic Cisco REM Device

## Using the Extract Config script

Use the following script to extract the textual configuration of the device (or devices) within a Network, and write the textual configuration to a file (or files) on the file system.

- Use this command on Solaris and Linux: **`./extract_config.sh`**
- Use this command on Windows: **`extract_config.pl`**

## Valid Options

Option	Description of Option
network network_name	Name of the network from which the device configurations have to be extracted.
outputdir path_name	The directory into where the configs need to be extracted.
user user_name	Login user name (valid user name) used to log into Network Configuration Manager.
password user_password	Valid password to access Network Configuration Manager.
ext file_extension_name	File extension for each configuration file, for example, .txt.
debug	With this option, there will be more logs generated. It is useful for debugging purposes.

For Windows Only:

The extract\_config.pl utility in Windows 2003 does not work if there are spaces included in the folder name.

For example, you must use:

```
C:\Program Files\Network Configuration Manager\tools>extract_config.pl -network Cust1
-outputdir \"C:\Program Files\" -user xxxxx -password xxxxx -ext .txt
```

The output would then be:

- Devices found in network : **9**
- Devices without config files : **1**
- Devices captured successfully : **8**

## Working with the DNS Wizard

### Wizard Overview

Building on the concept of standardized templates, a Wizard delivers intelligent automation to configuration tasks. The DNS Wizard generates Cisco IOS 12.0 and above code.

The DNS Wizard is accessible by right-clicking a device, and selecting **Wizard** from the right-click menu.

Device Name	Device Class	Model
172.22.2.54	172.22.2.54	Business Policy S...
350t		BayStack 350-24T
Adtran1224	Compliance Audit	NetVanta 1224
ARN2-Lab	Enforce Policy	Nortel ARN
ASN-1-TelnetTF	Cut-Through	Nortel ASN
BIGGlon4Kay	Editor	B4000
bigip		Big-IP-HA
Cat1900-1	Edit Device	Catalyst 1900
Cisco3000-3	Pull	C3005 VPN Conce...
CiscoCSS1	Quick Commands	CSS 11050
Lab-470	Saved Commands	BayStack 470 - 48T
MILANsmnp801		MilanSME801P
netvanta3200	Save To...	NetVanta 3200
NetVanta3200-2	Update OS Image	NetVanta 3200
netvanta3205		NetVanta 3205
netvanta3305	Wizards	NetVanta 3305
Nortel 450	Navigations	BayStack 450-24T
Passport-8106		Passport 8106
ProCurve Switc	Compare Configs	J8692A ProCurve ...
r1841-1Test	Properties	1841

The **DNS** connection wizard is included in the release. See [The DNS Wizard Overview](#)

Although more than one device can be in the Selected Devices column when choosing which devices will be used in the Wizard, the Selected Devices column can **only have two devices listed** before being able to proceed to the **next step** of any Wizard. Since a Wizard is accessed by right-clicking on a selected device, the selected device(s) display in the Selected Device column when a Wizard is opened.

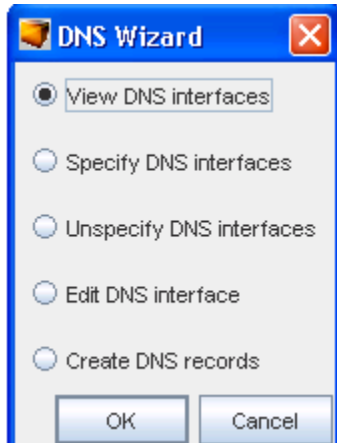
To move devices from one column to another, use the **Add** and **Remove** buttons. The selected devices can be moved back and forth between the columns until you have two devices to be used in the Wizard.

## The DNS Wizard Overview

**Note** Virtual Devices are not supported in the DNS Wizard.

The DNS wizard is used to generate **DNS records** that are sent to the DNS Administrator. Unlike the other wizards in Network Configuration Manager the DNS wizard allows you to select more than two devices. This is allowed because the focus is not the devices, but the **interface s on the devices**.

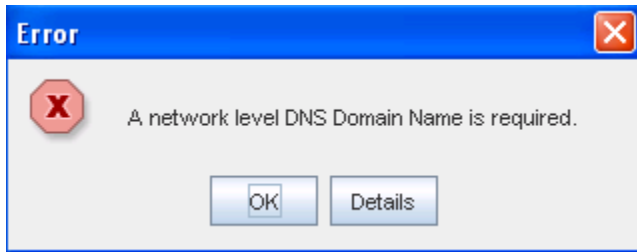
The following are functions used in the DNS Wizard.



DNS Wizard Functions	Description
View DNS Interfaces	Shows the DNS interfaces, IP addresses, and CNAME of interfaces currently specified for the device
Specify DNS Interfaces	Allows you to specify interfaces for selected devices for which DNS records are generated
Unspecify DNS Interfaces	Allows you to unspecify a specific DNS interface from a DNS
Edit DNS Interfaces	Allows you to edit the CNAME of the interface
Create DNS Records	Allows you to generate records that can be e-mailed to the DNS Administrator, or can be saved

### Important Information!

Before you can specify a DNS interface, the domain name must be set at the current network level. The following error displays if the domain name is not set for the network.



See [Setting the Domain name](#) for more information.

Once a domain name is set up, you can select an option, then click **OK** to access any of the functions.

## RSA

### About RSA

RSA, The Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. Ra information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance and access control, data loss prevention, encryption and key management, compliance and security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit [www.RSA.com](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).

# NETWORK ADMINISTRATORS - Getting Started

# 7

This chapter includes the following topics:

- Getting Started - Network Administrator Tasks
- Working with Networks
- Working with Network Settings
- Working with Change Audit
- Automation Library
- Working with Template Merging
- Working with OS Image Inventory Manager
- Managing Credentials
- Working with Update Credentials

## Getting Started - Network Administrator Tasks

The first task you may want to accomplish is creating a Network. As the **Network Administrator**, you have very specific tasks. These tasks may include (but are not limited to) the following:

- Working with Networks
  - Creating Networks
  - Associating Device Servers
- Working with Out-of-Band Service
- Working with Device Servers
- Working with Credentials and Credentials Configuration
- Working with Auto Discovery Manager
- Working with Maintenance Windows
- Working with Device Classes
- Working with Devices



- Working with IP Address Pools
- Working with NAT Configuration
- Working with Network RSA Token Viewer

Once you complete a Auto Discovery on devices, you can then complete other tasks.

To work with Users and Groups, you must have permission from the System Administrator.

## Working with Networks

### Networks Overview

Network configuration is the "backbone" of the tool. A properly configured network speeds productivity when sending changes to multiple devices on the network.

Networks are completely configurable by adding and removing devices. Regardless of the size of a network, the focus is on *ease of management*. Management of large networks is aided by the use of **Sites** and **Views**. Using these two features allows you to either create a hierarchical site construct, or to create user-defined views of specific devices.

By taking advantage of the access controls, you are able to dictate who and how networks are accessed. While the access to networks is provided by assigning users or groups to networks, further enhancements allow you to provide security at not only the network level, but the device level as well.

Network level permissions are setup in the **Access Control Administration** window. When users are created, they can be provided permissions to networks individually, where permissions are defined specific to the user, or assigned to a group, where the same permissions are granted for each user within the group.

When creating networks, you may want to use the following steps (in sequence):

- 1 Associate Device Servers
- 2 Schedule and Run Auto Discovery
- 3 Create Users and Groups
- 4 Set User/Group Permissions
- 5 Assign Users and Groups to Network
- 6 After Auto Discovery, Manage Devices to Networks
- 7 Set Network Credentials

Once you have completed these steps (in sequence), the network can be accessed by other users or groups.

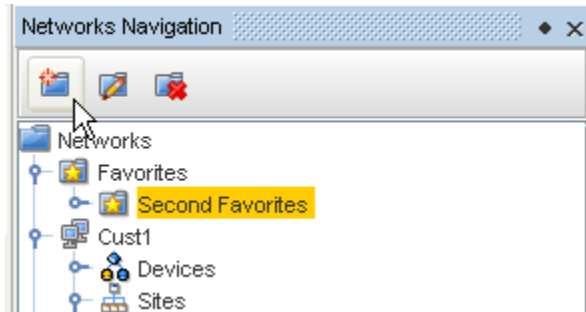
**The Network area** is where you:

- Manage networks

- Create auto discovery jobs
- Manage device level credentials and communications

### Managing Network Folders

From the Network Navigation view, you can use the icons to Add a New Folder to the Network, Edit an existing Folder Name, or Delete a Folder from the Network.

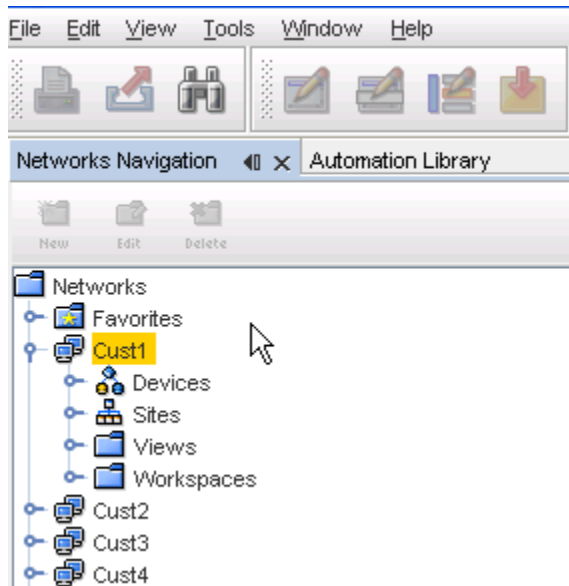


- Working with Networks
- Creating Networks
- About Network Properties
- The Dashboard
- Assigning Device Servers
- Scheduling Auto Discovery Jobs
- Creating Users
- Setting Network Level Permissions
- Auto Discovery Overview
- Setting Network Level Credentials

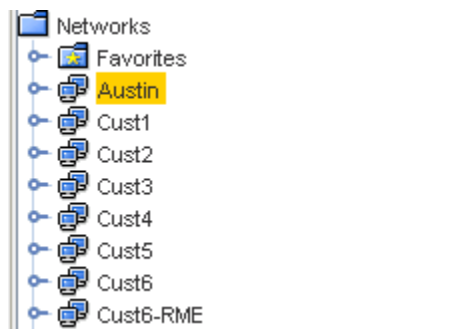
### Working with Networks

To work with Networks, you must first select **Networks Navigation** from **Tools** on the menu bar.

Once Networks Navigation is selected, your existing Networks are listed. For example, the Networks Cust1, Cust2, Cust3, and Cust4 are listed. Notice also that the Devices, Sites, Views, and Workspaces are also displayed. These options are offered for each Network.



Within Network Configuration Manager, a **Network** is defined as a logical partitioning of the devices that are in a physical network. A network is also often times referred to as a "container".



- Networks can be created to best model your business environment. For example, networks can be created and defined by customer, region, subsidiary, or responsibility; for example, corporate vs. division.
- Within networks, devices can be further organized logically and physically. In addition, you can design and stage modifications to the devices in user-defined workspaces.
- Networks, when created, contain basic information about the network (name, description and domain).
- The content of a network is determined by selecting devices that are housed on the devices servers. Once selected, these devices make up a network.
- Depending on the size of the network, Network Configuration Manager has included two interfaces for viewing a network; Table and Diagram layout.

A network is a container that groups the following:

Feature	Description
Devices	A specialized view that contains all network devices

<b>Sites</b>	A hierarchical structure that allows physical segmentation of devices. Sites are viewed and updated in the Site view of a network by authorized users only. Sites uses locations to reference the devices network organization. For example, geography, building, and rooms.
<b>Views</b>	A folder containing user-defined views. Views contain user-defined groupings of operational network devices
<b>Workspaces</b>	A folder containing user-defined workspaces. Workspaces are "sandboxes" for storing and staging device configuration changes, and can be used for design and complex changes

Extremely large networks, even when arranged in manageable sites, can become unmanageable. With this in mind, there are several filtering options that have been included that allow you to filter what is seen in the interface you are using and segmenting options (views and sites).

For information on creating new networks, see [Creating Networks](#).

**Note** Networks can only be created by users who have adequate permissions. If you are unable to create a network, contact your System Administrator.

- [About Network Properties](#)
- [Workspaces Overview](#)
- [How Sites and Views Work](#)
- [Favorites Overview](#)

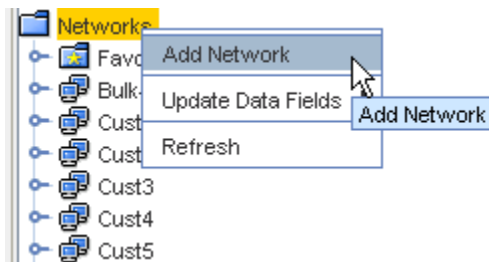
## Creating a New Network

Networks are created to hold devices. A network can contain a single Site, with an unlimited number of Views and Workspaces with any configuration.

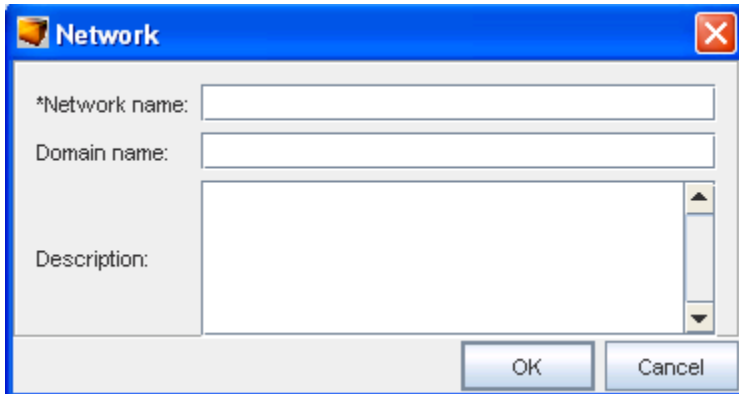
**Note** Sites, Views, and Workspaces are not required for your network, but are added to allow you to segment your network into manageable portions.

To create a Network,

- 1 At the navigation pane, right-click the **Networks** folder.
- 2 Select **Add Network** from the options .



The network window opens.



3 In the Network window, enter the following:

- Network Name
- Domain Name (optional)
- Description (optional)

4 Click **Ok**. Now, notice the new Network is now listed under Networks in the navigation pane.

Now that the Network is created, you can complete the following tasks:

- [Creating the Site Hierarchy](#)
- [Creating Views](#)
- [Creating Workspaces](#)

---

**Important** Use the **Refresh** option to refresh the network information when you have created or added information to the network.

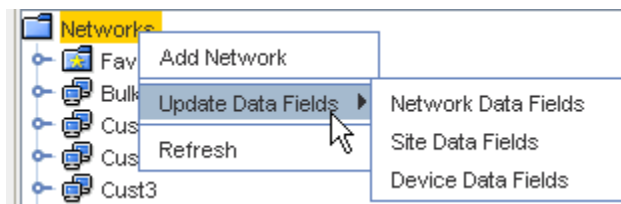
---

## Update Data Fields

From the Networks right-click options, you can select Update Data Fields to update the Network, Site or Device existing Data Fields.

**Note** Data Fields are used to create attributes, and to assign values to devices. You must **first** have added data fields to a Network, Site or Device before you can update them. For information on adding Data Fields, click [Adding a Data Field](#)

---



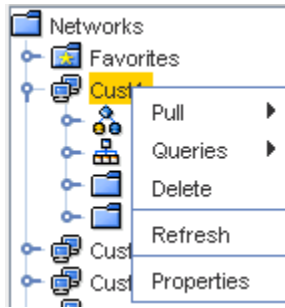
From this option, you can select to update the following:

- Network Data Fields

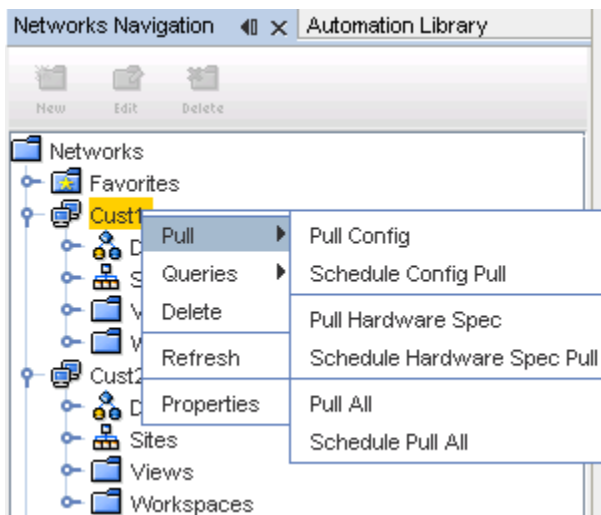
- Site Data Fields
- Device Data Fields

## Network Right-Click Options

When working with Networks, you can also complete other tasks having to do with the selected network. From the Network, right-click to view the options.



The first option is **Pull**, with additional options offered in a submenu.



For more information on using the **Pull** option, and the options related to Pull, access the following:

[Pull Config](#)

[Schedule Config Pull](#)

[Pull Hardware Spec](#)

[Schedule Hardware Spec Pull](#)

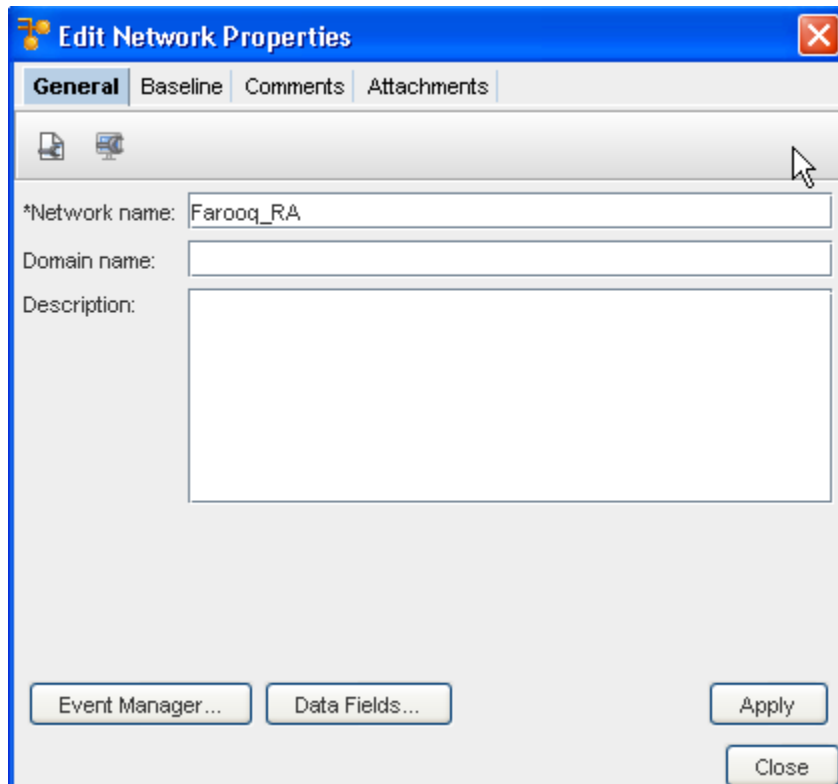
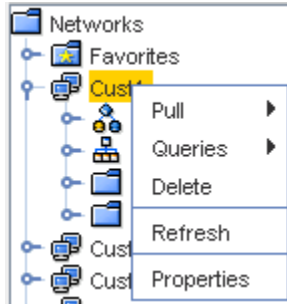
[Pull All](#)

[Schedule Pull All](#)

## About Network Properties

When networks are created, basic information about the network is entered. After creation, additional information can be entered.

- 1 View this information by selecting a **Network** from the Networks Navigation Pane.
- 2 Next, right-click on the Network name, and select **Properties**.



There are four tabs of information that can be entered regarding network **Properties**:

- The General Tab
- The Baseline Tab
- The Comments Tab
- The Attachments Tab

Additional options on the Edit Network **Properties General tab** include:

- **Event Manager** - when selected it takes you to the Event Manager feature

- **Data Fields** - click this to get the latest view including any recent changes
- **Apply** - click this to apply and save all your edit changes.

**Note** Clicking **Close** at the bottom of each window (while in any tab) closes the Edit Network Properties window. If you have information to be entered on more than one tab, click each tab and save according to the provided instructions.



## The General Tab

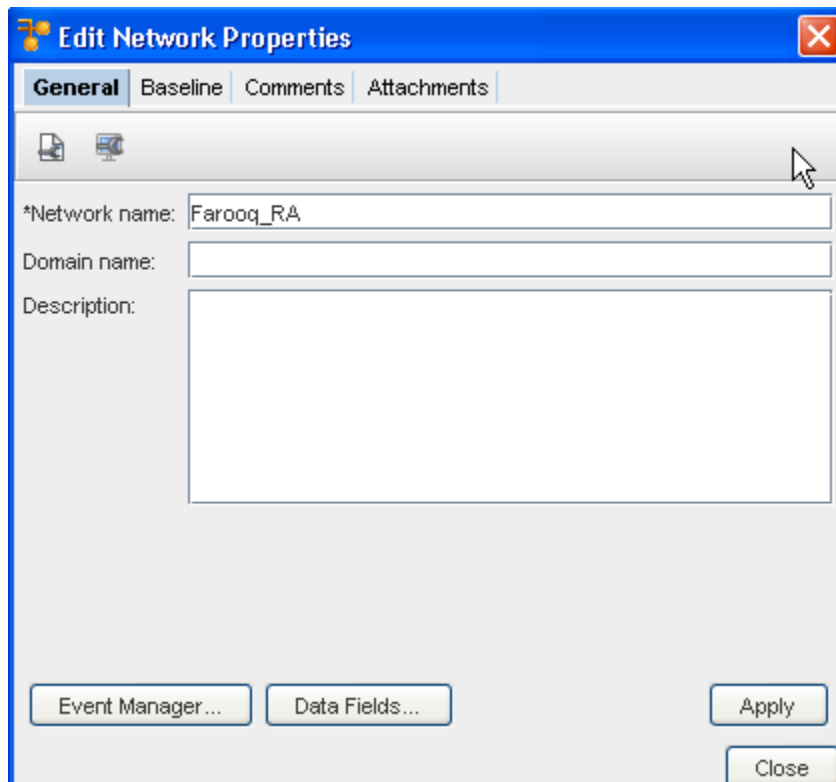
The **General** Tab contains the basic information that was initially entered when the network was created.

- Network Name - Name the network is referred to in Network Configuration Manager
- Domain Name - For example: customer.com
- Description - Information about the network and it's devices

All fields on the General tab can be edited. Only the Network name is required. The Network name is used to identify the network in the Networks Navigation pane.

The General tab also provides access to the following:

-  Scheduling Network Level Config and Hardware Spec Pull Jobs
-  Scheduling Network Level Config and Hardware Spec Pull Jobs



The screenshot shows the 'Edit Network Properties' dialog box with the 'General' tab selected. The dialog has a blue title bar with a close button (X) in the top right corner. Below the title bar are four tabs: 'General', 'Baseline', 'Comments', and 'Attachments'. The 'General' tab is active and contains the following fields:

- \*Network name: Farooq\_RA
- Domain name: (empty text box)
- Description: (empty text area)

At the bottom of the dialog, there are four buttons: 'Event Manager...', 'Data Fields...', 'Apply', and 'Close'.



To edit or change information in this tab if needed,

- 1 Change the existing **Network Name**.
- 2 Change the **Domain Name**.
- 3 Change the **Description**, then click **Apply** and **Close**.

---

**Note** You can access the [Event Manager Overview](#) as well as Data Fields from the General tab.

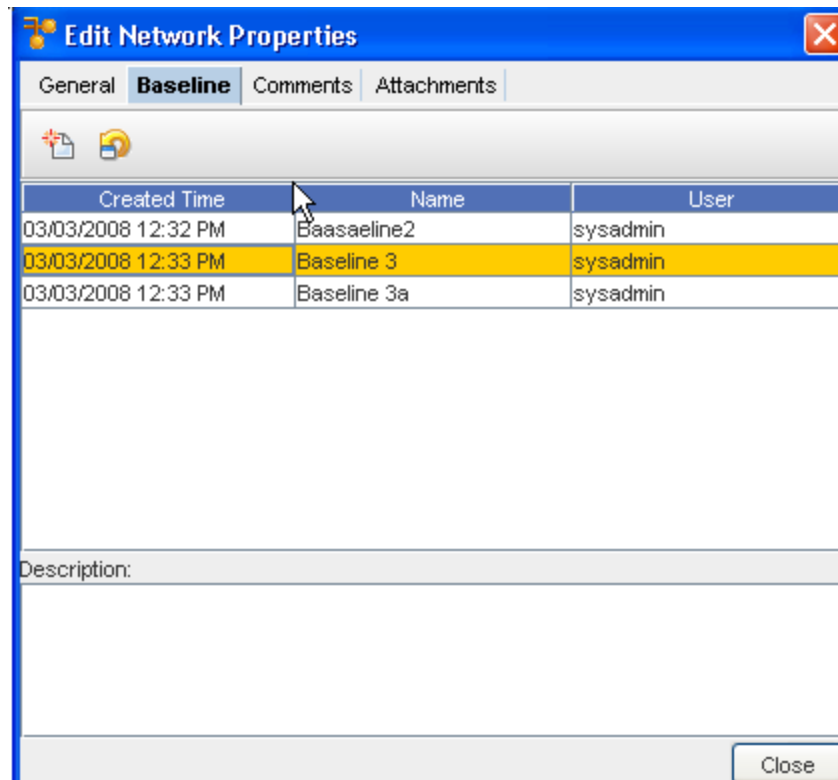
---

## The Baseline Tab

The Network **Baseline** tab allows you to tag all current configuration revisions for the network devices as a **baseline** for future comparisons. Baselines are helpful when you would like to maintain a consistent production collection of configs for your network devices.

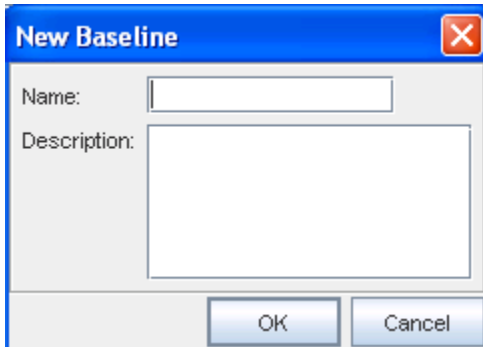
Once set at the Network level, a baseline can be reviewed by device, and a configuration rollback scheduled, if a change occurs on a device.

A baseline snapshot can be updated at any time. To review a device baseline, see the section on the [Baseline Tab Overview](#).



To create a baseline,

- 1 On the Baseline tab, click the **New**  icon. The New Baseline dialog window opens.



- 2 Enter a **Name** for the baseline. The name of the baseline should be reflective of the network configuration.
- 3 If the baseline name does not convey intuitive information about the network, enter a **Description**.
- 4 Click **OK**. The New Baseline window closes. The baseline is added to the Network Properties window. At this point, all device configurations are marked as part of the baseline configs.

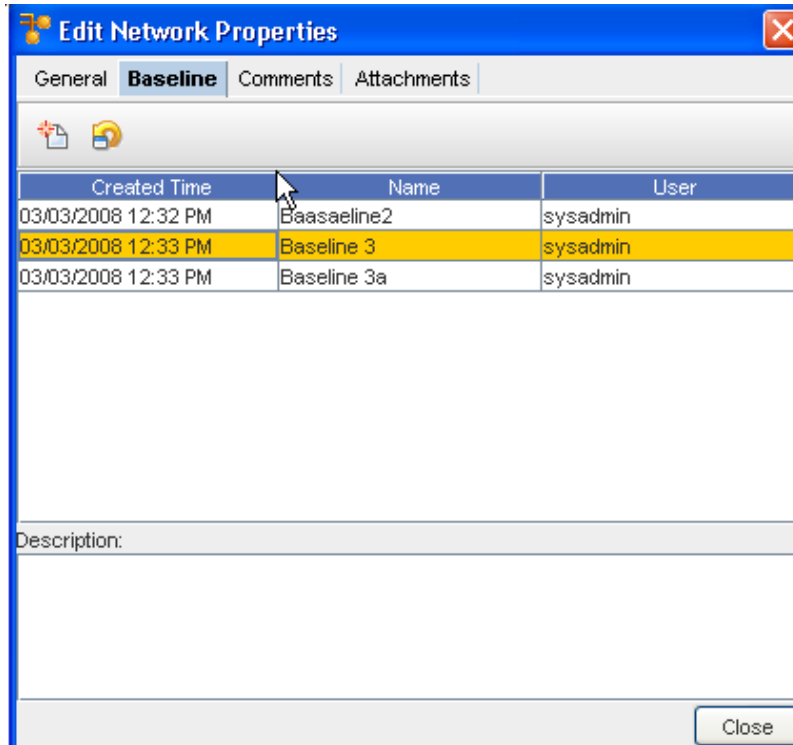
To Rollback to the Baseline,

---

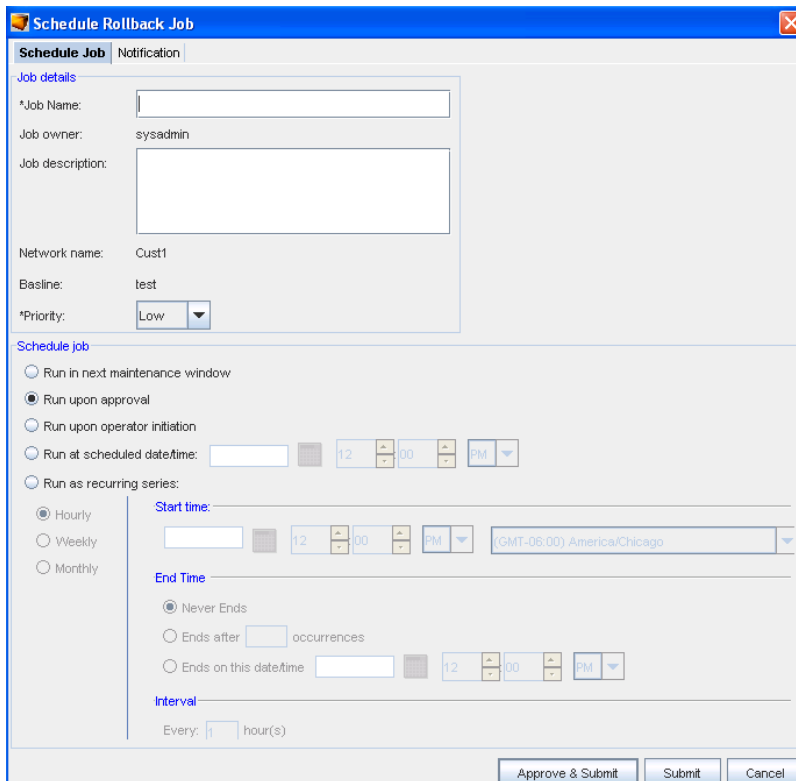
**Important** You can now **rollback any/all devices** that have a new and different configuration revision than the configuration revision that previously existed at the baseline. You can access this feature using the **Rollback icon**.

---

From this window, you can roll back to the baseline - back to the beginning.



- 1 Select the Baseline, then click the **Roll Back** icon to display the Schedule Rollback Job window.



- 2 Complete the information needed in the **Job Details** section of this window, including selecting a **priority** from the drop-down arrow.

- Next, schedule a time in the **Schedule Job** portion of the window.
- Schedule the users you want notification of this job to go to accessing the **Notification tab**.

---

**Important** For more information, go to [Using the Scheduler](#).

---

- After making your revisions, or adding additional information, click **Submit**. This starts your job in the process, with the revisions.
- You can now **Close** the Edit Network Properties window.

---

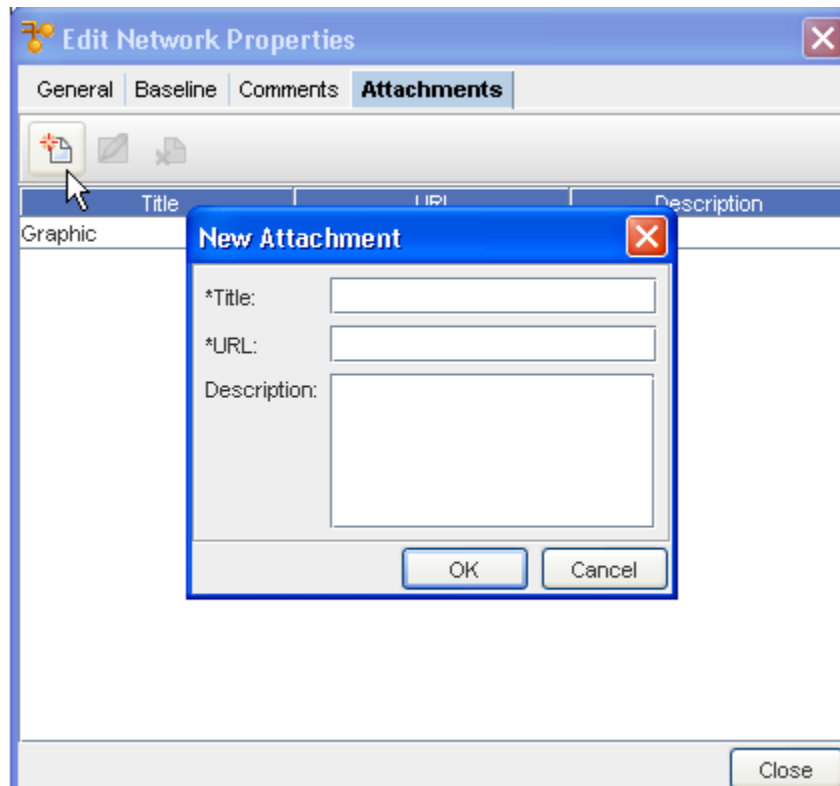
**Note** You can click **Approve & Submit** if you have the appropriate permissions.


---

## The Comments Tab

The **Comments** tab contains a running list of comments, related to the Network, its devices, or other components. The comments are logged as they are entered. Each comment includes a header with the author's name, and the date the comment was created. Comments are separated by a series of dashed lines.

To create a comment,

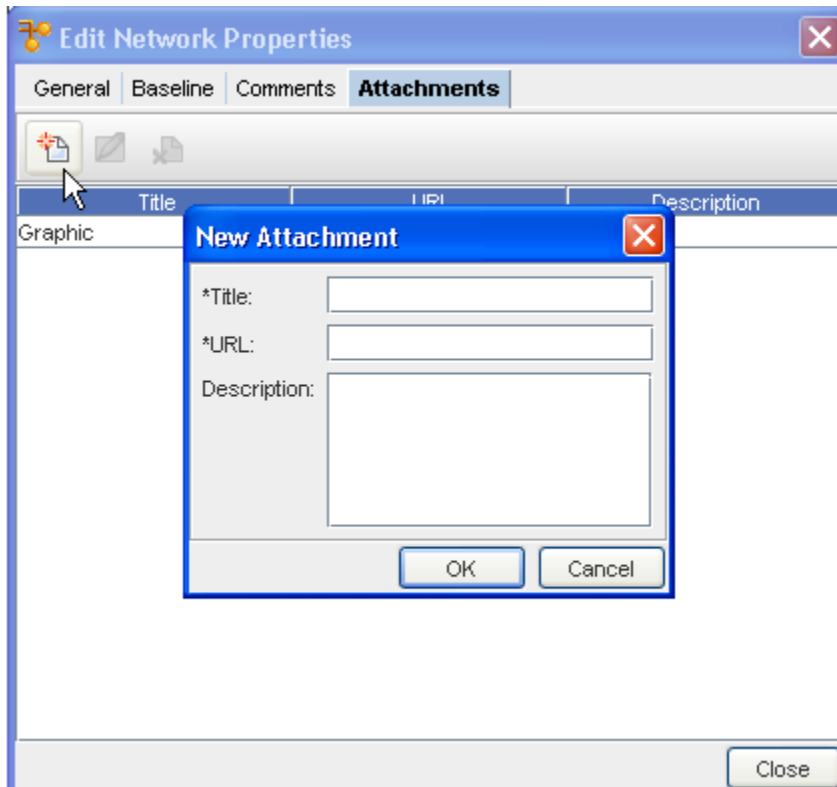


- On the Comments tab, click the **New**  icon. The New Comment dialog window opens.
- Enter **comments**. The Enter key can be used to create paragraph breaks while you are entering your comments.
- Click **OK**. The New Comments window closes. Each new comment is added at the top.

- 4 For each additional comment, repeat **steps 1-3**.
- 5 Click **Close** when you are finished entering comments.

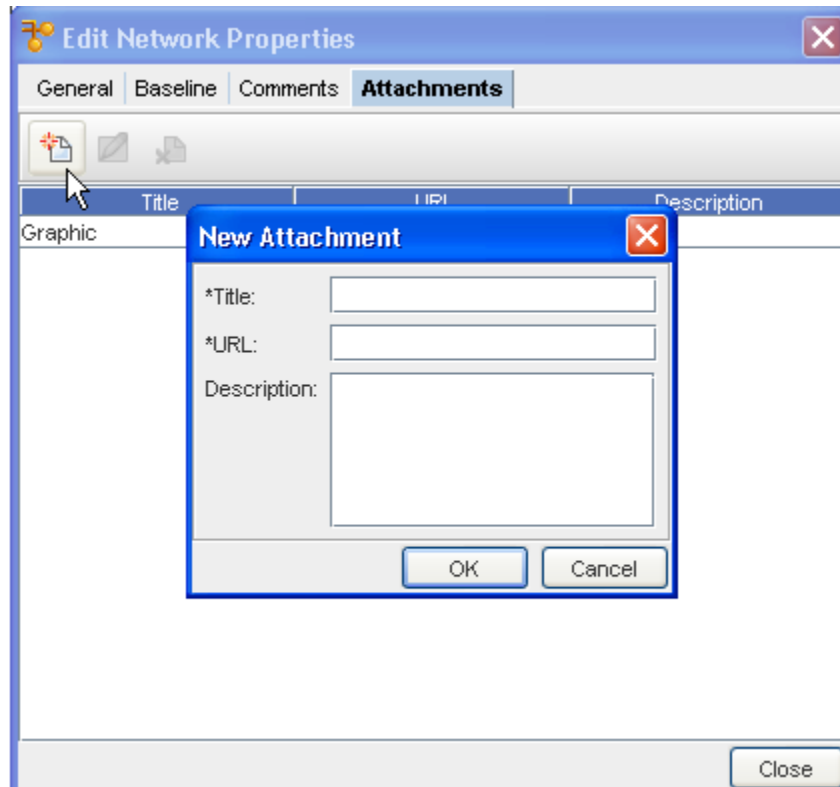
## The Attachments Tab

The **Attachments** tab allows you to associate an **external file to the site** . This can include worksheets, documents, or .html files. Any document that can be opened in a web browser can be mapped as an attachment. Multiple attachments can be added to each site.



- 1 Click the **New** icon, and then enter as **many attachments** as needed.
- 2 Click **Close** when you are finished adding attachments.

## Adding an Attachment



To add an attachment,

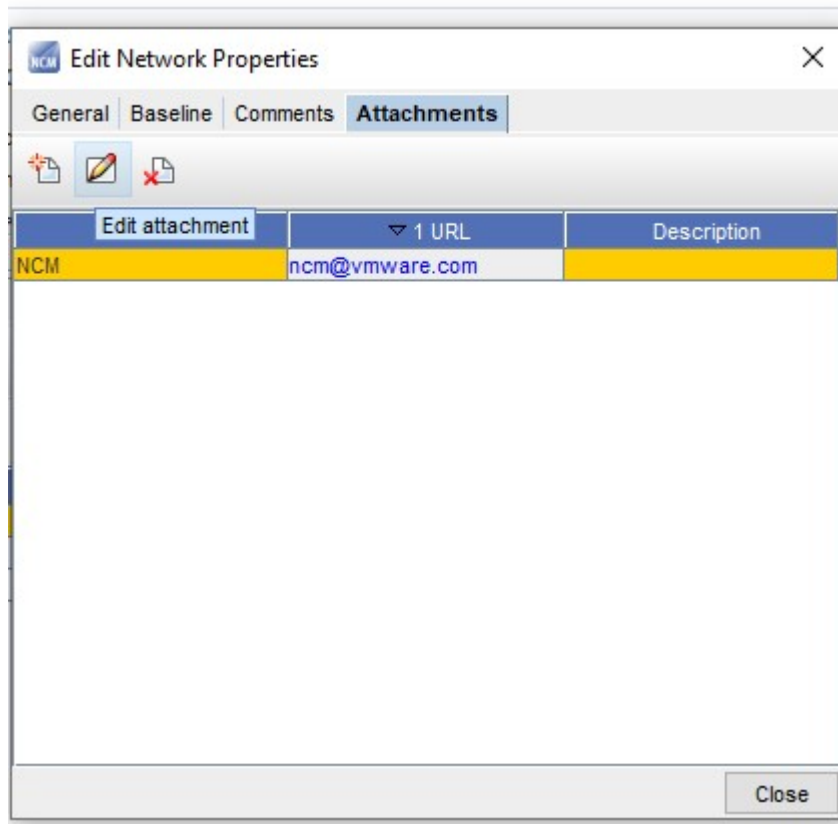
- 1 On the **Attachments** tab, click the **New icon**. The New Attachments dialog window opens.
- 2 Enter a title **for the attachment** .
- 3 Enter a **URL**. Remember, the document must be saved in a format that will open in a browser.
- 4 If needed, enter a **description**.
- 5 Click **OK**. The New Attachments window closes.
- 6 For each new attachment, repeat **steps 1-5**.
- 7 Click **Close** when you are finished adding attachments.

---

**Note** The Edit and Delete icons are only active when one or more attachments have previously been created.

---

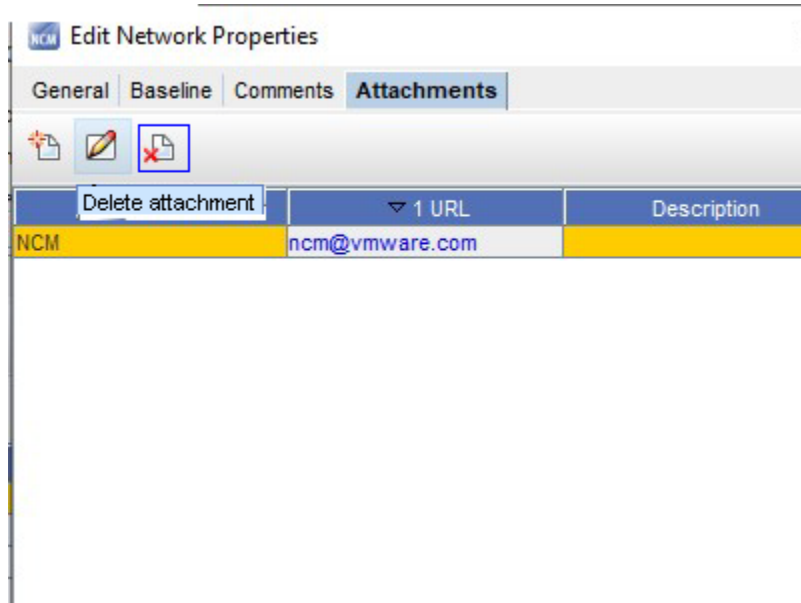
## Editing an Attachment



- 1 First, select an attachment from the listing of attachments.
- 2 On the Attachments tab, click the **Edit** icon. The Edit Attachments dialog window opens.
- 3 The Title, URL and Description fields can all be edited. Make any changes as needed.
- 4 Click **OK**. The Edit Attachments window closes. The attachment row updates with the edited details.
- 5 Click **Close** to close the Edit Network Properties window.

## Deleting an Attachment

When deleting an attachment, the actual document that you are referring to is **not** deleted. You are removing its linked reference from Network Configuration Manager.




- 1 First, select an attachment from the list of attachments.
- 2 On the Attachments tab, click the **Delete** icon. The Confirm dialog window opens asking, "Are you sure?".
- 3 To delete, click **Yes**.
- 4 Click **OK**. The Confirm window closes. The Attachment tab refreshes.
- 5 Click **Close** when you are finished deleting attachments from the list.

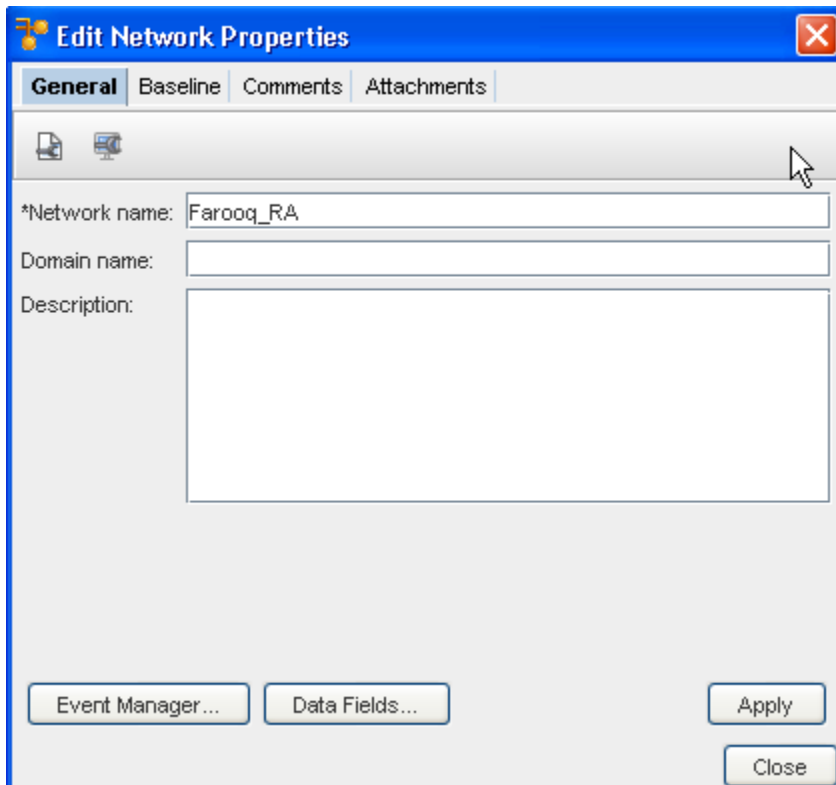
## Scheduling Network Level Config and Hardware Spec Pull Jobs

- Pulling of **Network and Hardware configurations** in this manner is typically completed when you do not have SNMP trap or syslogging enabled for devices.
- A Network level config pull job pulls all devices and updates your current Network configuration with any changes that have occurred since the last pull.
- A Network level hardware pull job polls each device and updates all hardware details. Hardware information is also revisioned.
- Both types of pull jobs use the Schedule Job window, and allow you to send email updates to other users (external and internal) who need to be notified on the status of the pull jobs (through the Notification tab)

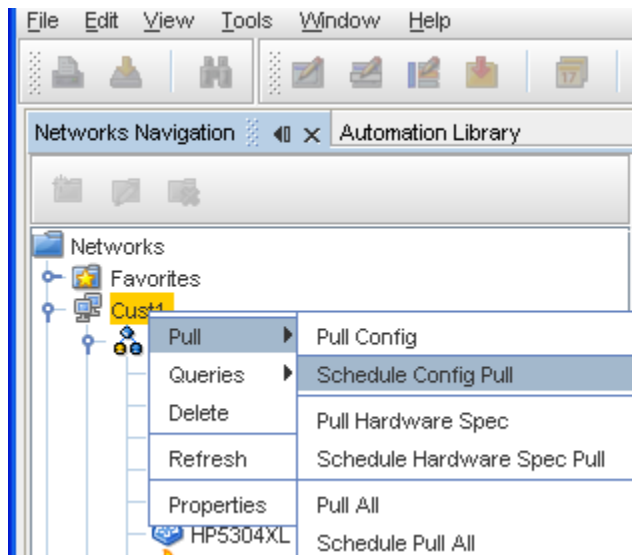
There are two ways to access this feature:

- 1 On the **Network Properties** window, click the **Config**  or **Hardware**  Polling Jobs icons.





- 2 In the Networks Navigation Pane, right-click on the **N e** twork name, select **Pull**, then select **Schedule Config Pull** .



The pulling of network and hardware configurations is typically used when a customer *does not* have SNMP trap or syslog capabilities. Setting up a **recurring pulling** of the network allows you to have the most current network information on a set schedule.

- A **Network Level Config Pull Job** polls all network devices, and updates your current network configuration with any changes that have occurred.

- A **Network Level Hardware Pull Job** polls all network devices, and updates all hardware details.

**Important** For more information scheduling jobs, see [Using the Scheduler](#).

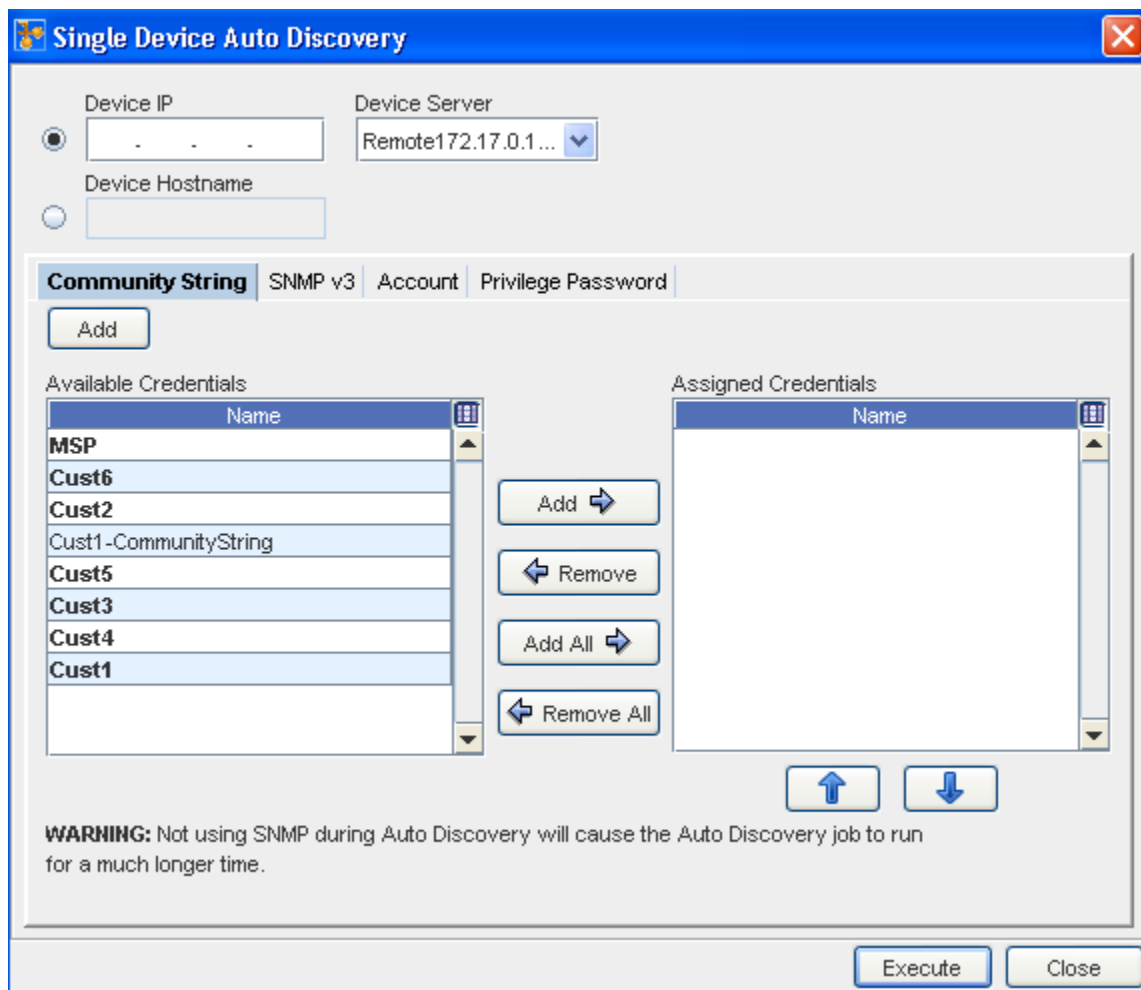
## Single Device Auto Discovery

Single Device Auto Discovery provides you with the ability to discover a single device from the Edit menu within a Network. This eliminates the need to access System Administration to manage newly deployed devices. You only have to enter the Management IP Address of the device to be discovered, complete the remaining options in the window and tabs, then Execute. The Scheduler Job window is bypassed for a Single Auto Discovery task.

While in the Devices view, you can select **Edit** from the menu bar, and then go to the **Single Device Auto Discovery**, to run an Auto Discovery job on a single Device.

- 1 From the menu bar, select **Edit** -> **Single Device Auto Discovery**.

The Single Device Auto Discovery window opens.



**Single Device Auto Discovery**

Device IP:  . . .

Device Hostname:

Device Server: Remote172.17.0.1...

Community String | SNMP v3 | Account | Privilege Password

Add

Available Credentials

Name
MSP
Cust6
Cust2
Cust1-CommunityString
Cust5
Cust3
Cust4
Cust1

Assigned Credentials

Name
------

Add

Remove

Add All

Remove All

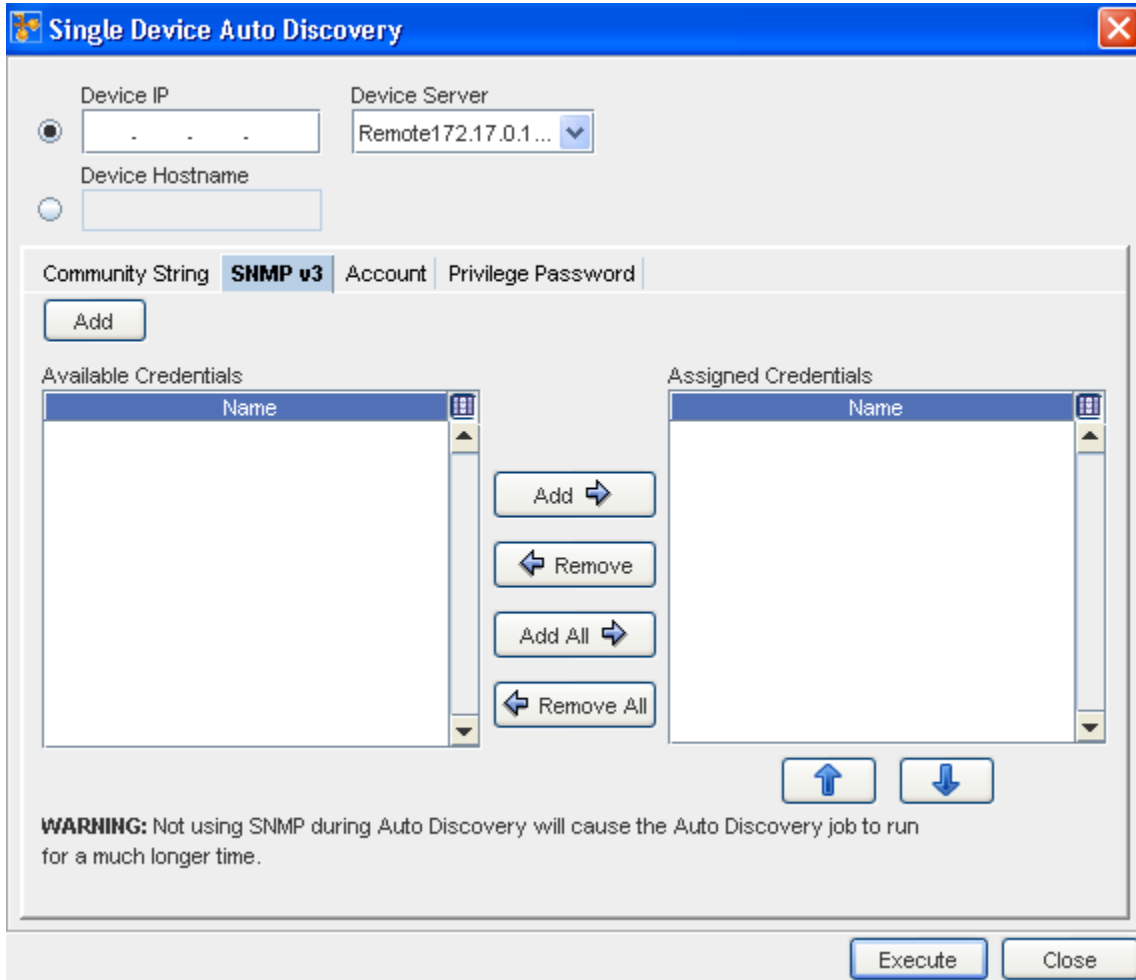
↑ ↓

**WARNING:** Not using SNMP during Auto Discovery will cause the Auto Discovery job to run for a much longer time.

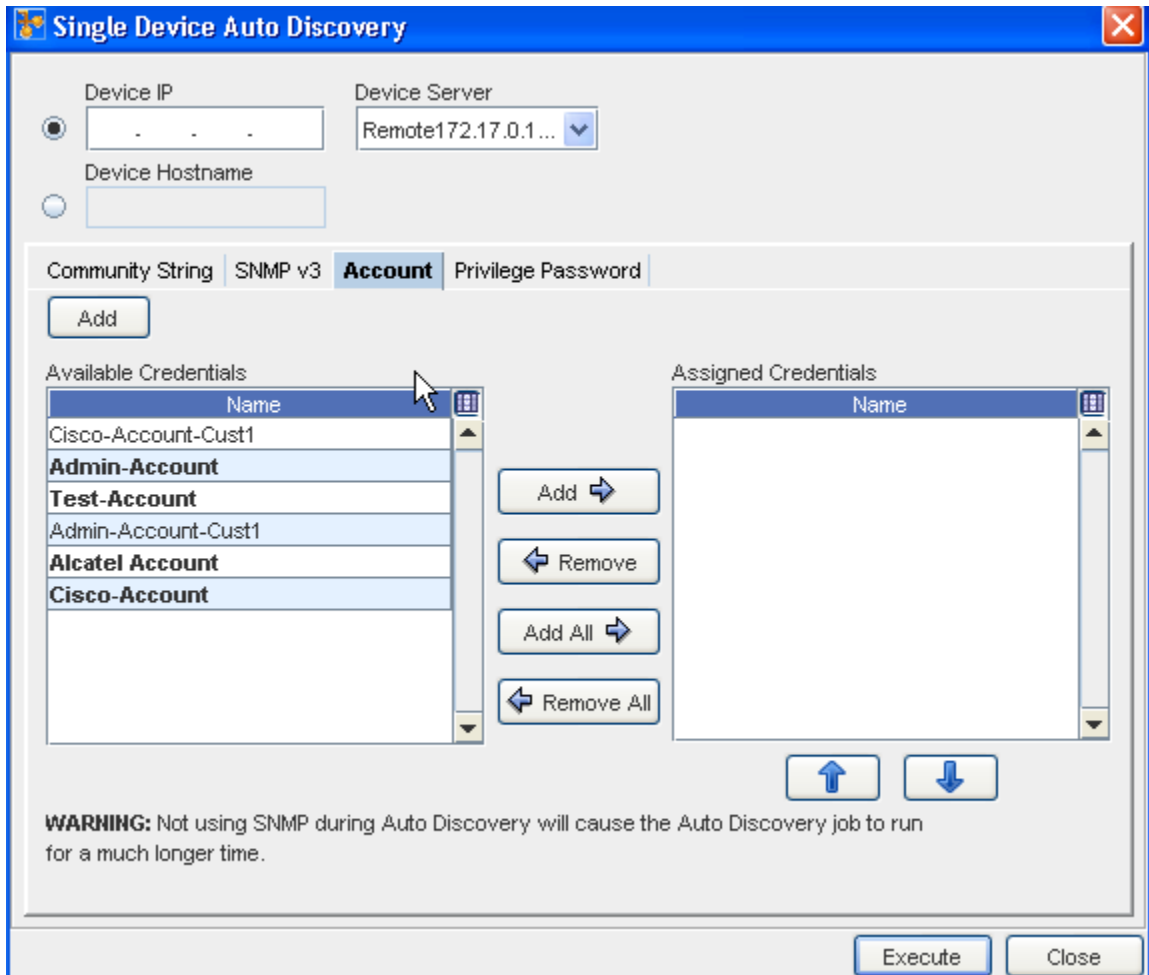
Execute Close

- 2 Enter the **Device IP Address** into the field.

- 3 Enter the **Device HostName**.
- 4 Click the **Device Server** drop-down arrow, and make a selection from the Device Server List.
- 5 In the **Community String** tab , click the **Add** button to Add a Credential, or from the list of Credentials, **Add Available Credentials** or **Remove Assigned Credentials**. As appropriate using the right arrow (->) to add Available Credentials, or use the left arrow (<-) to remove previously Assigned Credentials.
- 6 Go to the **SNMP v3** tab and make any needed additions or changes. From this tab, you can also Add or Remove credentials using the appropriate arrows.

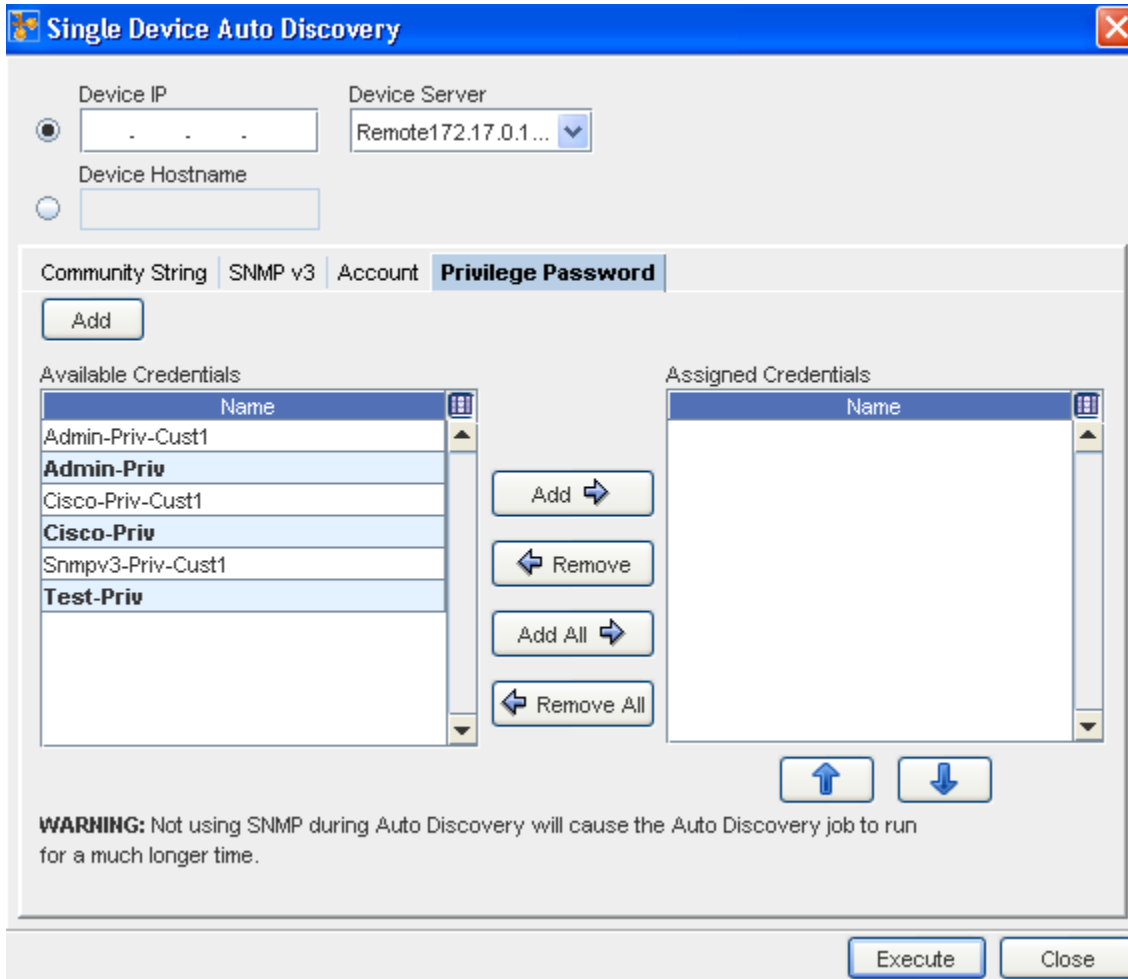


- 7 Go to the **Account** tab and make any needed additions or changes. From this tab you can also Add or Remove credentials using the arrows.



**Important** Make note of the Warning before executing the job.

- 8 Click **Execute** to run Auto Discovery on this single device. The results of the Auto Discovery are displayed.
- 9 Go to the **Privilege Password** tab and make any needed additions or changes to the credentials in the Available or Assigned panes.



10 Click **Execute** to begin the config pull.

## Scheduling Run Times

Regardless of how the Schedule Job window is accessed, the method for scheduling jobs is the same.

- All the required fields must be populated.
- Any required fields not filled generate errors until they are filled correctly.

For more information on the various settings, see [Scheduling Auto Discovery Jobs](#).

In the Schedule Job window (Job Details section),

- 1 Enter the **Job Name** .
- 2 Enter a **Description** (this is optional).

The screenshot shows the 'Schedule Job' window with three tabs: 'Schedule Job', 'Tasks', and 'Notification'. The 'Schedule Job' tab is active. Under 'Job details', there are three fields: 'Job Name' (empty), 'Job owner' (sysadmin), and 'Job description' (empty). At the bottom, there is a '\*Priority:' label and a dropdown menu currently set to 'Medium'.

3 From the drop-down list, select a **Priority level**.

The screenshot shows the 'Schedule job' window. It has several radio button options: 'Run in next maintenance window', 'Run upon approval', 'Run upon operator initiation', 'Run at scheduled date/time', and 'Run as recurring series'. The 'Run as recurring series' option is selected. Under this option, there are sub-options: 'Hourly', 'Weekly', and 'Monthly'. The 'Hourly' option is selected. The 'Start time' is set to 12:00 PM in the (GMT-06:00) America/Chicago zone. The 'End Time' is set to 'Never Ends'. The 'Interval' is set to 'Every: 1 hour(s)'. At the bottom right, there are three buttons: 'Approve & Submit', 'Submit', and 'Cancel'.

4 At the Schedule job section, by default, all jobs are scheduled to **Run upon approval** .

**Important** All selections (in the example shown here) are displayed as being active in the schedule for viewing purposes only. All selections may not always be active. With adequate permission, you can click the Submit button located at the bottom of the window.

5 Note that you can select to have the job **Run in next maintenance** window.

6 If you select the **Run upon operator initiation** option, and Submit for approval, this keeps the job in a pending state after approval. After this, any user with Schedule permissions, can then execute this job.

- 7 To set a specific time, select **Run at scheduled date/time** . The related date and time fields activate.
- 8 Enter a **date**. For assistance, use the Calendar icon to open a monthly calendar. Select the time. The hour, minute and AM/PM setting must be designated. If this option is okay, click **Submit**.
- 9 To set a recurring schedule, select **Run as recurring series** . The recurring setting options activate.

---

**Important** When the recurring schedule is selected, the new **time zone** drop-down options are available. Make your selection from the drop-down options. The time zone you select must be the **client's time zone** . The new time zone field will be propagated with the client time zone automatically when creating a new Maintenance Window or recurring scheduled job.

---

- 10 Set the recurring options: Frequency, Start and End Times, and Time Interval. If this option is okay, click **Submit**. The job is sent to the Schedule Manager and the Schedule Job window closes.








In the Schedule Job section of the window,

The **Cancel** button takes you out of this window, and back to the previous window you opened. The job is sent to the Schedule Manager, and the Schedule Job window closes.

- To review the process of a job, see the [Schedule Manager Overview](#) .
- Once scheduling for the run is completed, go to the [Using the Notification Tab to Send an Email](#) to send email.

## Sending Email Notifications

The available states for Email notifications are:

Notification	Description
	<b>Pending Approval</b> - the scheduled job is waiting to be approved by a user with the appropriate permissions
	<b>Approved</b> - notifies the recipient when the scheduled job has been approved
	<b>Rejected</b> - notifies the recipient that the job has been rejected
	<b>Running</b> - notifies the recipient that the job is currently running
	<b>Completed</b> - notifies the recipient that the scheduled job was pushed successfully, and is completed
	<b>Completed with Warning</b> - successful push with a warning to the recipient
	<b>Partial Completion</b> - notifies the recipient that the push was only partially completed



**Failed** - notifies the recipient that the push failed without making the changes contained in the file

---



**Expired** - notifies the recipient that the time for the push has expired

---



**Hold** - notifies the recipient that the scheduled job has been placed on hold

---



**Deleted** - notifies the recipient that the scheduled job has been deleted

---

See: [Using the Notification Tab to Send an Email](#) notifications for more information.

## Working with Network Settings

### Network Settings Overview

From this area within System Administration, you can create new Networks, set Network level communication protocols, create Network credentials, and run Auto Discovery jobs to manage devices within the Network. Also from this area, you can set Network priorities, schedule Network pull jobs, and create production network baselines.

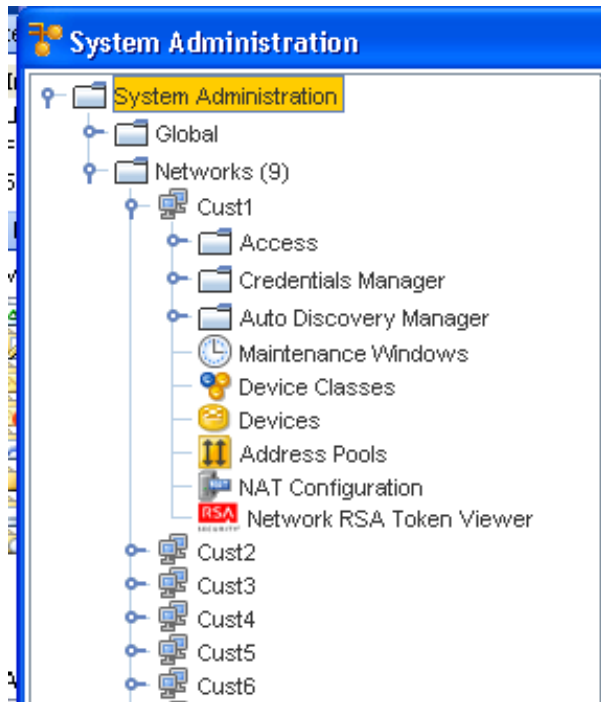
Network settings are used to configure Network Configuration Manager access and communication settings. Network Configuration Manager uses permission levels that permit you to strengthen the security of, and access to, your networks.

Network Configuration Manager has the flexibility to implement settings and changes down to the device level and the global settings level (a standard to which all networks, and their devices comply).

The **Networks** section allows you to complete the following:

- Creating networks
- Running Auto Discoveries
- Overriding Device Classes
- Communications
- Maintenance windows
- Creating IP Address Pools
- Establishing network-local credentials and out-of-band servers





The System Administration window has a traditional two frame view. On the left in the Navigation Pane, are the entry points to the major sections of the System Administration module, including:

- Access - which can be expanded to include:
  - Out-of-Band Servers
  - Device Servers

This allows you to configure device servers and out-of-band server settings, and which devices will be Auto Managed when the devices are Auto Discovered on the servers. You can also reassign a device to another device server from this view.

Here are the remaining components of Networks in the System Administration too:

- Credentials Manager
- Auto Discovery
- Maintenance Windows
- Device Classes
- Devices
- Address Pools
- NAT Configuration
- Network RSA Token Viewer

Within the above components, you are able to complete the following tasks:

- Configure any **Out-of-Band servers**

- Determine which **Device Servers** are associated with your network
- Set which devices are automatically managed by Network Configuration Manager when **Auto Discovery** runs
- Configure cross network **shared and local** credentials
- Add, edit and delete **Data Fields**
- Manage **users and groups** and their network permissions
- Manage the **Authentication Servers**, and determine user security
- Manage the **locking features**

## Creating Networks

The ability to create networks in Network Configuration Manager is reserved for users with *System or Network Administration privileges*.

After a network is created, but before any devices can be discovered into the network, you need to:

- Associate a network with one or more device servers that will manage the devices in the network
- Assign groups and users to your network
- Create auto-discovery jobs

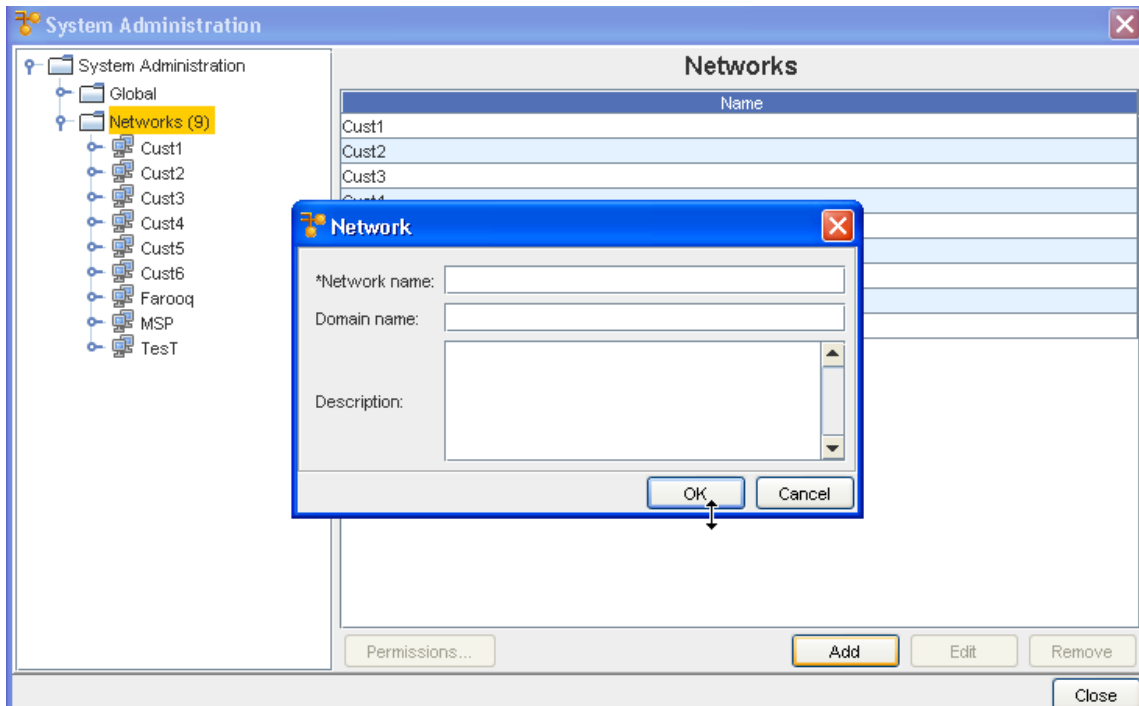
---

**Important** Depending on the way you setup your networks, the networks can be created *before* adding users and groups, or you can create the users and groups *before* creating the networks. Either way is acceptable.

---

To create a new network,

- 1 From the menu bar, select **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, click **Networks**. In the right pane, a list of all current networks displays and the Add button is activated at the bottom of the window.



- 3 Click **Add**. The Network window opens.
- 4 At a minimum, you must enter a **Network Name**.
- 5 Optionally, enter a **Domain Name** and **Description** of the network.
- 6 When finished, click **OK**. The Network window closes. The navigation pane refreshes and the new network is added to the list of networks.

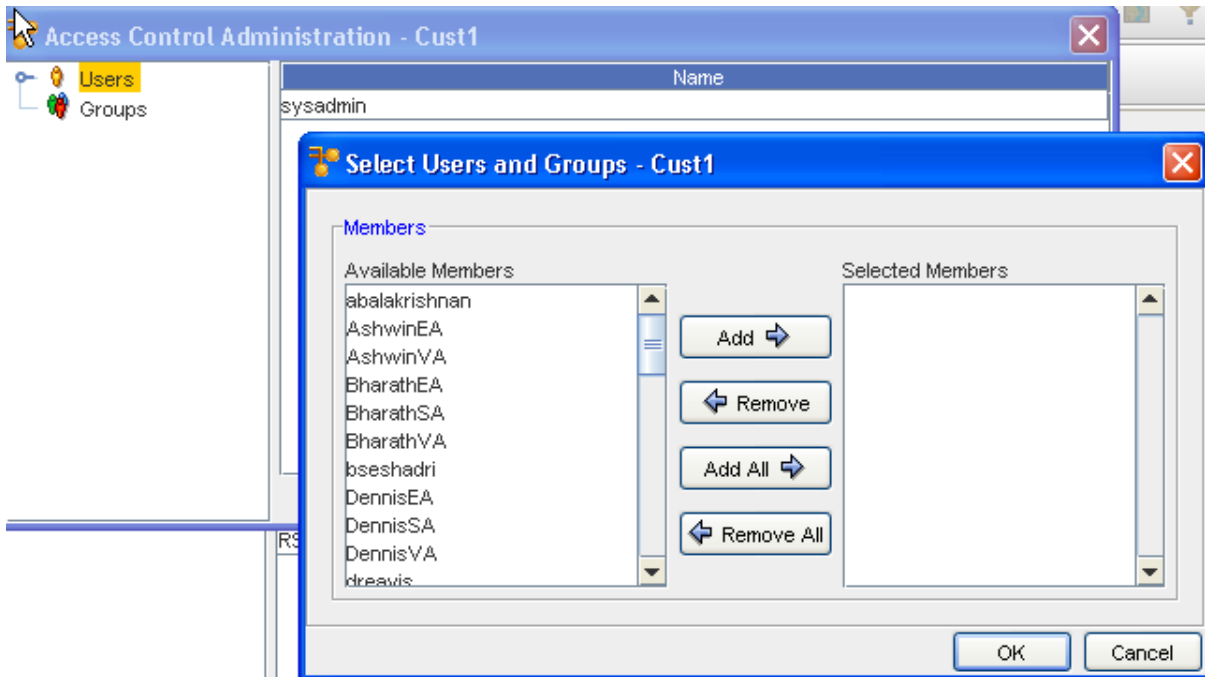
You can now add one or more device servers to manage your network devices.

## Setting Network Permissions

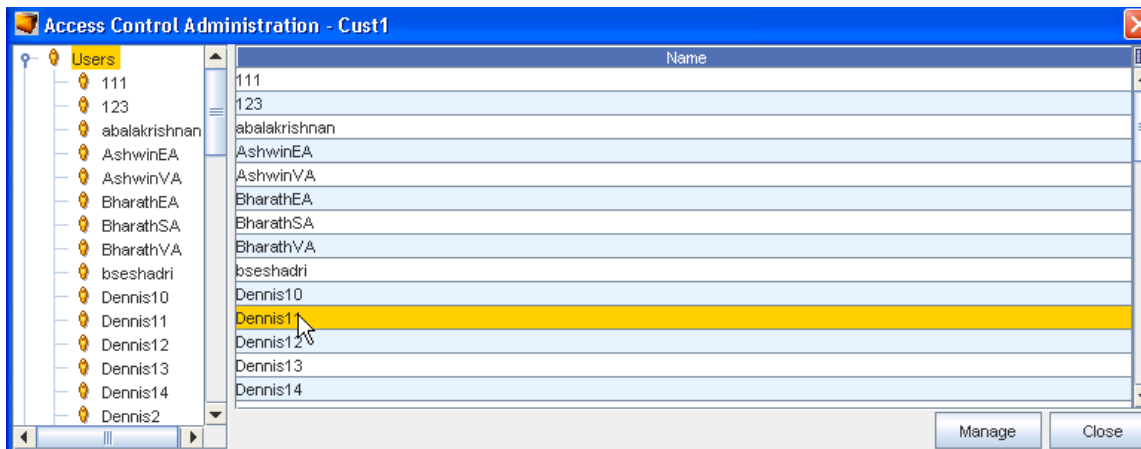
Setting permissions at the Network level for a specific user/group, overrides all other permissions assigned to the network for the specified users/group.

To set network permissions for a user/group,

- 1 After selecting a network, click **Permissions....** The Select Users and Groups - [Network Name] window opens.



- 2 In the navigation pane, select the **User or Group** whose permissions are to be defined.
- 3 Select the User name or names, then click Add.
- 4 Now, click and expand on the Users name in the left panel.



The right pane populates, and displays as follows:

The permissions set in the right pane dictates the actions that the user/group can complete at the

network level. Each action has been grouped according to the module where it resides.

Set permissions for BharathEA

Override Credentials

Manage User Access

Manage Templates

Manage Queries

Manage Compliance

Network

Edit  Delete  View

Workspace

Create  Edit  Delete  View

Device

Create  Edit  Assign Credentials  View Details

View Sensitive Data  Manage OS  Run Non-Scheduled  Run Cut-Throughs

Job

Schedule  Approve

View

Create  Edit  Delete

Override

Select All Deselect All

Reset Apply Close

By default, if the highest level check box is selected, the user/group receives permissions for **all actions** within the group. For example, in the above graphic, View has been selected at the highest level and each included tasks is also selected.

- 5 Select the **areas** for which the user is to have access.
- 6 If the user/group does not require one or more of the included task permissions, click that related check box to de-select the option.
- 7 Repeat **steps 3 and 4** for each area where the user/group requires access.
- 8 If a user/group requires access to all network options in the Access Control Administration window, at the bottom of the window, click **Select All**.
- 9 When finished, click **Apply**. The window remains open allowing you to select other users (or groups) and then set other permissions.

Override Credentials	Allows user/group to set this override for an individual use. This allows the user to update credentials for a job or non-scheduled tasks. For example, when one user must complete an operation or task for another user.
Manage User Access	Allows user/group to manage the access each user has
<b>Manage Templates</b>	Allows user/group access to Create or Modify Templates that reside in the Automation Library. By default, you can view existing templates.
<b>Manage Compliance</b>	Allows user/group to Manage the Compliance attributes
Manage Queries	Allows the user/group to Create, Update, and Delete existing queries
<b>Network</b>	Allows the user/group to <b>Edit, Delete</b> or <b>View</b> networks details. By default, if you are provided Edit or Delete permissions, View is automatically set.
<b>Workspace</b>	Allows the user/group to <b>Create, Edit, Delete</b> or <b>View</b> workspaces. By default, if you are provided Create, Edit or Delete permissions, View is automatically set.
<b>Device</b>	<p><b>Note</b> By default, when a user/group is given permissions to view Networks and Workspaces, they are able to view their devices.</p> <p>Allows the user/group to <b>Create</b> and <b>Edit</b> devices. The <b>View Details</b> check box gives the user/group the ability to view the device properties.</p> <p>The <b>View Password</b> check box allows user/group to View the passwords that must be used to access the device properties.</p> <p><b>Manage OS</b> check box allows the user/group to Modify the OS of the device.</p> <p><b>Assign Credentials</b>, complete <b>Run Cut-throughs</b>, and <b>Run Non-Scheduled Jobs</b></p>
<b>Job</b>	Allows the user/group to <b>Approve</b> or <b>Schedule</b> jobs that are created for the device config
<b>View</b>	Allows the user/group to <b>Create, Edit</b> or <b>Delete</b> Views of the network
<b>Override</b>	Selecting this option allows the user/group to Override any permissions that are set on levels with the permissions defined here

Or, if you are not making changes to the other permission level settings, click **Close**.

## Editing Networks

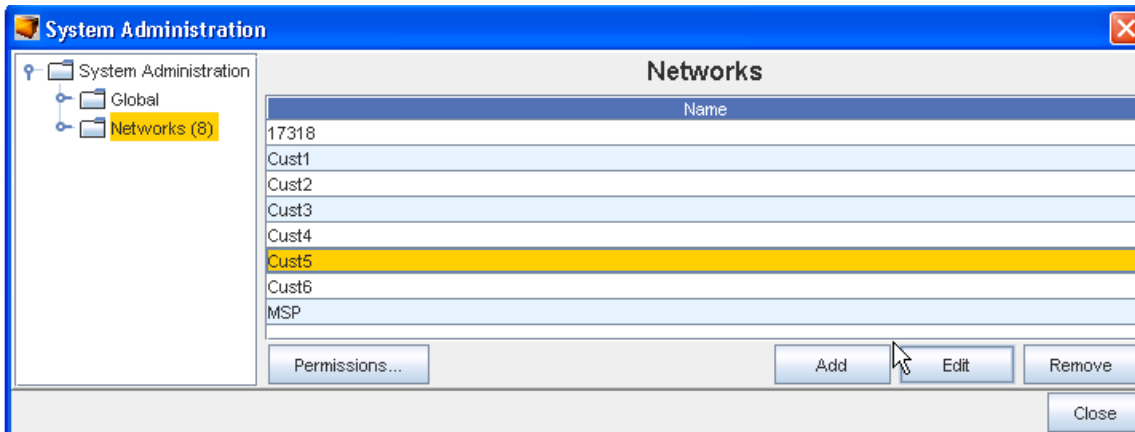
When networks are created, only basic information about the network is entered, such as the name and the domain. After you have created a network, additional information can be entered.

**Note** Network Properties can be managed for a network from inside of System Administration by any user with System or Network Administration privileges.

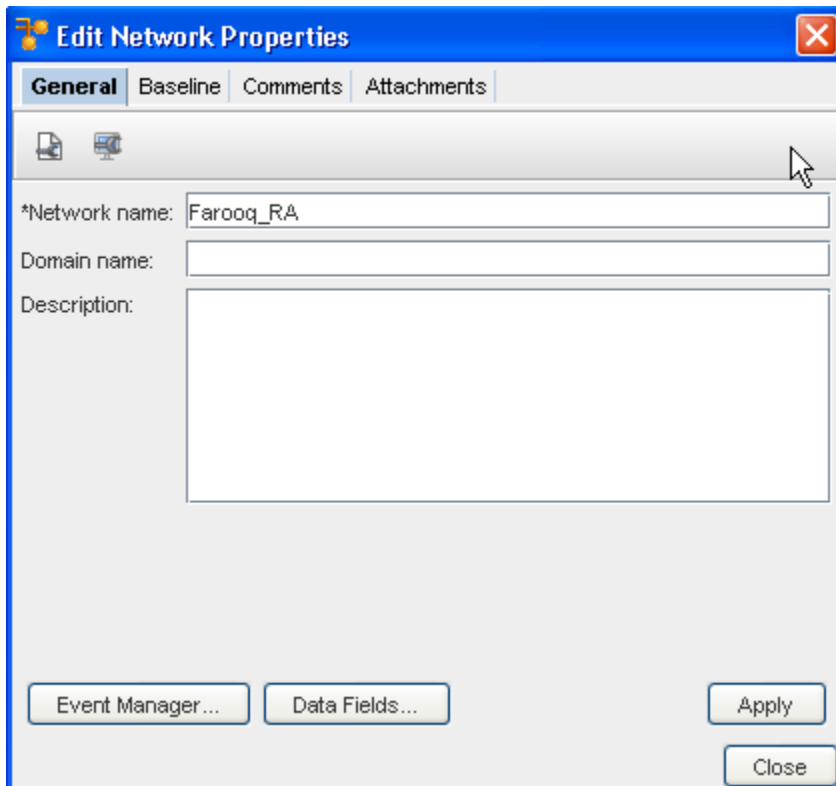
To edit network properties,

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, open **Networks**. In the right pane, a list of all current networks is displayed.

- 3 Click the **network name** . The Edit button is activated at the bottom of the window.



- 4 Click **Edit**. The Edit Networks Properties window opens.



- 5 At the Edit Network Properties window, make the needed changes to the information contained within each tab.
- 6 Click **Apply**, then **Close** when you have completed your changes.

Data Fields

## Removing Networks

When networks are removed, the devices that are managed by the networks are returned to an *Unclassified state*, unless they are also being managed in other networks.

If a network is managed by another network, the status of the device will remain as Managed. Be sure to consider the ramifications to a device before deciding to delete a network.

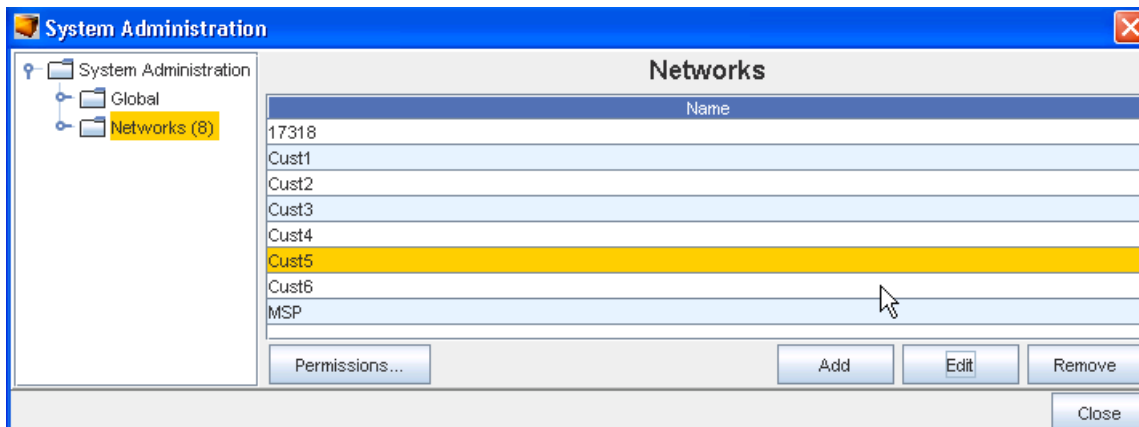
---

**Note** Once a network is deleted, there is no retrieval mechanism to restore the network. Take care when deleting networks.

---

To delete a network,

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, click **Networks**. The right pane refreshes with the list of current networks.



- 3 In the right pane, select the **network** to be removed. At the bottom of the window, the Edit and Remove buttons activate.
- 4 Click **Remove**.
- 5 If Okay, click **Yes**. If **Yes** is selected, the network is removed from the list of networks in the navigation pane.

## Managing Network Access Permissions

When a network is created by the System Administrator, users and groups must be assigned permissions to the network before they can complete any network tasks.

If network permissions are not set by the user/group, then the general permissions assigned to the user/group is used by default.

---

**Note** Each user/group is assigned their own permissions when they are set up in Network Configuration Manager. These default permissions can only be changed by overriding them, and setting specific permissions.

---

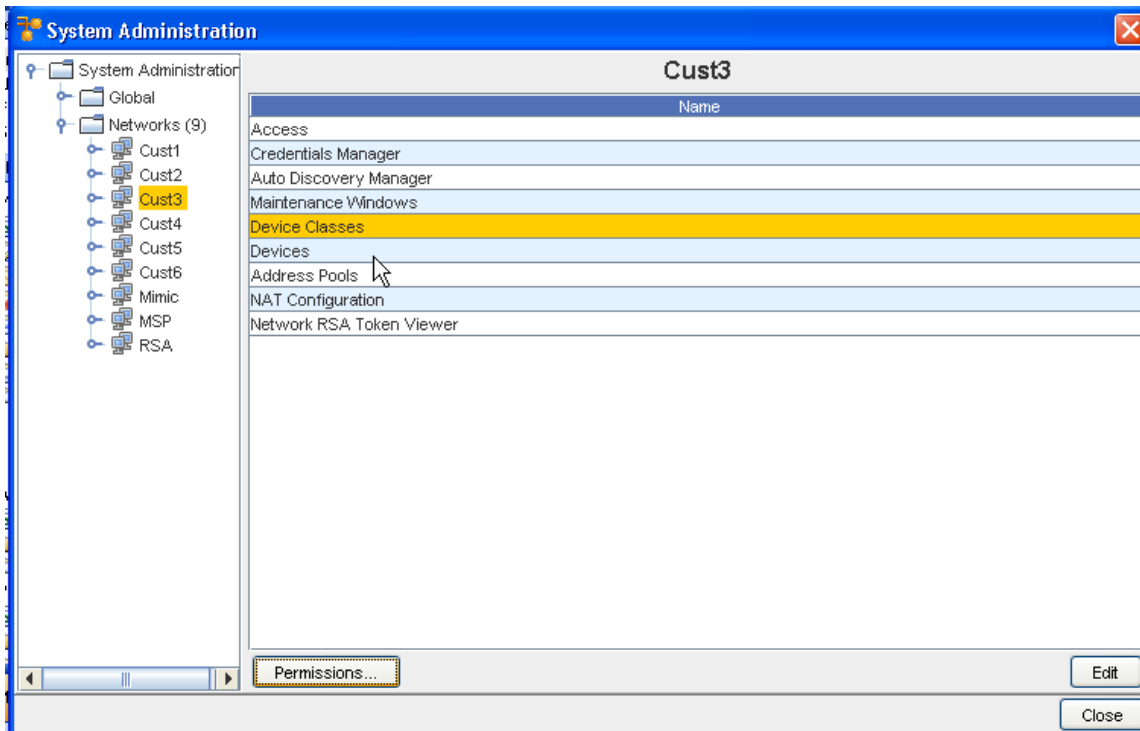


Setting network permissions for users/groups is a two step process:

- Select the user/group who is to have access to the network
- Select the network permissions for the user

To designate users and groups to have Network permissions,

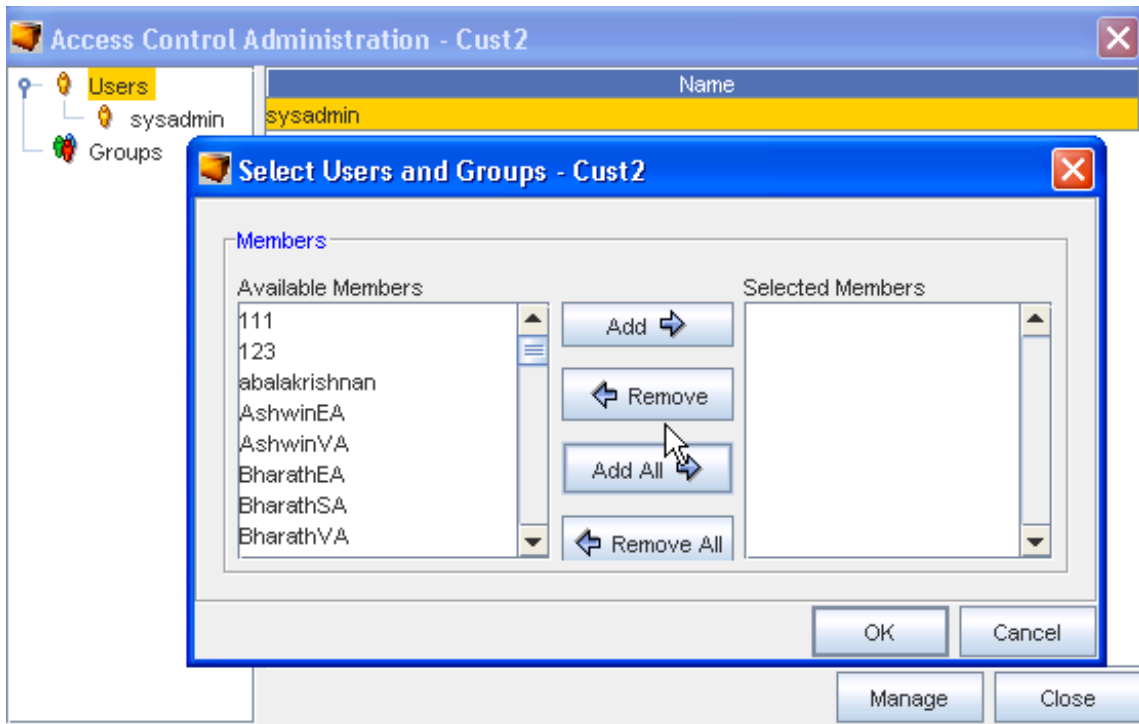
- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand **Networks**. The right pane contains all available networks. Select the **network** from this list. Or... In the navigation pane, select the **Network**. The right pane contains the Network sub-menus.
- 3 In the lower left portion of the window, click **Permissions**. The Access Control Administration - [Network Name] window opens.



There are two groups:

- Users
- Groups

All users and groups that are available in Network Configuration Manager are in the tree menu. Depending the network selection, the right pane contains a list of all Users or Groups currently associated to the network.



- 4 After selecting Users or Groups, click **Manage**. The Select Users and Groups [Network Name] window opens.
  - Users and groups that do not have permissions are listed in the **Available Members** column.
  - All users and groups with permissions are listed in the **Selected Members** column.

By default, your own user name is listed as a user. All others that have been given permissions are categorized, and listed in one of the two groups.

- 5 To give users or groups permissions to the workspace, click the **name of the user or group** in the Available Members column.

---

**Note** A string of users/groups can be selected by holding down the Shift-key while selecting users/groups. Or, select multiple, non-sequential users/groups can be selected by holding the Ctrl key while selecting users/groups.

---

- 6 Click **Add**. The selected users and groups are moved to the **Selected Members** column, and now have permissions to the workspace. Or... To remove a user or groups permissions, in the **Selected Members** column, select the name or group.
- 7 Click **Remove**. The selected users and groups are moved to the Available Members column and no longer have permissions to the workspace.
  - Clicking **Add All** moves all users and groups listed in the Available Members column to the Selected Members column.

- Clicking **Remove All** moves all users and groups back to the Available Members. If you complete this action, remember to put your own user name back into the Selected Members column.
- 8 Once you have assigned the users and groups that are to have access to the workspace, click **OK**. The Select Users and Groups window closes, and your selection is added to the list of Users (or Groups).

The Access Control Administration window refreshes. All users and groups are re-categorized to reflect the changes that were made. You are now able to [Setting User and Group Permissions](#)

## Setting Workspace Permissions for Each User and Group

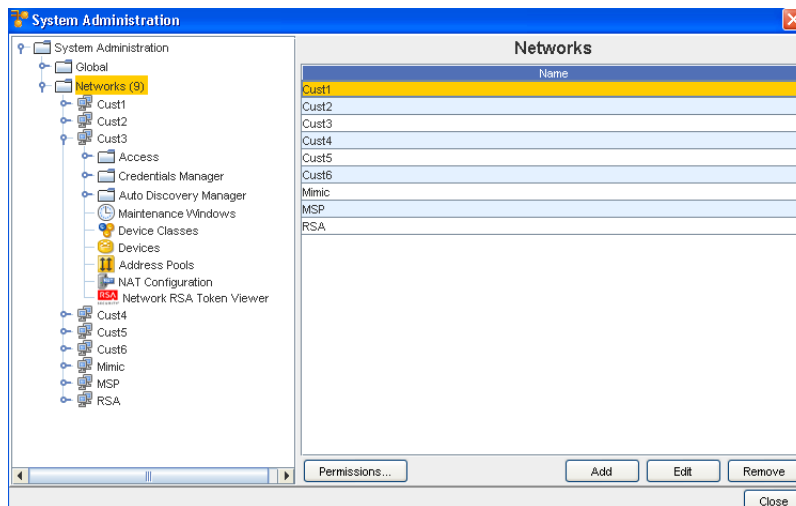
There are two phases for setting permissions for a workspace:

- [Setting Workspace Permissions](#)
- Selecting the permissions that each user and groups will have to the workspace

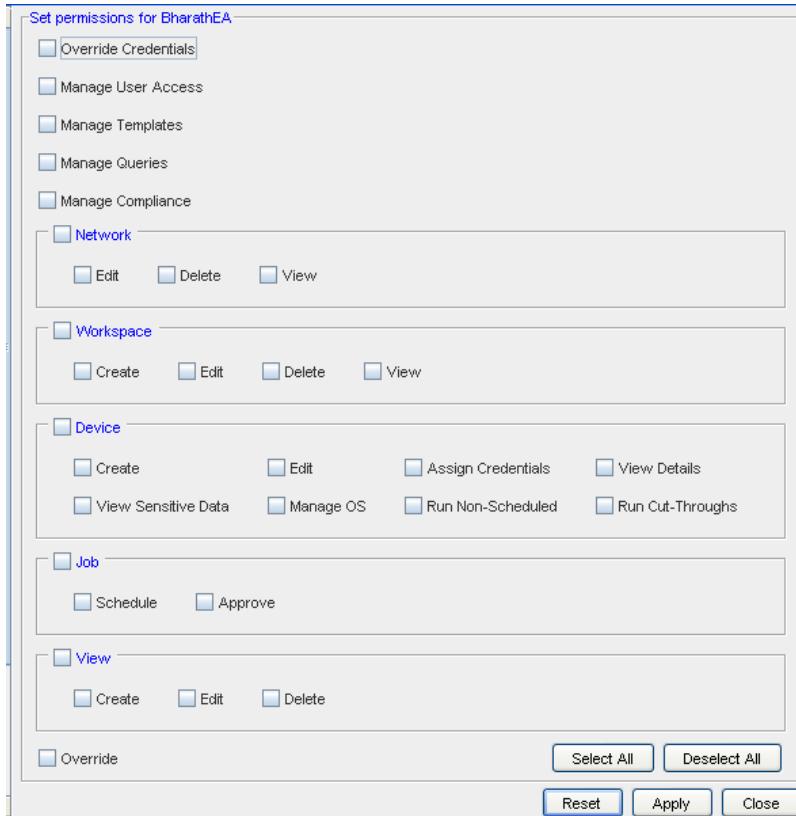
Once you have determined the users and groups that have permissions to your design workspace, you can determine the set of permissions the users and groups will have.

Permissions are set through the Access Control Administration window. For more information on using this window and setting the permissions, see [Setting Workspace Permissions](#)

To set permissions for each user and group,



- 1 From System Administration, select **Networks**. Next, make a selection (in this example, Cust3 was selected from the listing of networks). Now, select **Permissions** to get to the Access Control Administration window. Expand the navigation tree and locate the **user or group**.
- 2 Click the **user or group**. The Set Permissions available for the displays in the right pane.



- 3 By default, all users and groups are provided view access. Using the check boxes, select any additional permissions for the user or group.
- 4 Make your selections for **each task** detailed in this window.

---

**Note** Selecting or clearing the top check box of any category of permissions automatically selects or clears all permissions within the category.

---

- To select all permission, click **Select All**.
  - To clear any existing permissions, and begin your selections with a clean slate, click **Deselect All**.
  - To return to the original set of permissions, click **Reset**.
- 5 Once you have finished setting the permissions, click **Apply**. The Set permissions pane closes, and the Access Control Administration window refreshes.

For a user

## Network - Access

## Network - Out-of-Band Servers

### Out-of-Band Servers Overview

Network Configuration Manager provides an option for setting up *alternative communication methods* using Out-of-Band Servers.

For example, if there is a problem with a device and traffic cannot flow through the network, an *alternate path* can be set using a terminal server to reach the network nodes--even when the network is down!

Out-of-Band servers are used when you need a secure, remote, emergency network access path to **manage** and **troubleshoot device issues** when:

- The device is not on the network
- The device is not network manageable
- The network is down

Network Configuration Manager allows you to set up out-of-band servers at two levels:

- Global level
- Network Level

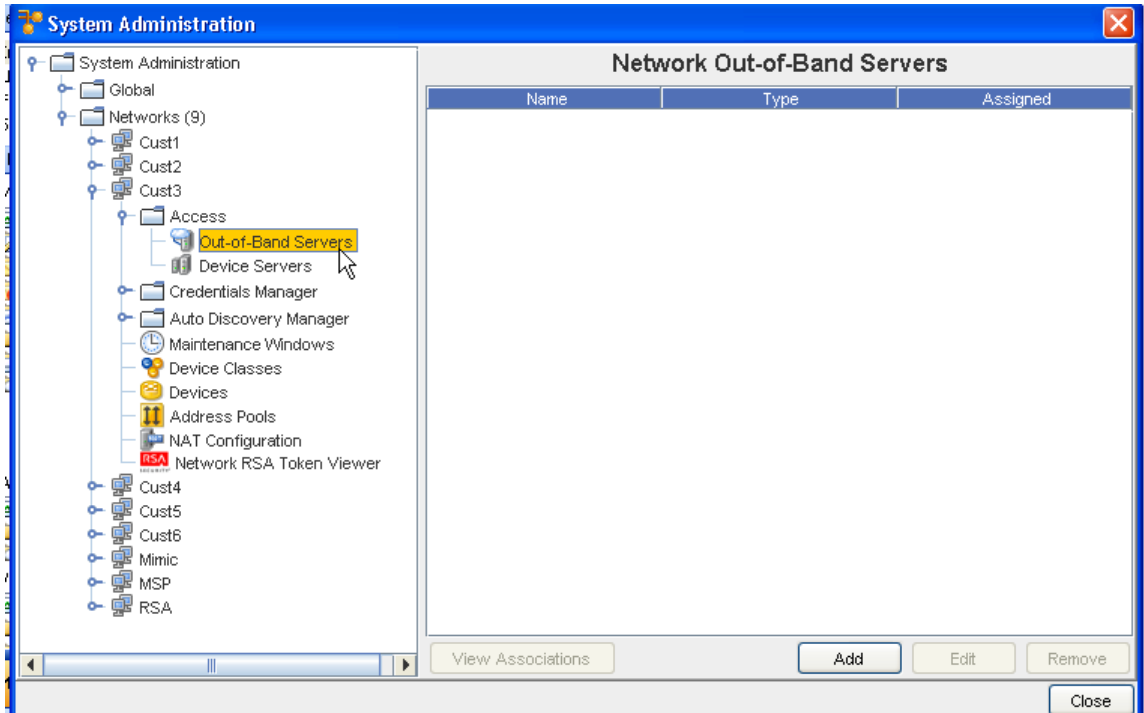
**Network level out-of-band servers** allow you to set up access to out-of-band servers that are used by specific networks only.

When you have configured an out-of-band server for a network, the network defaults to use the network level out-of-band server, unless otherwise indicated.

### Out-of-Band Servers (Networks)

To access the Network Level set up,

- 1 From the menu bar, select **Tools** -> **System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Networks folder**.
- 3 Double-click the **network name**.
- 4 Expand the **Access** folder.
- 5 Click the **Out-of-Band Servers** . The Network Out-of-Band Servers window opens in the right pane.

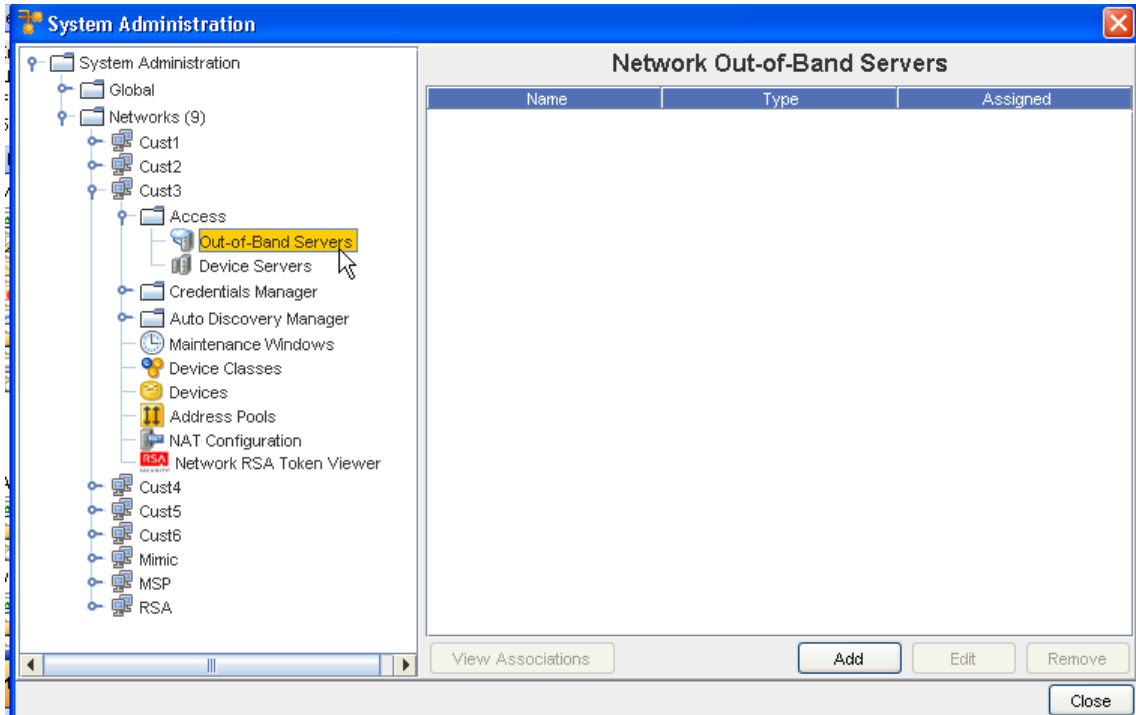


From this window you can View Associations, Add a server, Edit existing servers, or Remove an out-of-Band Server.

### Network - Viewing Associations

To view Associations,

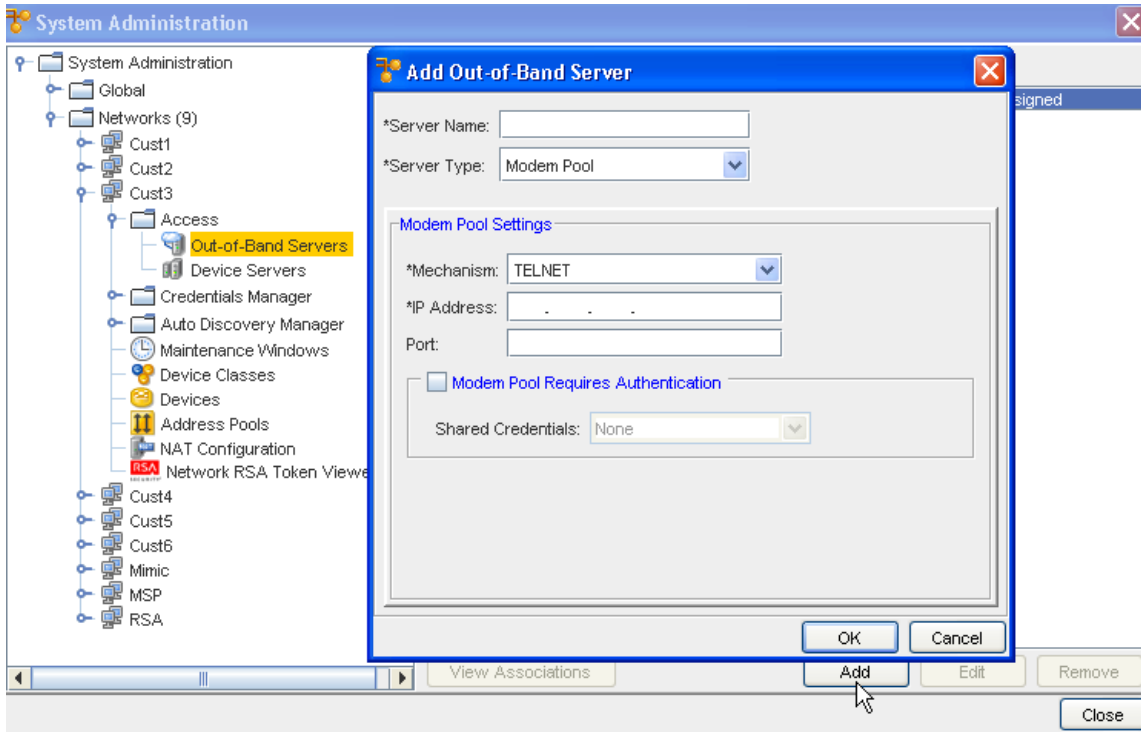
- 1 From the **Network Out-of-Band Server** window, click **View Associations**.
- 2 The View Associations window for that Server opens, allowing you to view the Devices associated with the server. You can resort the order of Devices and Device Classes using the up arrow. Click **Cancel** to leave this window.



### Network - Adding Out-of-Band Servers

To Add an Out-of-Band Server,

- 1 From the **Network Out-of-Band Server** window, click **Add**. The Add Out-of-Band Server window opens.



The following fields are available. Note that the required fields are identified by an asterisk (\*).

- 2 Complete the setup of the out-of-band server options, as needed.
- 3 When finished, click **OK**. The Add Out-of-Band Server window closes.

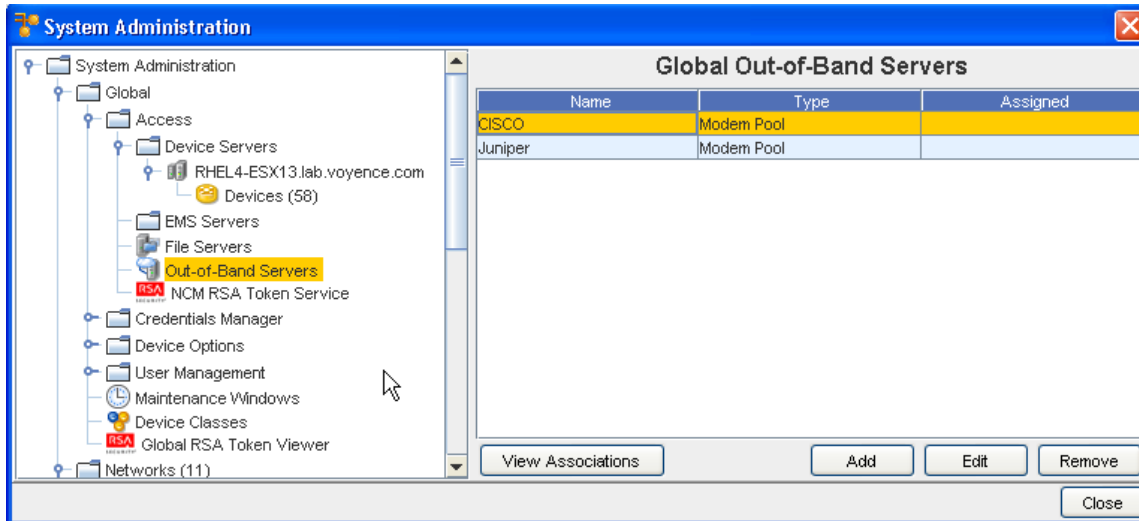
Field	Description
Server Name	The name of the server being used for out-of-band access
Server Type	The type of server being used. Current options: - Modem Pool Settings - Terminal Settings
Modem Pool Settings	Based on the selected server type, the available fields are:
Mechanism:	Telnet or SSH
IP Address:	IP address used for connection
Port:	The Port Number
<b>Modem Pool Requires Authentication</b>	The <b>Modem Pool Requires Authentication</b> check box should only be used if you have configured a User name and Password access security in Shared Credentials. You can also select from the listing of <b>Shared Credentials</b> using the drop-down arrow to see the list.

The configured out-of-band server is listed in the Out-of-Band Server window.



## Editing an Out-of-Band Server

- 1 Select a Server from the listing in the **Network Out-of-Band Servers** window, then click **Edit**.



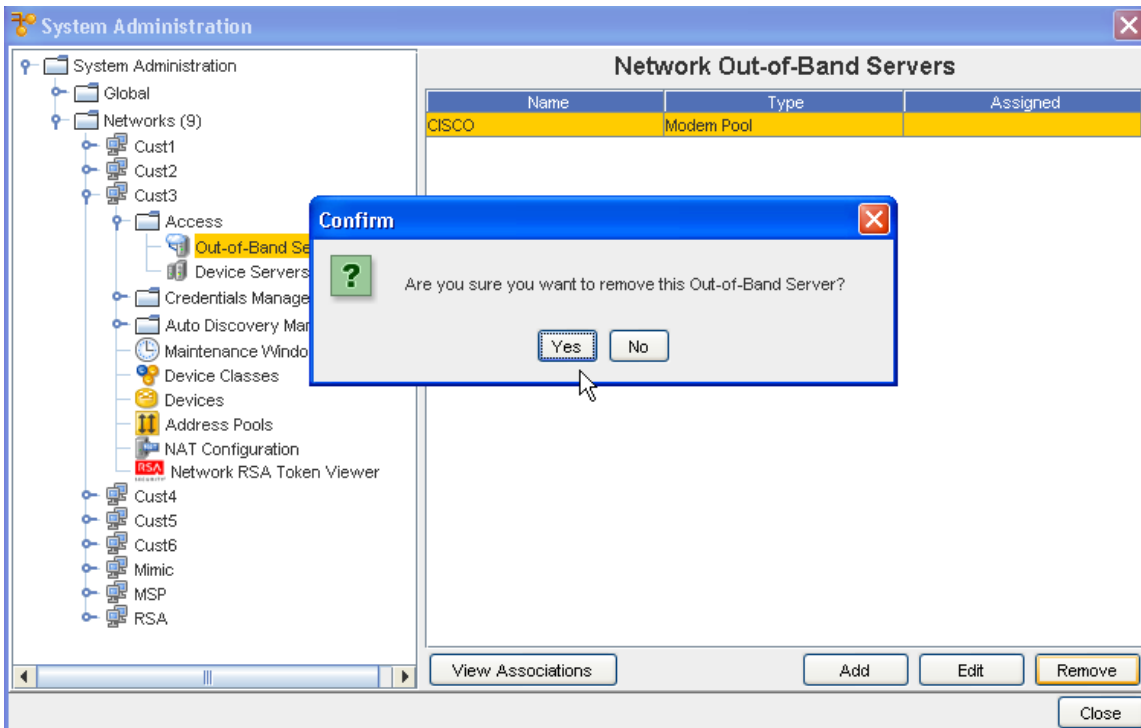
The Edit Out-of-Band Server window opens.

- 2 Make any changes needed to the existing information, then click **Ok**.

## Removing an Out-of-Band Server

To Remove an out-of-band set up at the network Level,

- 1 From the menu bar, access **Tools** -> **System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Networks** folder.
- 3 Double-click the **network name**.
- 4 Expand the **Access** folder.
- 5 Click the **Out-of-Band Servers** . The Network Out-of-Band Servers window opens in the right pane.



- 6 Select the server you want to remove, then click **Remove**.
- 7 Click **Yes** at the confirmation message.

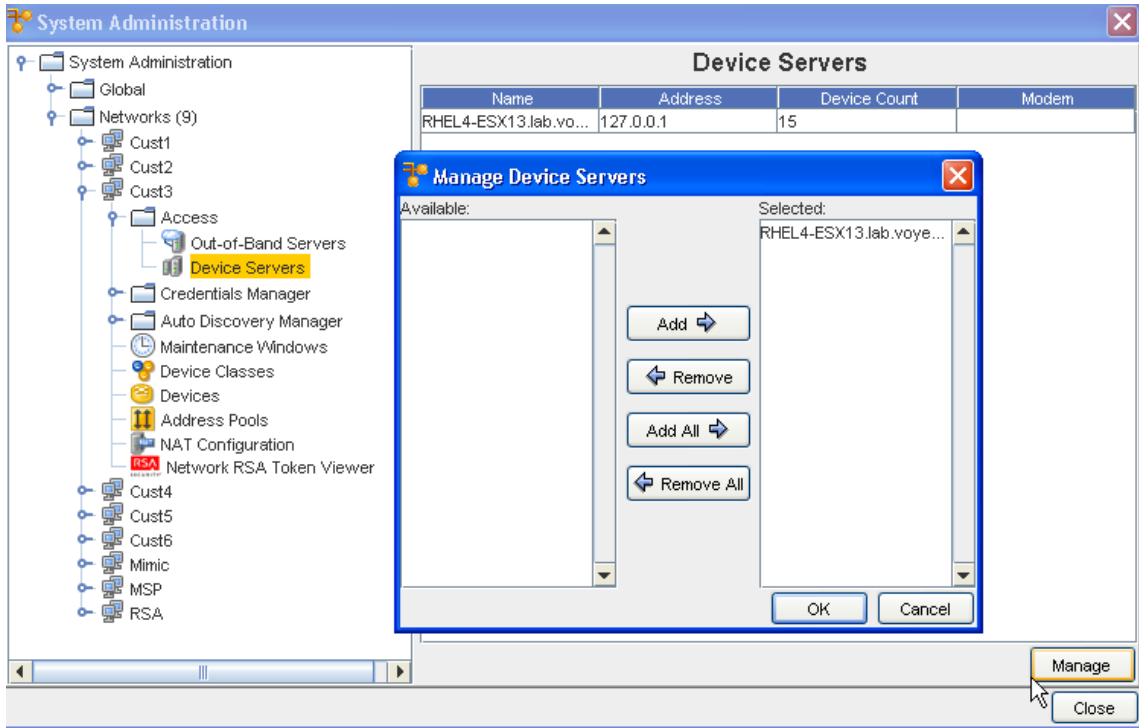
## Network - Device Servers

### Assigning Device Servers

Device Servers provide the control and communications or all network devices.

To assign a device server,

- 1 From the menu bar, access **Tools**.
- 2 From the menu options, select **System Administration**. The System Administration window opens.
- 3 On the tree menu, expand the **Networks -> Access** folders.
- 4 Open the **Device Servers** folder . At a minimum, at least one Device Server is available.



The basic properties of the Device Servers are listed on the right. Except for the number of the devices on the Device Server, these details can be edited on the Properties tab.

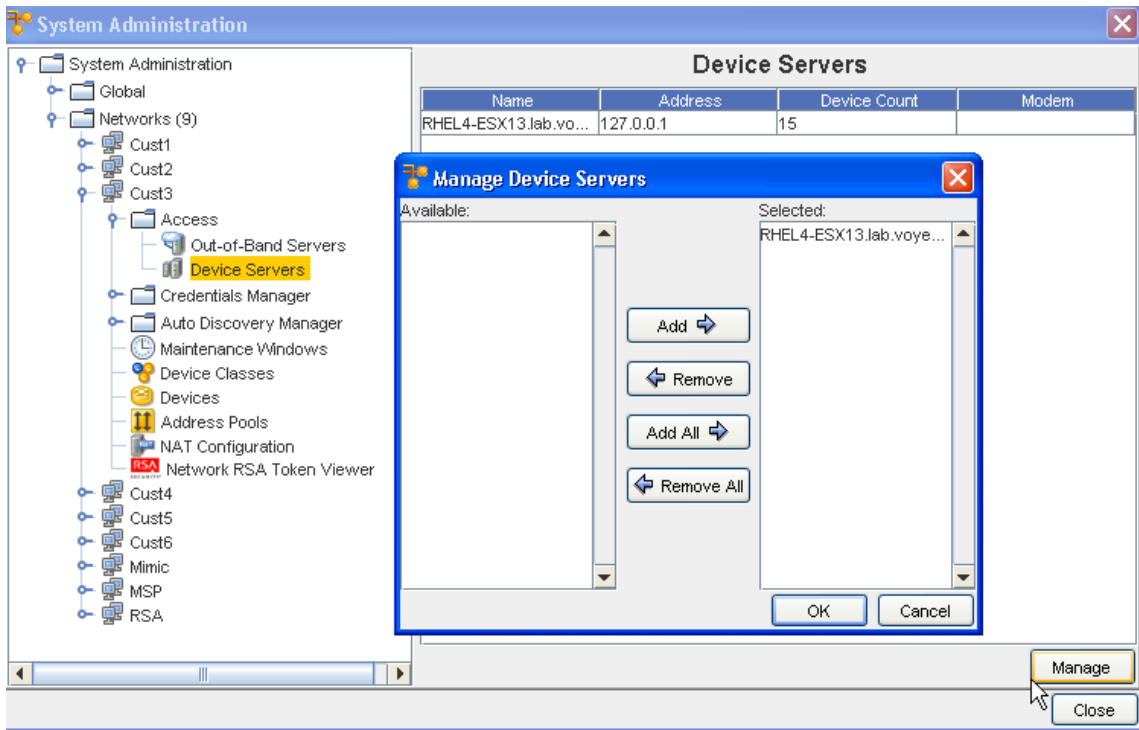
- To access the **Manage** feature, in the right pane, select a **Device Server**, then click **Manage**.
- Select at least one Device Server from the **Available** section, and move the selected servers into the **Selected** section. You can also remove unneeded servers back into the Available pane using the Remove buttons.
- Click **Ok** after moving the selected servers. Servers selected are now listed in the Device Servers window.

## Managing Network Devices

Once Networks are created, they need to have a device server associated to them. The device server is the *container* that holds the devices. You cannot complete an Auto Discovery until you have associated one or more device servers to a network. The device server to device relationship is set when creating an Auto Discovery job.

To associate device servers,

- From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- In the navigation pane, expand **Networks**. The current network list displays.
- Expand the network folder, then click **the network name**.
- Open the **Access** folder. The Access folder contains two options:



- Out-of-Band Servers
  - Device Servers
- 5 Click **Device Servers** . All device servers currently associated with the network display in the right pane.
  - 6 Click **Manage**. The Manage Device Servers window opens.  
The Manage Device Servers window has two columns:
    - Available - Contains device servers that can be associated with the network
    - Selected - Contains device servers that are currently associated with the network
  - 7 In the Available column, select a **device server**.
  - 8 Click **Add**. Or, to remove a device server from the Selected column, in the Selected column, select the **device server**.
  - 9 Click **Remove**. The device server is moved back to the Available column, and is no longer associated with the network. If needed, the device server can be re-associated at a later date.
  - 10 When finished, click **OK**. The Manage Device Servers window closes.  
The System Administration window now reflects the adjusted device servers list.

## Networks - Credentials Manager

### Credential Manager Overview

Credential management permits the secure abstraction of User ID and Password pairs from those who use them. There are four credential types; Account, Community String, SNMPV3, and Privilege Password. Account credentials can consist of a User ID/Password pair and a Privilege Password reference.

Bulk load utilities permit the mass association and change of credential to devices, or from device properties and the right-click menu.

Credential associations show the devices that are currently assigned to each credential.

Additional internal auditing enhancements are now available allowing a System Administrator more insight into who is accessing devices, and what tasks are being completed within the system.

- As the System Administrator, you now have a method of dynamically controlling the credentials used for any device operation, as well as being offered the flexibility to deal with special and exception scenarios to manage certain devices.
- As a System Administrator, you can now determine if credentials are to be governed by Global Credential Configuration settings, or allow Credential Configurations at the Network level to override the Global Configuration settings.

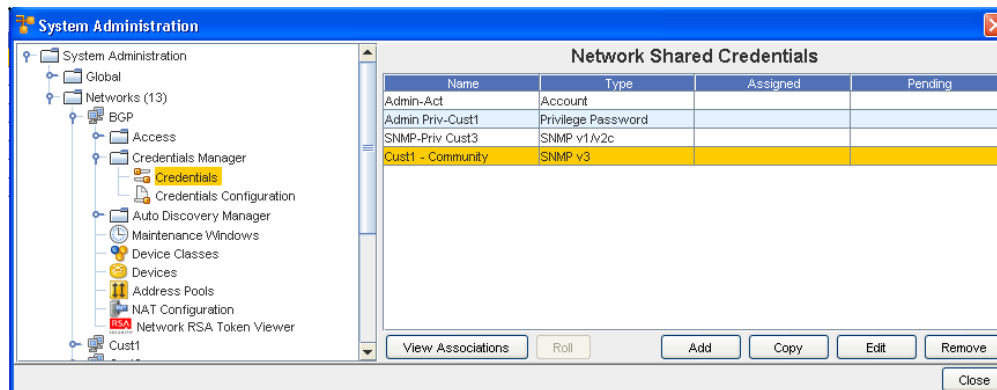
---

**Important** The Network credentials can override the Global configurations providing the user the ability to set Credential Policies for an individual Network.

---

The Credentials Manager has two options that you can view and work with:

- Credentials
- Credentials Configuration



From **Credentials** you can:

- View Associations
- Roll
- Add
- Copy
- Edit

- Remove

From **Credentials Configurations** you can select configuration options:

- Use Static Device Assignment
- Use Login Credentials
- Prompts User

## Credentials Best Practices

- Use credential management to specify how to secure your device communications.
- Use Credentials Configurations to determine the credentials that need to be used for communication with the devices.
- Manage credentials on a network or global basis, **not per device** . This allows you to make changes to a single credential, rather than make changes to each of many individual devices.
- If your Device Server and its devices are within a secured private network, then using unsecured protocols such as Telnet, FTP, and SNMP provides better overall performance and management ease, as well as better device coverage.
- If your Device Server and its devices are not within a single secured private network, then use credential management to disable non-secure protocols, and allow only secure protocols, such as SSH and SCP.

### When using SNMP Communications

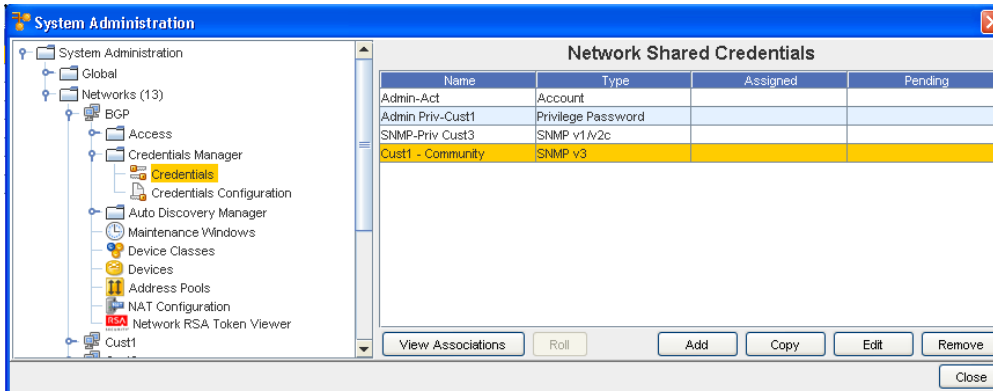
- Enabling SNMP communications provides the best overall quality of device information, with the greatest span of device coverage. The cost is a lower network security on traffic between the Device Servers and the monitored devices.
- Disabling SNMP communications gives you improved network security (by disabling non-secure SNMP traffic). The cost is having less device-specific information available, from a fewer number of device types. Information that is lost could include connection information, memory availability, and system information.

## Setting Network Level Credentials

To set credential access,

- 1 From the menu bar, access **Tools -> System Administration**.
- 2 In the navigation pane, select **Networks**.
- 3 Expand the Networks folder and select the appropriate **network**.
- 4 Expand the Network's folder, then select **Credentials Manager, and then Credentials** .

The Network Shared Credentials window appears similar to the following:

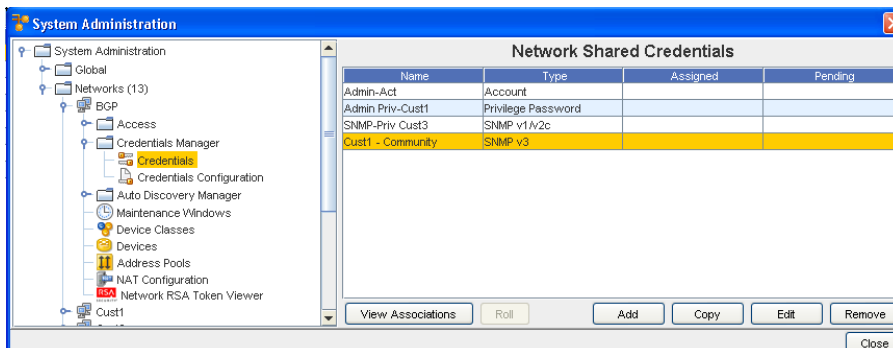


- 5 From here, you can **Add** a new credential, or if there are existing network credentials, you can complete the following actions:
  - [Viewing Network Credentials Associations](#) - to view the associations and review the Devices and the Auto Discovery information
  - [Rolling Credentials](#) - to go to the Roll Candidate Selection screen and select a candidate. Then go to the Credential Roll Job window to schedule the roll.
  - [Copying Network Shared Credentials](#) - to make an exact copy of this credential
  - [Adding Global Shared Credentials](#)- to add a credential
  - [Editing Network Credentials](#) - to make changes to existing information
  - [Remove Network Credentials](#) - to remove (delete) the credentials
  - **Close** - to leave this window

## Viewing Network Credentials Associations

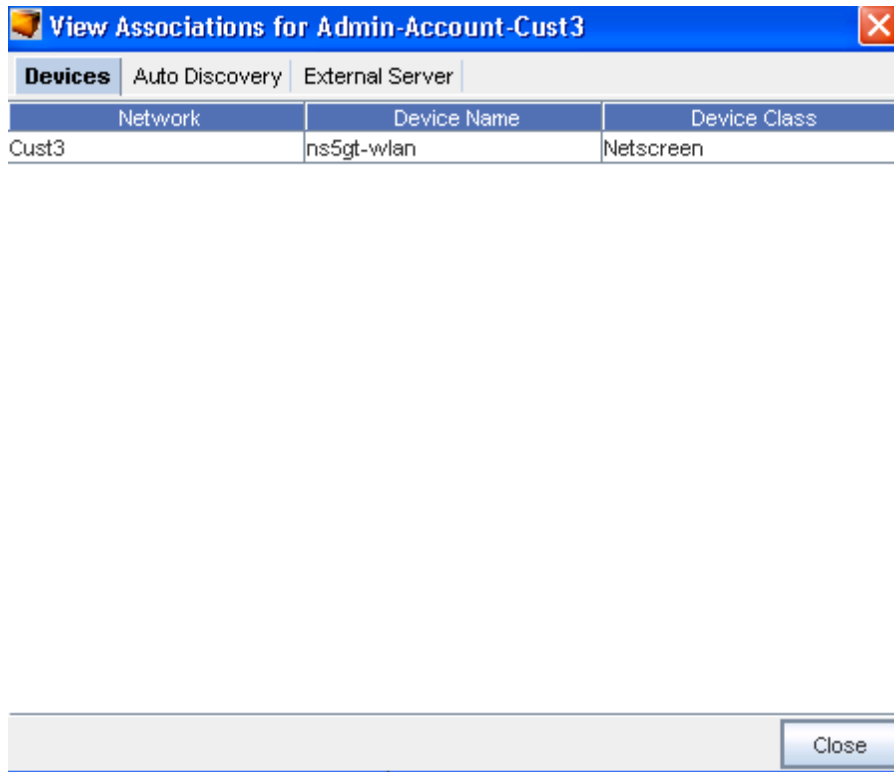
Credential management is provided at the Network level, as well as at the Global level. Network credentials are only available for devices within that specific Network. There is only one credential set used for a device, which can be associated from the list of Network or Global credentials. When assigning credentials, both Network and Global credentials are available in the credential window.

When using the **Network Shared Credentials** window, you can select to complete tasks using the option buttons located at the bottom of the window.



These options include **View Associations**, Roll, Add, Edit, Copy, Remove, and Close.

When you select to **View Associations**, you go to the View Associations window for the Name and Account you selected.



From this View Associations window you can see the:

- Network, Device and Device Class information for that account from the **Devices** tab
- Network, Name and Type from the **Auto Discovery** tab.
- Server Name and Server Type from the **External Server** tab.

**Note** After reviewing the information contained within each tab, click **Close** to close this window and return to the Network Shared Credential window.

## Rolling Credentials

To simplify account and password updates, credentials can be rolled within Network Configuration Manager. Rolling credentials updates all devices associated with one credential to the login and passwords on a second credential. You can roll credential information for devices, as well as create a job to update the devices configurations with the new login and password.

When using the **Network Shared Credentials** window, you can select to complete tasks using the option buttons located at the bottom of the window.

Using **Roll**, you can now:

- Select to roll from one credential to another credential



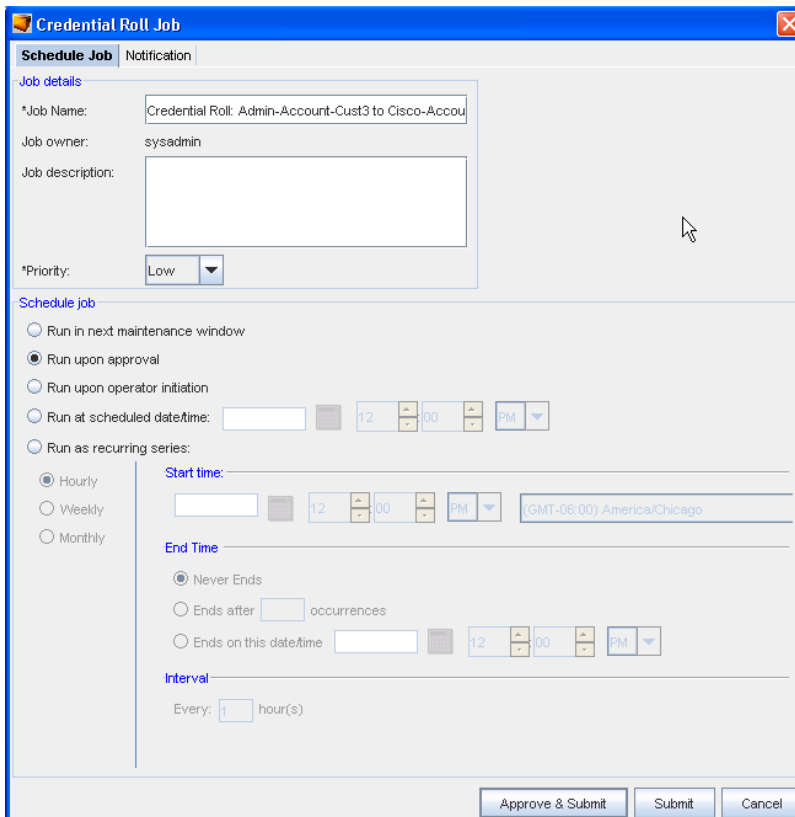
- Manage credentials on devices
- View a history of the credentials and their devices

These options include View Associations, **Roll**, Add, Edit, Remove and Close.

When you select **Roll**, you go to the Roll Candidate Selection, where you can select the Account you want to assign. Using Roll allows you to assign the Account before it is actually scheduled. Once scheduled, the status changes from Assigned to Pending until the scheduled job is run.

You can select to **Roll** from one credential to another credential.

- 1 Click the **Account** name (one or more) in the Roll Candidate Selection window to assign, then click **Ok**.
- 2 At the Credential Roll Job window, make your selections, and complete the information contained within the [Using the Schedule Tab](#) and [Using the Notification Tab to Send an Email](#) tabs. You must also complete and make selections in the **Schedule Job** section.



- 3 Click the appropriate action to **Approve and Submit** or **Submit**.

### Viewing the Credentials Roll Out Log

- 1 In a telnet window, verify your command results by entering change directory ( **cd** ) to **\$VOYENCE\_HOME / logs**, then pressing **Enter**. The log file to review is **credential-rollout.log**.

- 2 You can also go to the System Administrator **Credential** screen in Network Configuration Manager to verify that the credentials on the devices have been changed (rolled).

## Adding Network Shared Credentials

There are five classes of Shared Credentials:

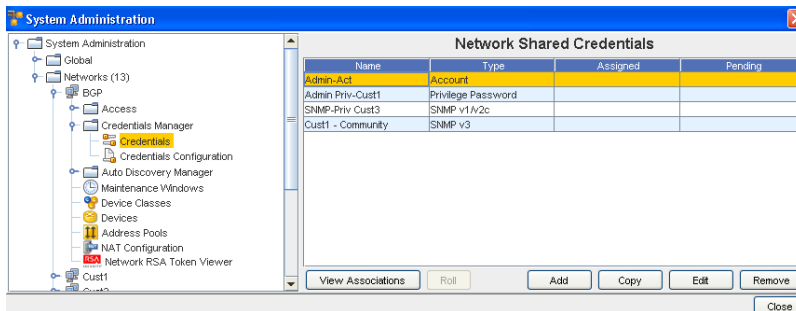
- Account
- Privilege password
- SNMP V1/V2c
- SNMP v3
- RSA

**Note** To import credentials in bulk, see [Using the Command Line Interface](#) for more information.

### Creating Shared Credential - Account Class

To Create a shared credential with the class type of Account, follow these steps:

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Credentials**.



The **Network Shared Credentials** window displays, with a listing of pre-assigned, shared credentials.

At the bottom of the window are the View Associations, Roll, Add, Copy, Edit, and Remove buttons, along with the Close option.

- 3 Click **Add** to display the Add Credential window.
- 4 Enter the **Credential Name** .

- From the **Credential Type** section, select **Account** type from the options shown (using the drop-down arrow to display your selection).

**Important** Depending on the credential type you select, additional information is displayed in the lower portion of the window. For example, when you select Account as the credential type, additional fields display where you enter information. See [Unique Credentials](#) for more

The screenshot shows the 'Add Credential' dialog box. The title bar is blue with the text 'Add Credential' and a close button. The main area is light gray and contains the following elements:

- \*Credential Name: [Text Input Field]
- Credential Type: [Dropdown Menu showing 'Account']
- Voyence Unique Credentials    Length: [Text Input Field]
- User Name: [Text Input Field]
- Password: [Text Input Field]
- Confirm Password: [Text Input Field]
- This account is managed by an external authentication server.
- Generate... [Button]
- OK [Button]    Cancel [Button]

information.

- Complete the following steps:
  - Enter the **User Name** .
  - Enter a **Password**. Confirm the Password.
  - Select the check box if this account is managed by an external authentication server.
- Click **OK** when you have completed these steps.

### Creating Shared Credential - Privilege Password Class

With the **Network Shared Credentials** window displayed showing a listing of pre-assigned, shared credentials:

- Click **Add** to display the Add Credential window.
- Enter the **Credential Name**.
- From the **Credential Type** section, select **Privilege Password** from the options shown (using the drop-down arrow). See [Unique Credentials](#) for more information.

- 4 Enter a **Password**. Confirm the Password you just entered. **Note:** You can also click the **Secure** check box, then click **Generate** to have the application generate a system-only-known password.
- 5 Click **OK** when you have completed these steps.

#### Creating Shared Credential - SNMP v1/v2c

With the **Network Shared Credentials** window displayed showing a listing of pre-assigned, shared credentials:

- 1 Click **Add** to display the Add Credential window.
- 2 Enter the **Credential Name**.
- 3 From the **Credential Type** section, select **SNMP v1/v2c** from the options shown (using the drop-down arrow). See [Unique Credentials](#) for more information.
- 4 Complete the following steps for the **Read-Only** section:
  - Enter the Community String.
  - Confirm the Community String entered.
- 5 Complete the following steps for the **Read-Write** section:
  - Enter the Community String.
  - Confirm the Community String entered.
- 6 Click **OK** when you have completed these steps.

**Add Credential**

\*Credential Name:

Credential Type: **SNMP v1/v2c**

Voyence Unique Credentials    Length:

**Read-Only**

\*Community String:

\*Confirm Community String:

**Read-Write**

Community String:

Confirm Community String:

### Creating Shared Credential - SNMP v3

With the **Network Shared Credentials** window displayed showing a listing of pre-assigned, shared credentials:

- 1 Click **Add** to display the Add Credential window.
- 2 Enter the **Credential Name**.
- 3 From the **Credential Type** section, select **SNMP v3** from the options shown (using the drop-down arrow). See [Unique Credentials](#) for more information.

The screenshot shows the 'Add Credential' dialog box with the following fields and options:

- \*Credential Name: [Text Input]
- Credential Type: **SNMP v3** (Dropdown)
- Voyence Unique Credentials Length: [Text Input]
- Security** Context (Tab)
- \*User Name: [Text Input]
- Security Level: **AUTH\_PRIV** (Dropdown)
- Authentication Protocol: **HMACMD5** (Dropdown)
- Privacy Protocol: **DES** (Dropdown)
- \*Authentication Password: [Text Input]
- \*Reenter Auth. Password: [Text Input]
- \*Privacy Password: [Text Input]
- \*Reenter Privacy Password: [Text Input]
- Generate... (Button)
- OK (Button) Cancel (Button)

When **SNMP v3** is selected as the Credential Type, the information you need to select and enter is divided between two tabs; **Security** and **Context**.

- From the **Security** tab, complete the following steps:
- Enter a User Name
- From the drop-down arrow, select Security Level. Depending on the Security Level you select, Authentication Protocol and Privacy Protocol may not be selectable.
- From the drop-down arrow, select a Authentication Protocol (if appropriate).
- From the drop-down arrow, select a Privacy Protocol (if appropriate).

---

**Note** You can select **AES192W3DESKEYExt** and **AES256W3DESKEYExt** protocols, only for the Cisco specific device(s).

---

- Enter an Authentication Password, then re-enter the password once again.
- Enter a Privacy Password, then re-enter the password once again. Note that you can click Generate to have Voyence create passwords for you.
- Once your passwords are verified, click **Ok**.

---

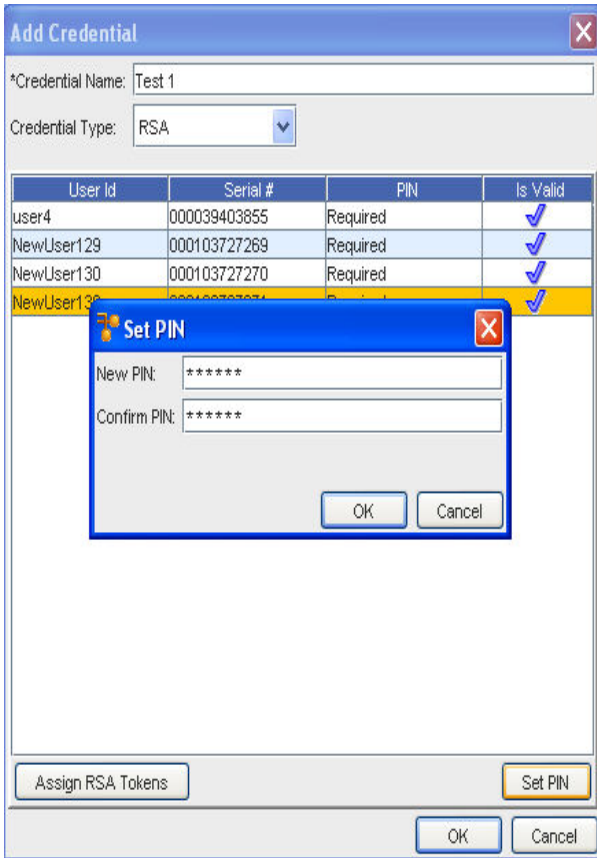
**Note** MIBs refer to **Management Information Bases** , and OIDs refer to **Object Identifiers** .

---

- From the **Context** tab, complete the following steps:
- Enter the Context Name.
- Enter the Context Engine ID.
- Enter a User Group Name.
- Enter a View Name.
- Select a View Access from the drop-down arrow.
- Enter the MIBs/OIDs you want included.
- Enter the MIBs/OIDs you want to be excluded from these credentials.
- Click **Ok** to keep your selections.

### Setting RSA Token PINs

- 1 From the list of RSA tokens, select an **RSA token**. RSA tokens that have not had the PIN set, show as Required under the PIN column.
- 2 At the bottom of the Manage RSA Tokens pane, select **Set PIN** . The Set PIN window (for the user you selected) now opens.



- 3 At the Set PIN screen, enter a **valid PIN** in the New PIN field.
- 4 Enter the PIN again in the **Confirm PIN** field.
- 5 Click **Ok**.

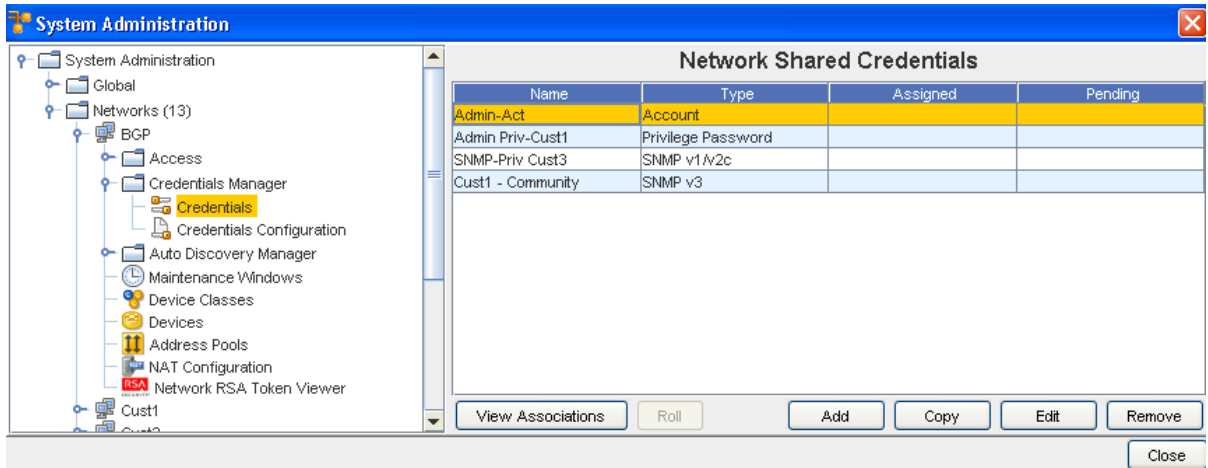
## Copying Network Shared Credentials

### Creating Shared Credential - Account Class

To Copy a shared credential with the class type of Account, follow these steps:

- 1 From the menu bar, select **Tools -> System Administration**.

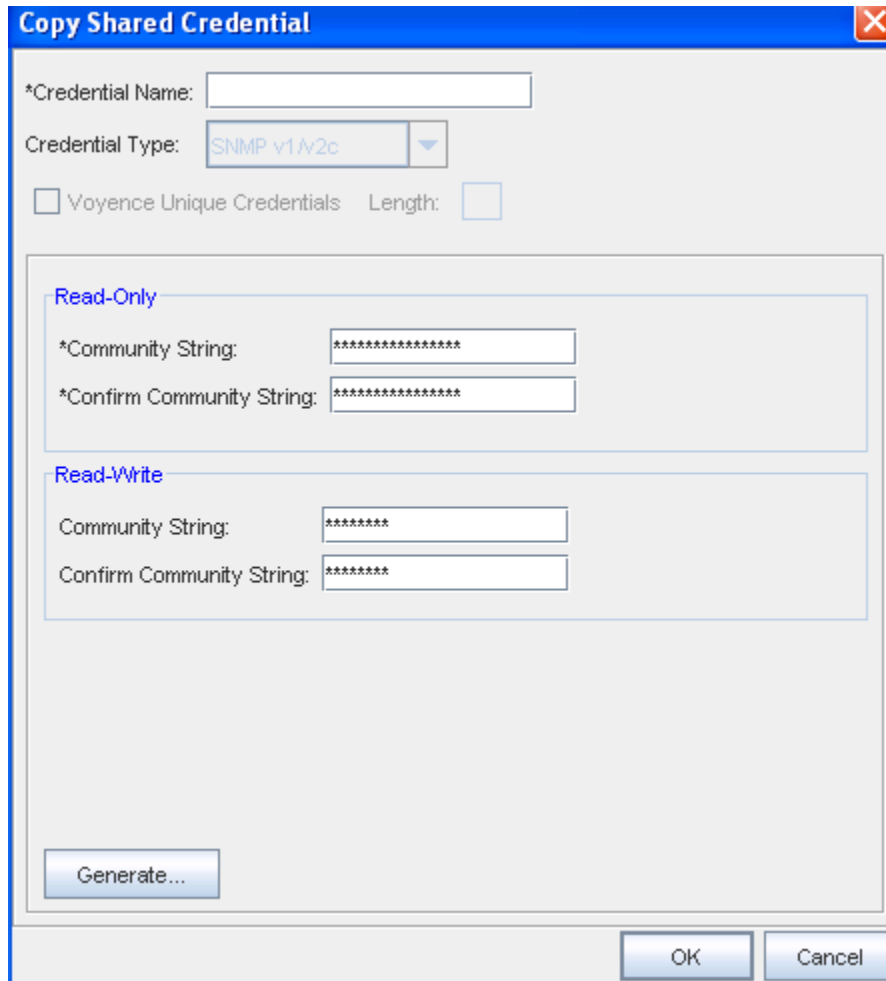




The **Network** Shared Credentials window displays, with a listing of pre-assigned, shared credentials.

At the bottom of the window are the View Associations, Roll, Add, Copy, Edit, and Remove buttons, along with the Close option.

- 2 Click **Copy** to display the Copy Credential window.
- 3 Enter the **Credential Name** .
- 4 Click **Ok**. Now, the copy of the Credential you selected is now in the list of Network Shared Credentials.



**Copy Shared Credential**

\*Credential Name:

Credential Type:

Voyage Unique Credentials Length:

**Read-Only**

\*Community String:

\*Confirm Community String:

**Read-Write**

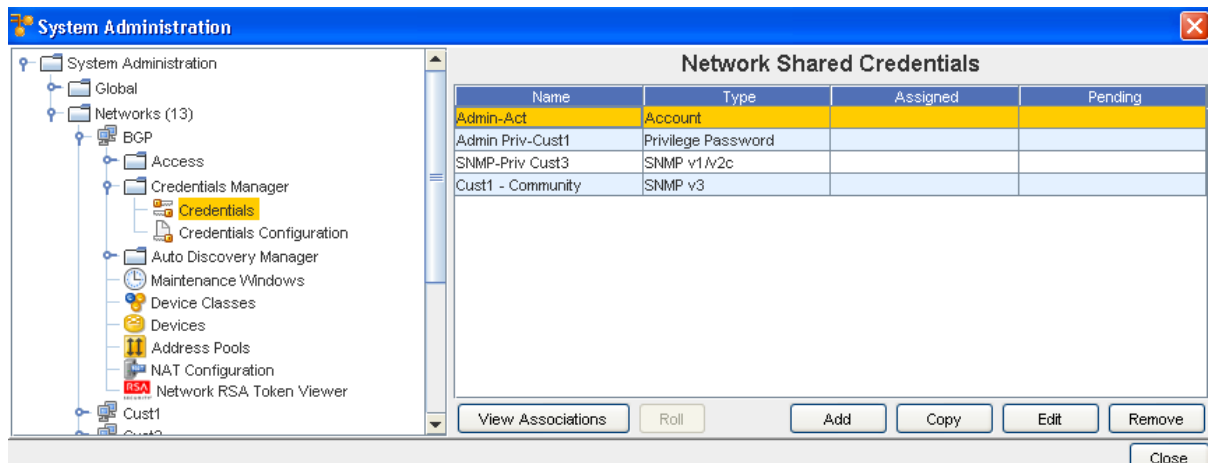
Community String:

Confirm Community String:

## Editing Network Credentials

To edit Network Shared Credentials,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Credentials**.



**System Administration**

**Network Shared Credentials**

Name	Type	Assigned	Pending
Admin-Act	Account		
Admin-Priv-Cust1	Privilege Password		
SNMP-Priv-Cust3	SNMP v1/v2c		
Cust1 - Community	SNMP v3		

The **Network Shared Credentials** window displays, with a listing of pre-assigned, shared credentials.

- 3 Select a credential from the list, then click **Edit** to display the Edit Shared Credential window.
- 4 Make any changes to the existing information, based on the Credential Type you selected when you created the credential.
- 5 Click **OK** to save your edits.

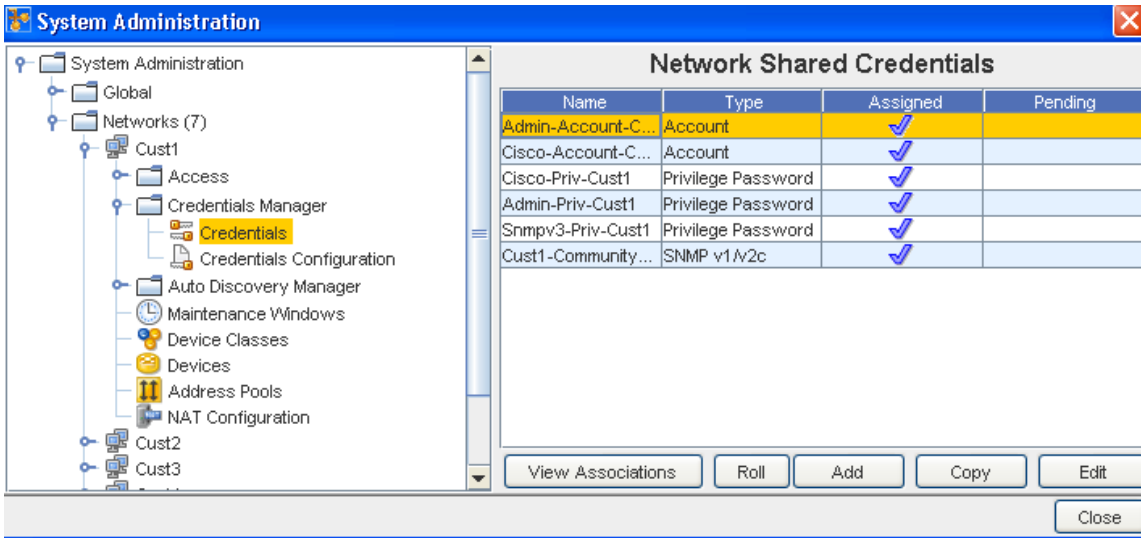
#### Notes:

- The updating credentials process requires that an account be associated with a device. This account is used to establish the initial session into the device to make the credential updates.
- This manual process creates an association with the credential and the local device to represent the username/password that is present on the device.
- If an Autodiscovery is made with an established account credential, the manual process of association is not required. The Communication tab on a device contains the account association for the Primary In-Band mechanism.

## Removing Network Credentials

To remove Network Shared Credentials,

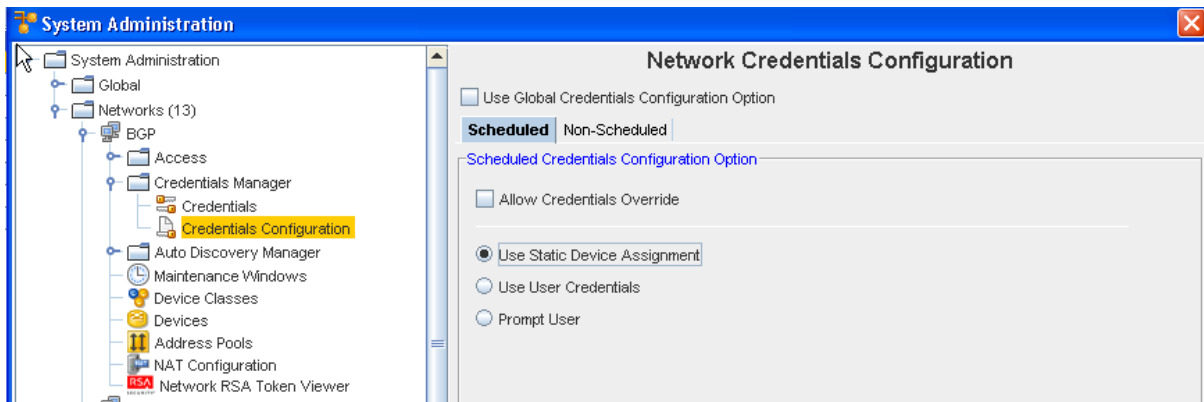
- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Credentials**. The **Network Shared Credentials** window displays, with a listing of pre-assigned, shared credentials.



- 3 Select the network credential you want to remove from the list.
- 4 Next, click **Remove**.
- 5 At the confirmation message, click **Yes** to remove this network shared credential.

## Using Network Credentials Configuration

Access to the Credentials Configuration is through the **Credentials Manager** .



## At the Network Credentials Configuration Level

At this level, you are provided the options to determine the credentials that need to be used for communication with the device. This includes scheduled jobs, as well as synchronous operations targeted on a device, such as cut-through, quick commands, and more.

- The **Scheduled** tab refers to the jobs that can be scheduled to run (with the exception of Auto Discovery and Pulls).
- The **Non-Scheduled** tab refers to those operations (Cut-Through, Quick Commands, and Save Commands, for example) that are not scheduled.

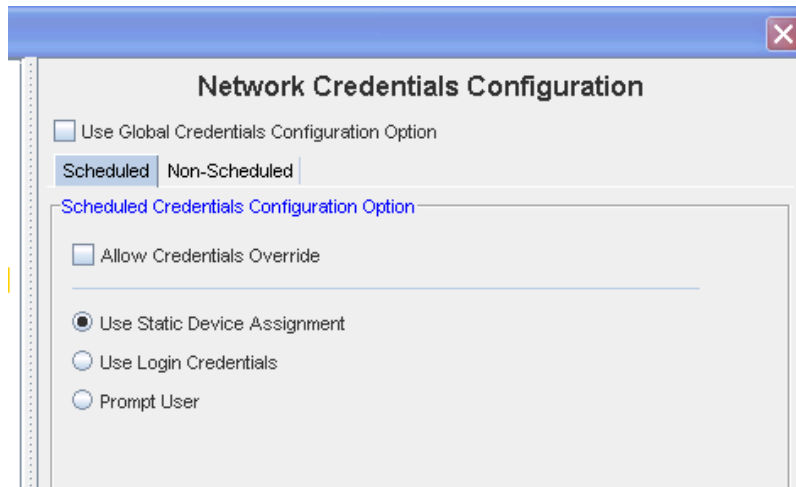
When the **Use Global Credentials Configuration Option** is not selected, your options can be selected from the Scheduled and Non Scheduled tabs. If selected, there are no other options available to you from these tabs.

You can select from the following options:

### The Scheduled Tab

#### Users Static Device Assignment

- **Uses Static Device Assignment** - If Uses Static Device Assignment is selected- this indicates to the system to use the Shared Credentials assigned at the device level within a network. This is the default option.

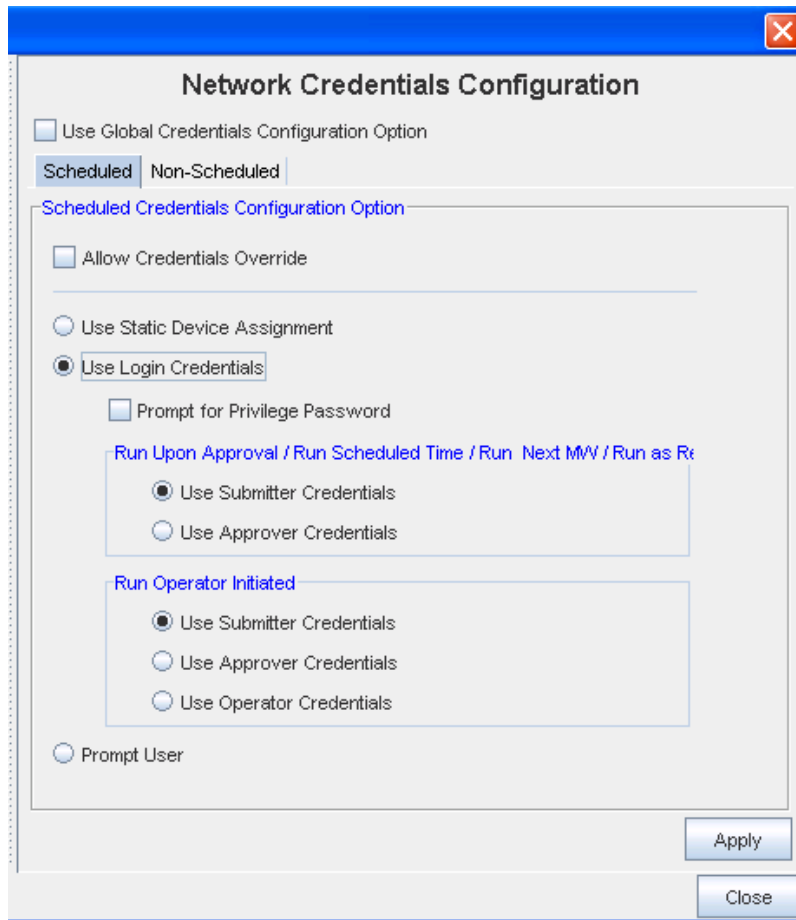


#### Use Login Credentials

- **Use Login Credentials** - When **Use Login Credentials** is selected - this indicates to the system to use the user's application login account as the device credentials (the account name/account password).

You have the choice to select any of the options of when the user's are now prompted to enter account and password information before completing tasks.

- You can select to **Use the Global Credentials Configuration Option**
- You can also select to **Allow Credentials Override**



**Important** In some cases where a job may be scheduled in the future, the user's login credentials may need to be preserved until the job executes (to construct the device server request). These credentials must be discarded immediately after the task request is sent to the device server. You must pay attention to jobs with "Preserve Order" selected, as each task execution depends on the success of the previous task in the list (the credentials must be preserved until the last task executes).

- You can select to **Prompt for Privilege Password**

To determine whose credentials are to be used for jobs, the following options are available for each run option as applicable, **one** of which must be selected:

- **Use Submitter Credentials** – In case of scheduled operations, the system uses the submitter's credentials. This includes any job submission through "Submit" button on the scheduler.
- **Use Approver Credentials** – In case of jobs, the system uses the approver's credentials. This includes any job submission through –Approve&Submit– button on the scheduler or the "Approve" icon on the Schedule Manager.
- **Use Operator Credentials** (in case of jobs whose run option is "Run Operator Initiated") – In case of jobs, the system uses the credentials of the user attempting to manually execute the job.

In case of non-scheduled operations, the login credentials of the user executing the operation will be used and above options are redundant.

If Prompt User is selected from this window , see the following information.

### Prompt User

- **Prompts User** - When Prompts User is selected - this indicates to the system that the user is to be prompted for the credentials before the device operation , based on the following options: Account Password, and Privilege Password.

To determine whose prompts are to be used for jobs, the following options are available for each run option as applicable, **one** of which must be selected:

- Run on Approval
- Prompts on Submit - Prompts at the time the job is submitted for "Pending Approval"
- Prompts on Approval - Prompts at the time the job is Approved
- Run Operator Initiated
- Prompts on Submit - Prompts at the time the job is submitted for "Pending Approval"

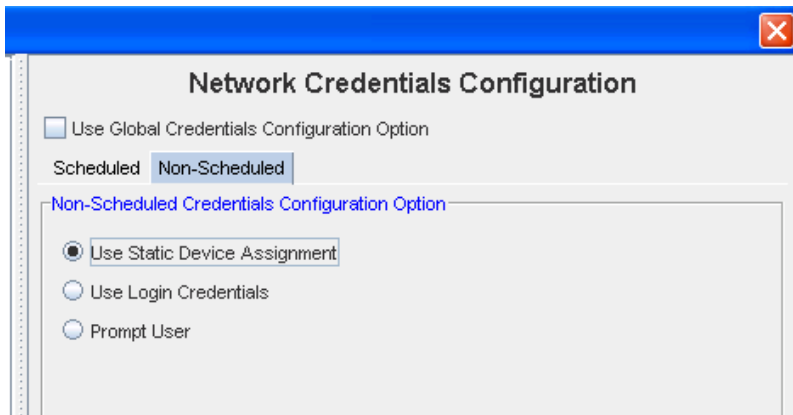
- Prompts on Approve - Prompts at the time the job is Approved
- Prompts on Manual Execute - Prompts at the time the job is manually executed.
- Run Scheduled Time / Run Next MW / Run as Recurring Series
- Prompts on Submit - Prompts at the time the job is submitted for "Pending Approval"
- Prompts on Approval - Prompts at the time the job is Approved

**Note** You also have the option of selecting **Invalidate Credentials on Job Modification** . If this is selected, after a job is **edited**, any credential associated with that job is now invalid.

- 1 After making your selections from the various options, click **Apply** to apply your credential choices.
- 2 Read the system message carefully to fully understand your selection to apply the changes you have made, then select **Yes to Continue**.
- 3 If applicable, click **Yes** at the Confirmation message.

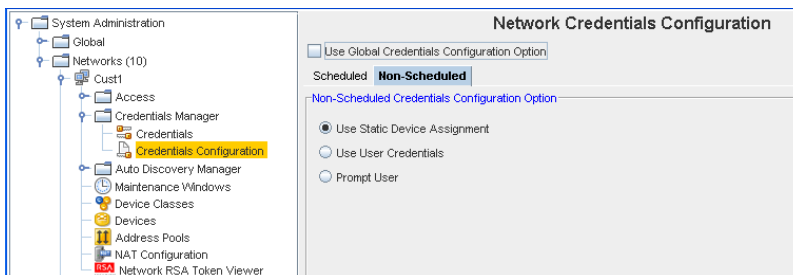
### The Non-Scheduled Tab

The **Non-Scheduled** tab refers to those operations (Cut-Through, Quick Commands, and Save Commands, for example) that are not scheduled to run.



### Users Static Device Assignment

- **Uses Static Device Assignment** - If Uses Static Device Assignment is selected- this indicates to the system to use the Network Shared Credentials assigned at the device level within a network. This is the default option.



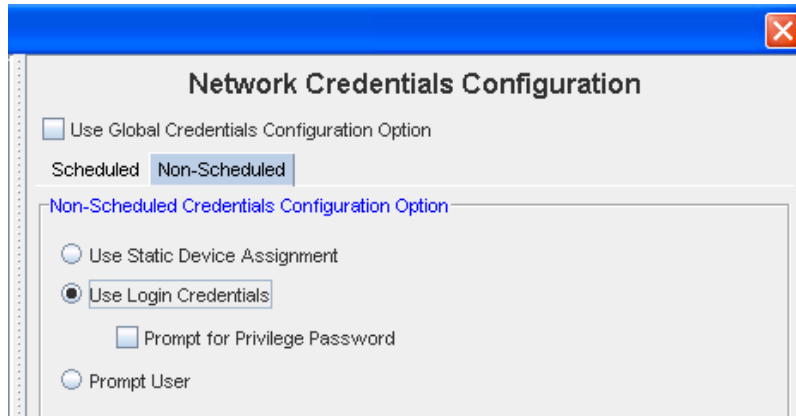


## Use Login Credentials

- **Use Login Credentials** - When **Use Login Credentials** is selected - this indicates to the system to use the user's application login account as the device credentials (the account name/account password).

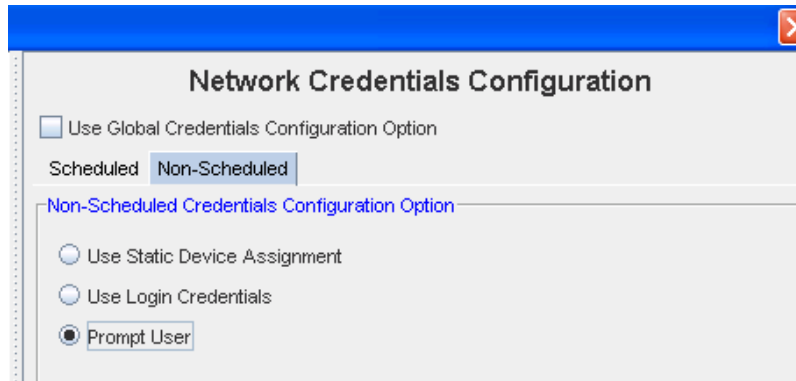
You can select to have the user prompted for their **Privilege Password** information before completing tasks.

- You can also select **Prompt User** from this window.



## Prompt User

**Prompt User** - When **Prompt User** is selected - this indicates to the system that the user is to be prompted for the credentials before the device operation , based on the following options: Account Password, and Privilege Password.



## Auto Discovery Manager

### Auto Discovery Overview

Network Configuration Manager has a robust Auto-Discovery capability which can find the devices on a network, categorize them, and determine the communication methods available for management of the devices.

Before your network devices can be managed in Network Configuration Manager they must first be discovered. The process by which devices are entered into the application for management is known as **Auto Discovery**. Auto Discovery associates network devices with a Network Configuration Manager device server and your networks.

- Auto Discovery jobs can be created and scheduled by System and Network Administrators, and are associated with individual networks.
- Jobs are maintained under the **Network** folder in the System Administration module. Each network has its own Auto Discovery module.
- If you have more than one network configured in Network Configuration Manager, Auto Discovery should be scheduled for each network.
- Auto Discovery can be set to run on a scheduled cycle, eliminating the need to "remember" to run Auto Discovery.
- Auto Discovery uses the Schedule Manager to push scheduled Auto Discovery jobs to the networks. Scheduling allows Auto Discovery to run at the best time, based on your network's requirements.
- Only devices in the *IP range* of an Auto Discovery job are attempted to be discovered. When a device is discovered, Network Configuration Manager identifies its device type, based on the supported device types within the system.
- If the device is **not** one of the types listed as significant in the Auto-Managed devices window, the device is ignored.
- Only devices with IPs in the include range of an Auto Discovery job that are of a device type listed in Auto-Managed Devices, will be managed into the network.

---

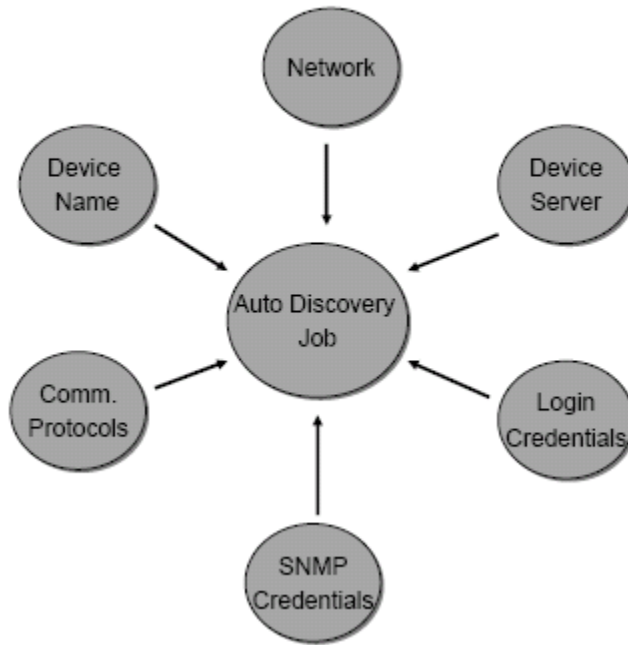
**Important** Auto discovery jobs cannot be created until at least *one device server* is associated with the network

---

### Auto Discovery Associations

The following graphic displays the associations with Auto Discovery

## Networks – Auto Discovery Associations



### Detecting Duplicates

Voyence uses a **"2 out of 3 rule"** to determine if a discovered device is new. The three items tested are:

- SysObjectID
- IP address
- Name or Serial Number

Depending on the device class of the device the "name" is the HostName, SysName, or serial number of the device.

The device server compares the found "Name" with its internal database of managed devices. If there are no matches, the device server compares the discovered IP address with the list of IP addresses in its internal database.

---

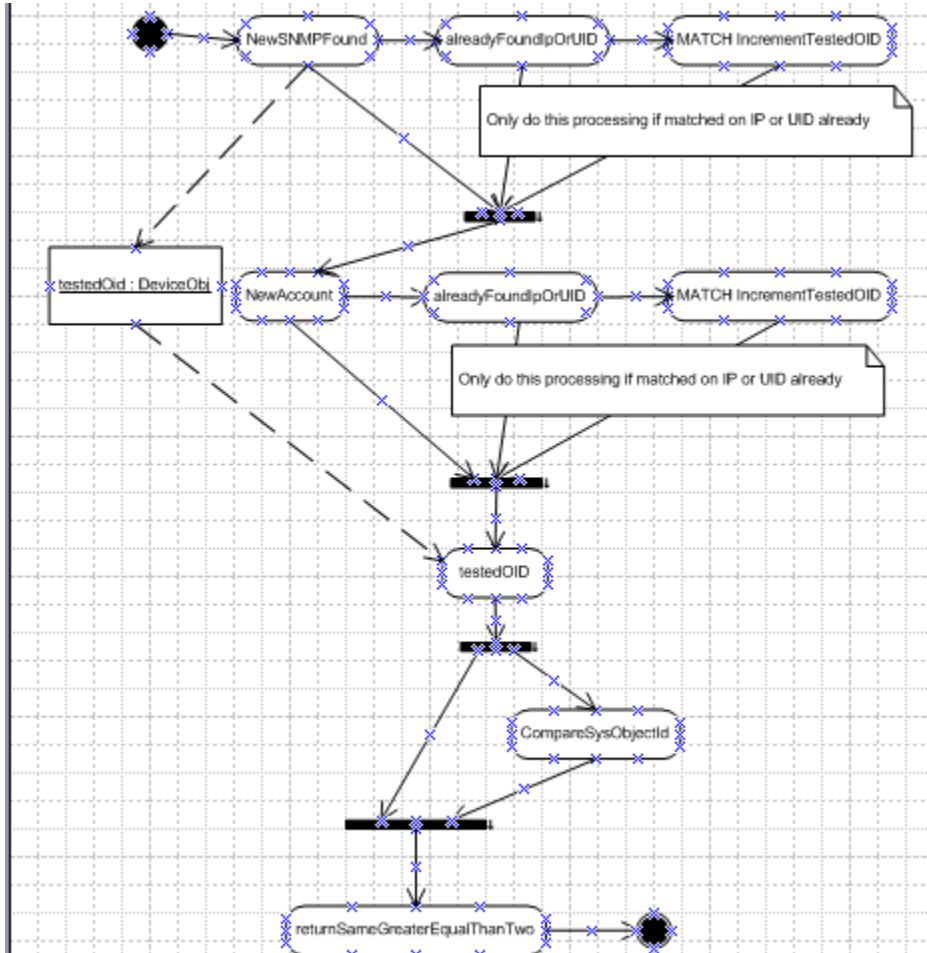
**Note** The internal database on the device server includes all the IP addresses for the devices it is managing, not just the management addresses. This ensures that a device is not just discovered via another interface.

---

If either the device name or the IP address is matched to a device in the internal database, the system compares the discovered SysObjectID with the SysObjectID of the matched device.

If these are a match, it is assumed that the discovered device is a duplicate, and it is assigned the matched device's IDX. If the SysObjectID's do not match, but both the device name AND IP addresses match, the device is assumed to be a duplicate, and is assigned the matching devices IDX.

If none of the three (or only one of the three) items match an existing device, the device is assumed to be a new device, and the device server assigns a new IDX number to the device.



### Auto Discovery Job Types

There are **three types** of auto discovery jobs that can be run on a network:


- Ping Sweep
- SNMP Sweep

- Multi-hop Discover
- **Ping-Sweep** – Takes a range of IPs. Pings each device twice to see if the device is active, then runs an SNMP-Sweep on each of the responding devices.
- **SNMP-Sweep** – Takes a range of IPs. (Note that SNMP's are not needed to discover Cisco devices.) This SNMP Sweep discovery type takes a range of IPs and attempts to discover each device IP. It uses an SNMP query first. If the SNMP string is incorrect, or the device just does not respond, it also attempts to login to the device, and try to discover it with account information.
- **Multi-hop Discover** – Takes the IP of a core seed router and a range. Pulls route and arp table information from the seed router, takes each IP in this list, and repeats the process until it exhausts the list of unique IPs in the range. A heavy load can be seen on routers in large networks, so this discovery type should not be used except as last resort in environments where users have no of what exists in their network.

Depending on the type of auto Discovery completed, details must be entered defining the Auto Discovery job. These details are located on four tabs.

- Properties
- Seed Addresses
- Ranges
- Credentials

---

**Note**  Do not use SNMP v3 Credentials for Auto Discovery if you have PIXes.

The Seed Addresses tab is only available when running a Multi-hop discovery.

---

Once devices are located, they are placed into the Auto Discovered network as managed devices, and system jobs are run in the scheduler to pull the configurations and hardware specs for the new devices.

Although devices enter a network as managed, they can be reclassified. The three device classifications available in Network Configuration Manager are:

<b>Managed</b>	Indicates devices that are associated with networks. Managed devices reside in the central repository, and are under the control of authorized network users.
<b>Unmanaged</b>	Indicates devices that have been discovered, but are not managed by a network and flagged, so that they are not rediscovered in subsequent Auto Discovery runs. All revision history about a device is lost when it is placed into an <i>unmanaged</i> state.
<b>Unclassified</b>	When a device is removed from all networks, it's state is changed to Unclassified. Unclassified devices cannot be managed until placed back into a network. The device retains all revision history while in an unclassified state.

---

## Creating Auto Discovery Jobs

Devices are associated with a Network through the Auto Discovery process. The Network Configuration Manager Auto Discovery mechanism offers three Auto Discovery options; Multi-Hop, Ping Sweep, and SNMP Sweep. Depending on the type of Auto Discovery selected, details must be entered into the four tabs.

Creating an Auto Discovery job is a multi-step process. Depending on the Auto Discovery type, you must provide details on the following tabs:

- Properties
- Seed Addresses
- Ranges
- Credentials (Common Strings, Accounts, and Privilege Passwords)

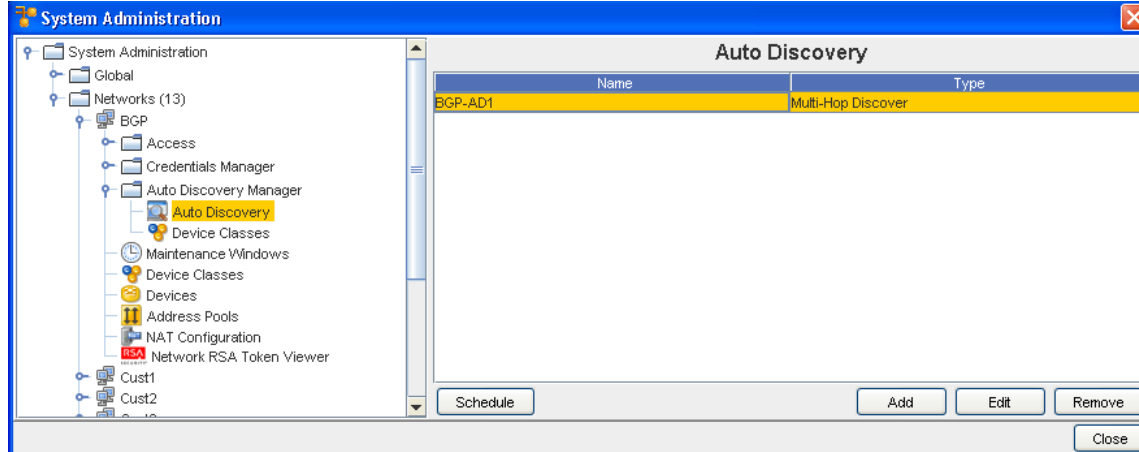
---

**Important** If insufficient details are entered on any tab, the Auto Discovery job may fail, or the job may not run completely.

---

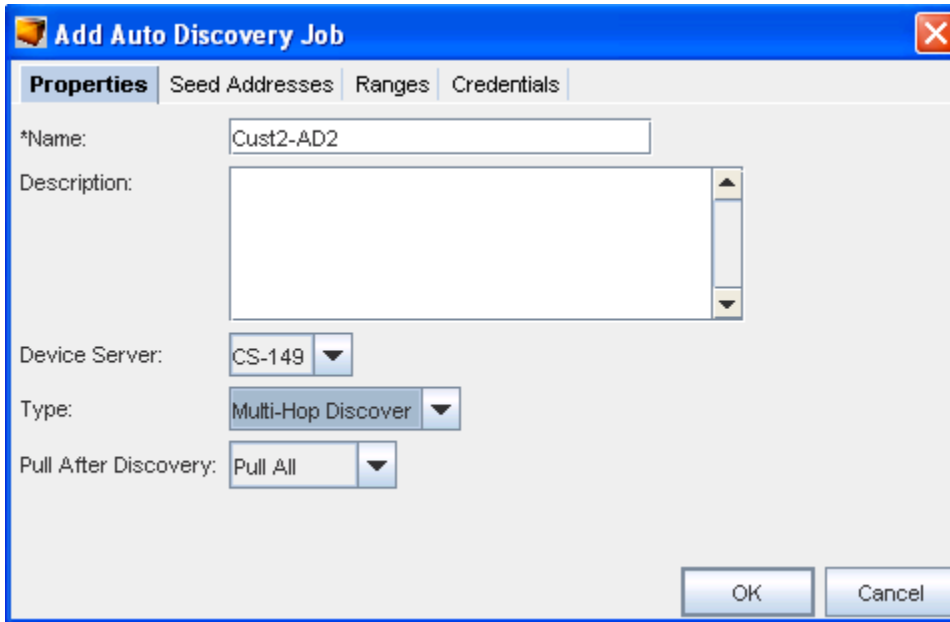
To create an Auto Discovery job,

- 1 From the menu bar, select **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Networks folder**.
- 3 Click **Auto Discovery**.



- The right pane populates with any Auto Discovery jobs that have already been setup.
- The Schedule, Add, Edit, and Remove buttons are all selectable in the window (when a device is selected, Prior to select the Add button is the only button selectable).
- Click **Add**. The Add Auto Discovery Job window opens.
- To define the Auto Discovery job, you must enter details in each of the following tabs:
  - Properties
  - Seed Addresses

- Ranges
- Credentials



Properties Tab

Seed Addresses Tab

Ranges Tab

Credentials Tab

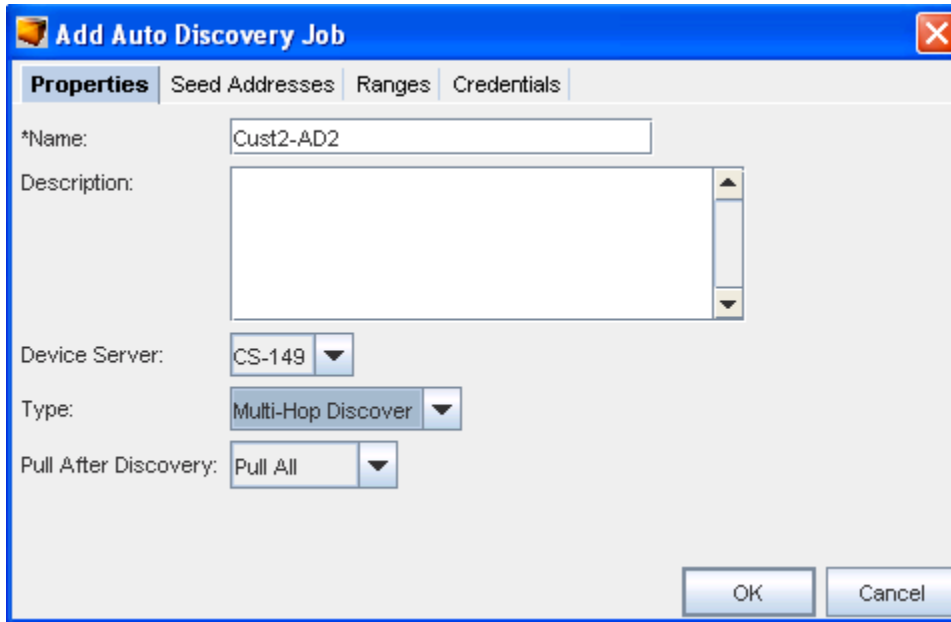
Editing Auto Discovery Jobs

Removing Auto Discovery Jobs

### Properties Tab

The **Properties** tab in Auto Discovery is the first tab you must complete. The Properties tab contains the basic description and type of Auto Discovery being run. You can also select the Pull After Discovery action.

The following fields are available.



Field	Description
Name	This field populates with an auto-generated name that can be edited.
Description	Descriptive summary of the Auto Discovery
Device Server	Contains the name of the Device Server
Type	Options include: Ping Sweep, SNMP Sweep, Multi-Hop Discover.
Pull After Discovery	Options include: Do not Pull, Pull Configs, and Pull All.

- 1 Type in a **Name** for the Auto Discovery job.
- 2 Optionally, enter a **Description**.
- 3 Select a **Device Server** from the drop-down listing.
- 4 Select a **Type** from the drop-down listing.
- 5 Make a selection from the **Pull After Discovery** drop-down listing.
- 6 Proceed to the next tab, **Seed Addresses**, or **Ranges**.

---

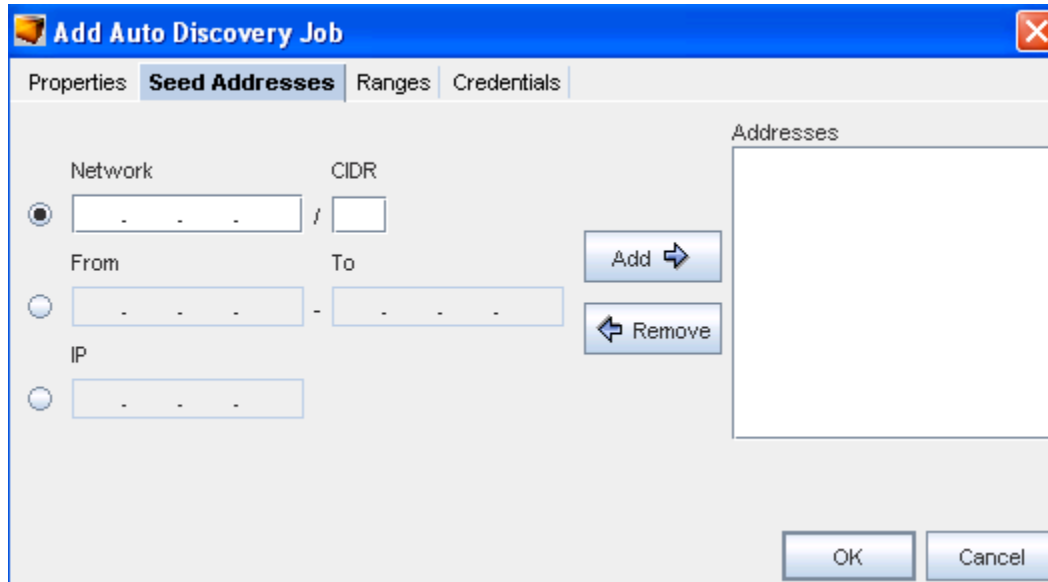
**Important** You can only continue on to the Seed Addresses if **Multi-hop** is selected in **Properties**. For all other selections, you do not have access to the Seed Addresses tab.

---

### Seed Addresses Tab

The **Seed Addresses** tab is only available when a **Multi-Hop Discover** job type is being completed. Seed Addresses are primer addresses to Network devices to be managed.





Seed addresses are portals to network devices that can be managed. This tab allows you to modify the seed addresses that are used during Auto Discovery.

The following fields are available:

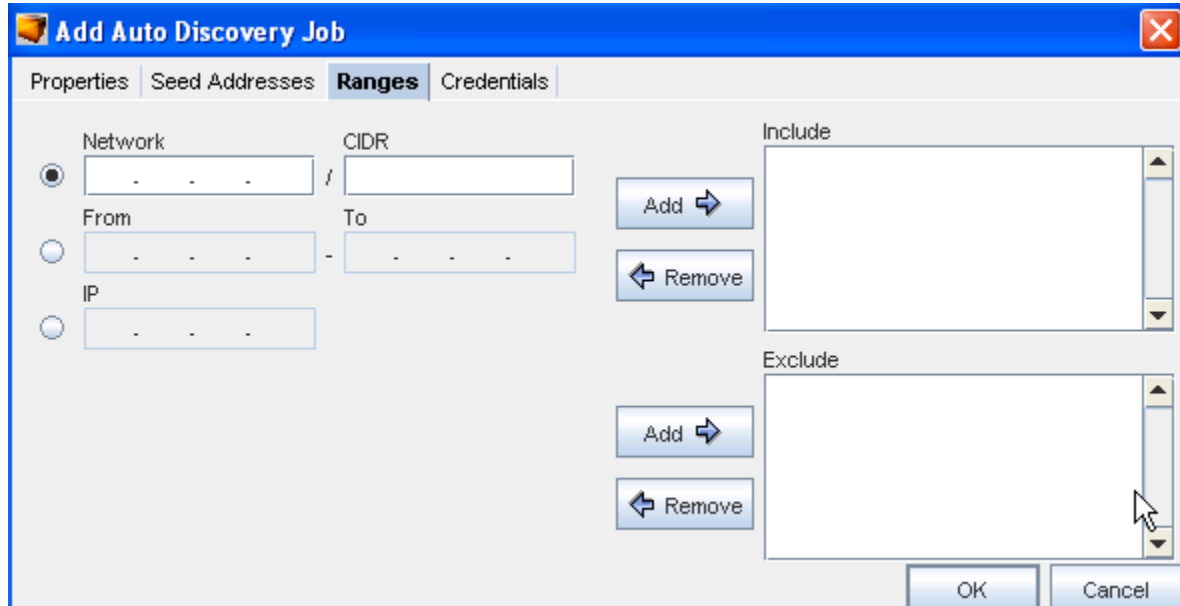
Field	Description
Network/CIDR	A single network subnet -default selection
From/To	Allows you to enter a span of addresses. You can then Add or Remove the content within the Addresses box.
IP	A single IP Address
Addresses	Contains all Seed Address types that have been entered. This list can be modified as needed, using the Add and Remove buttons.

- Complete **one or more** of the following:
- Enter a **Network/CIDR**. Note that, the CIDR number must be less than or equal to 32.
- Enter a **From/To IP address range**.
- **E nter a single IP Address**.
- Click **Add**. The addresses are now included in the Addresses box.
- Repeat the above steps until all the Seed Addresses are entered. Note that you can remove any exiting addresses using the **Remove** button, if needed.
- Proceed to the next tab. See **Ranges**.

### Ranges Tab

The **Ranges** tab allows you to enter ranges of IP addresses that are to **included** or **excluded** during Auto Discovery. IP addresses not included are ignored during Auto Discovery. IP Addresses located in the Excluded field are addresses within the included IP address ranges that should be ignored during Auto Discovery.

The Included and Excluded ranges can be modified as needed.



The following fields are available:

Field	Description
Network/CIDR	A single network subnet. Default selection
From/To	Allows you to enter a span of addresses
IP	A single IP address
Include	To include the first of IP Ranges that are included during the Auto Discovery
Exclude	To exclude the first of IP Ranges that are excluded during the Auto Discovery

To Include ranges,

- 1 Complete one or more of the following:
  - Enter a **Network/CIDR**
  - Enter a **From/To IP address range**
  - Enter a single **IP address**
- 2 Click **Add ->** in the **Include** section. The address are added to the Addresses column.
- 3 Repeat **steps 1 and 2** until all IP addresses needing to be included are added.

- 4 To remove included IP Addresses in the Include field, select the **IP Address**, then click **Remove**.

**Result:** The address is removed from the Include column. If the address need to be included in the future, it must be re-entered.

To Exclude ranges,

- 1 Complete one or more of the following:
  - Enter a Network/CIDR.
  - Enter a From/To IP address range.
  - Enter a single IP address .
- 2 Click **Add** -> in the Exclude section. The address are added to the Addresses column.
- 3 Repeat **steps 1 and 2** until all IP addresses that need to be excluded are added.
- 4 To remove excluded IP Addresses in the Exclude field, select the **IP Address**.
- 5 Click **Exclude**. The address is removed from the Exclude column.
- 6 Click **OK** when you have completed excluding ranges.
- 7 **Proceed to the next tab.**

[Auto Discovery Overview.](#)

[Seed Addresses Tab.](#)

## Credentials Tab

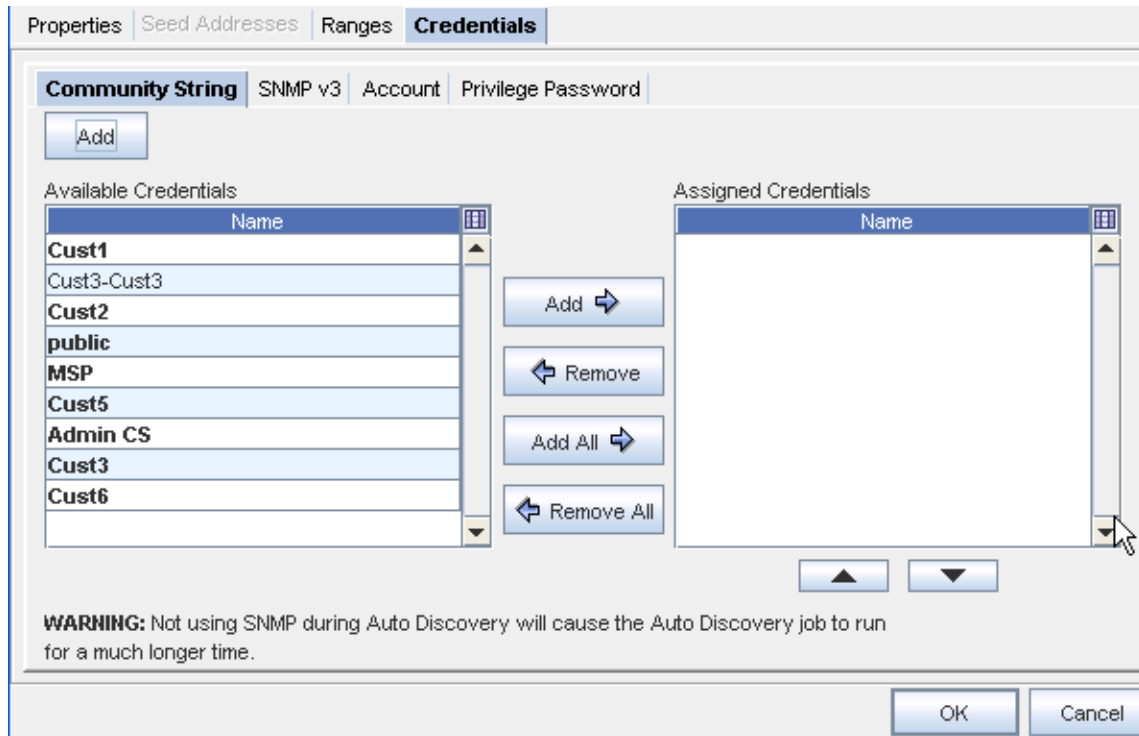
**Global credentials** appear in bold. Network credentials are plain text.

Auto Discovery uses your device class preferences to determine how to discover devices into your Network. Bulk Import utilities can also be used to trigger Auto Discovery or populate the device database.

Network Configuration Manager supports the use of standard R/O and RW Community strings, or the use of SNMPv3 credentials. SNMP strings are typically used for initial device discovery, and for pulling hardware information from the device MIB.


The Credentials tab contains four separate tabs.

- Community String
- SNMP v3
- Account
- Privilege Passwords



To work with the Community String window (in the Credentials tab),

- 1 From the **Available** Credentials listing, select a Credential, then click the **Add** button to move that credential into the Assigned Credentials list. You can also use the Add All arrow if needed.

 If you have added more than one credential into the Assigned column, you can use the up and down arrows to change the order of the list.

- 2 Click **Ok** to preserve the credentials within the list, and the order of the list.

To Add a Credential,

- 1 To add a new credential, click **Add**.
- 2 The **Add Credential** window displays.
- 3 Enter a **Credential Name**.

- If this is a Voyence Unique Credential, select the **check box** , and then enter the exact length of the unique credential.

---

**Note**

- Community Strings are authorized credentials used by SNMP to communicate with devices.
- Multiple Read-Only (RO) or Read-Write (RW) Community Strings can be added to support network environments requiring unique Community Strings for different devices or device types. The sequence of each type of Community String can be adjusted using the up and down arrows.
- During Auto Discovery, when SNMP is enabled, each RO and RW Community String is tried until matches are found. The following fields are available:

---

**Add Credential**

\*Credential Name:

Credential Type: Account

Voyence Unique Credentials Length:

User Name:

Password:

Confirm Password:

This account is managed by an external authentication server.

Generate...

OK Cancel

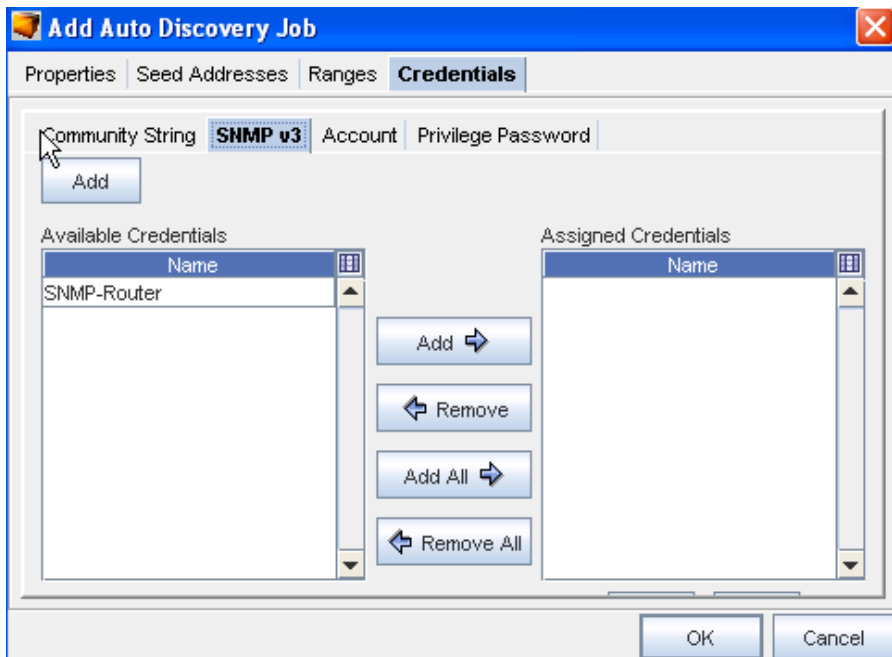
- 5 Enter the information needed for that window, and click **Ok** when you are finished.

Field	Description
Community String	Text field for entering community strings
Read-Write	Read-Writer community string list, which when discovered, can be updated with configs
Read-Only	Read-Only community strings list, which when discovered, cannot be written to or can a config be pulled from it

**Generate button** : Use the Generate button to have the system automatically generate Read Only and Read Write strings.

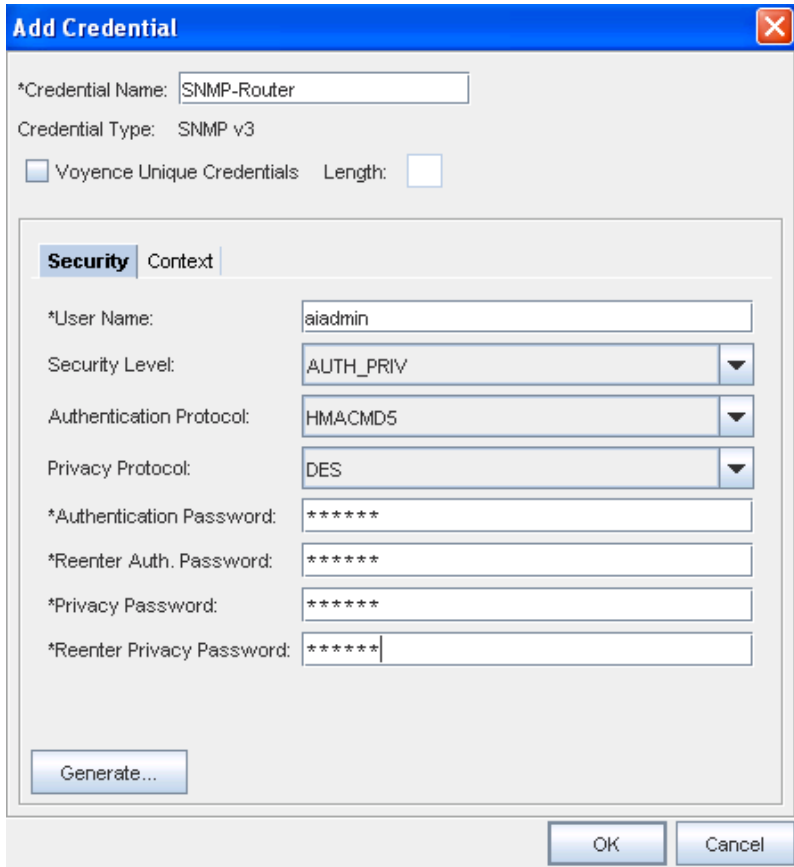
To work with the SNMP v3 window,

- 1 From the Available Credentials listing, select a Credential, then click the Add button to move that credential into the Assigned Credentials list. You can also use the Add All arrow if needed.



**i** If you have added more than one credential into the Assigned column, you can use the up and down arrows to change the order of the list.

- 2 To add a credential, click the **Add** button on the Add Auto Discovery Job windows (just above the Available Credentials pane).

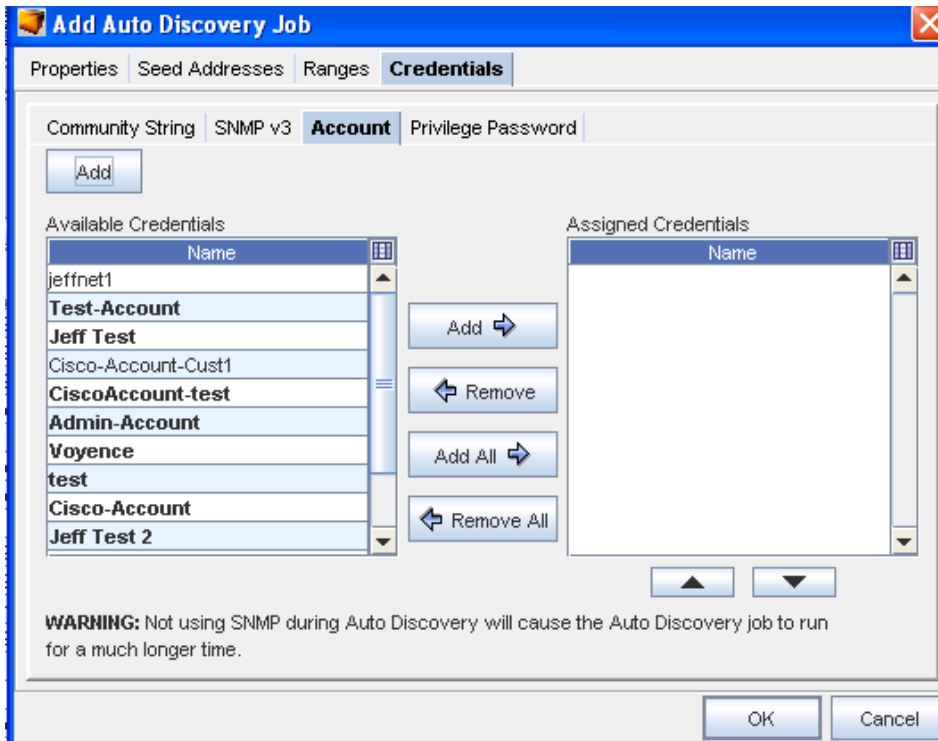


3 The **Add Credential** window displays.

4 Enter the information needed for that window, and click Ok when you are finished.

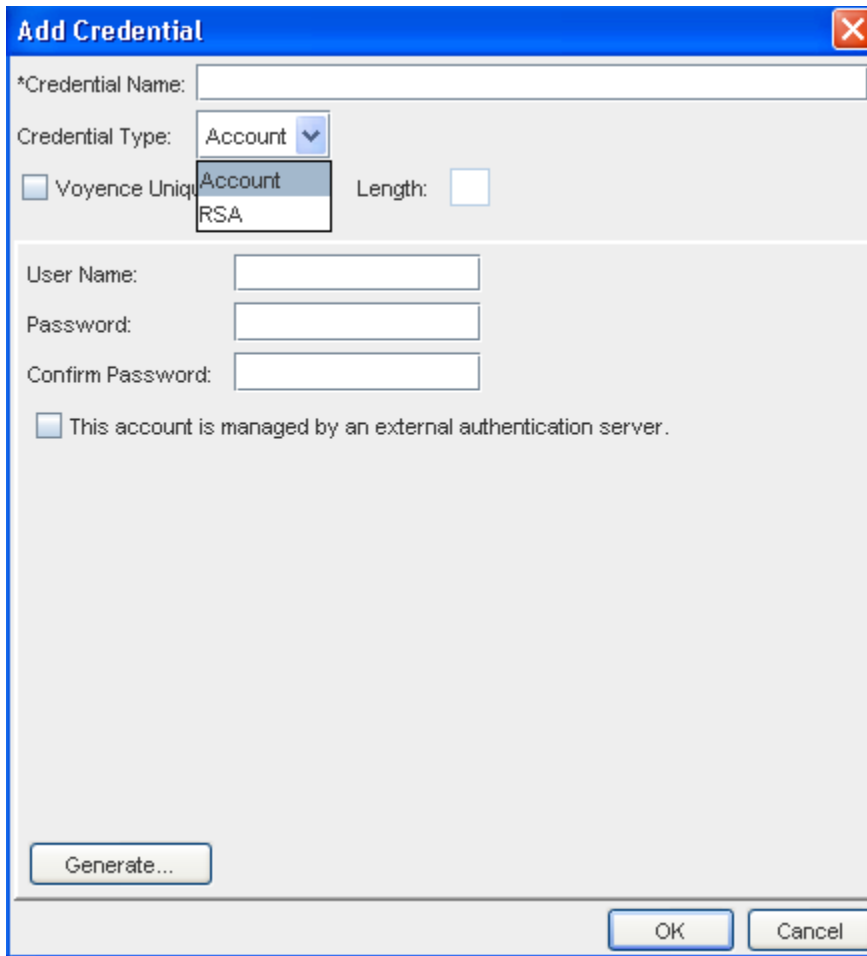
To work with the Account window,

1 From the Available Credentials listing, select a Credential, then click the **Add** button to move that credential into the Assigned Credentials list. You can also use the **Add All** arrow if needed.



- 2 Click **Ok** to preserve the credentials within the list, and the order of the list.

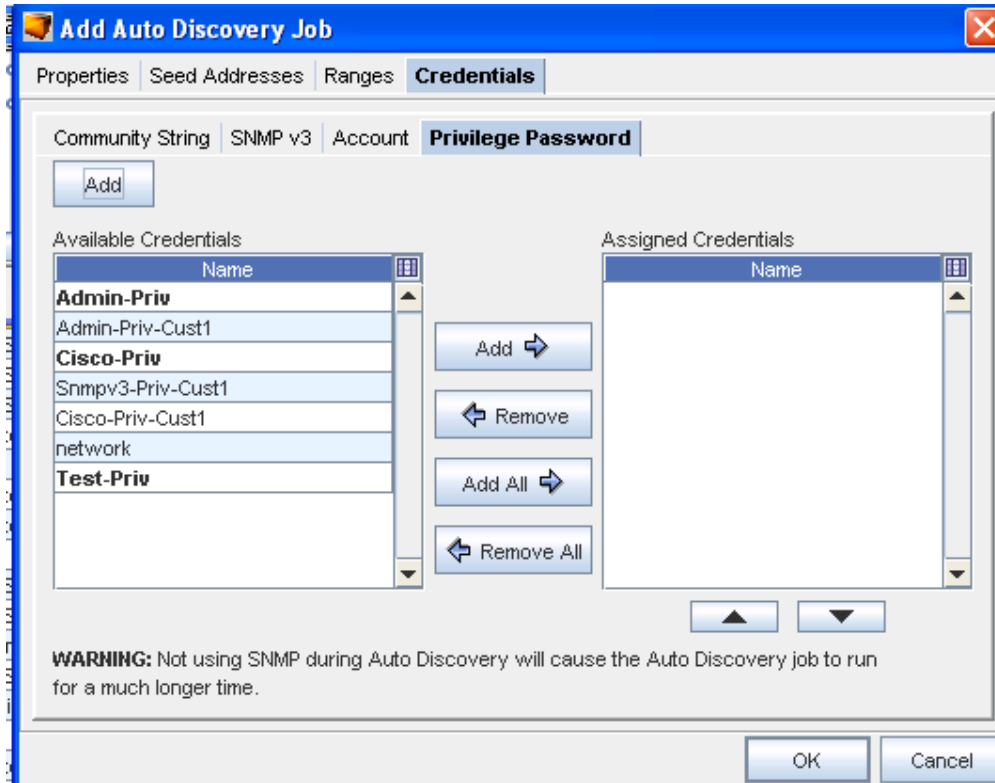




- 3 To add a new credential, click **Add**.
- 4 The **Add Credential** window displays.
- 5 Enter the information needed for that window, and click **Ok** when you are finished.

To work with the Privilege Password tab,

- 1 From the **Available Credentials** listing, select a Credential, then click the **Add** button to move that credential into the **Assigned Credentials** list. You can also use the Select All arrow if needed.



- 2 To Add a new Credential, click **Add**.
- 3 The **Add Credential** window displays.
- 4 Enter the information needed for that window, and click **Ok** when you are finished.

**Add Credential**

\*Credential Name:

Credential Type:  ▾

Voyence Unique

\*Password:

\*Confirm Password:

Secure

[Properties Tab](#)

[Seed Addresses Tab](#)

[Ranges Tab](#)

[Editing Auto Discovery Jobs](#)

[Removing Auto Discovery Jobs](#)

[RSA](#)

[SNMP Enabled/Disabled](#)

[SNMP Enabled](#)

If SNMP is **enabled**, and SNMP credentials are supplied, the device server attempts to determine which SNMP credentials are valid for the device. The device server starts with SNMPv1, then SNMPv2c, and finally SNMPv3. This order is used for performance reasons. Once a valid SNMP credential is found, the device is queried for its SysObjectID. This allows the device server to know which device driver to use for the remainder of the process.

---

**Note** While the discovery process starts with SNMPv1, the order of assignment is actually reversed. For instance, if all three SNMP versions are valid for the discovered device, the SNMPv3 mechanism is set as the active version .

---

Depending on the settings for the discovered device class, the device server now attempts to determine credentials for SSH, Telnet, FTP, and/or SCP. The management mechanism is set for the device based on the discovered credentials and the ordering options set in the application.

### SNMP Disabled

If SNMP is **disabled**, the device server attempts first to SSH, and failing that, Telnet to each device and determine the proper login credentials. Once the proper credentials are determined, the device server traverses through the device drivers to determine what the device class is for the connected device.

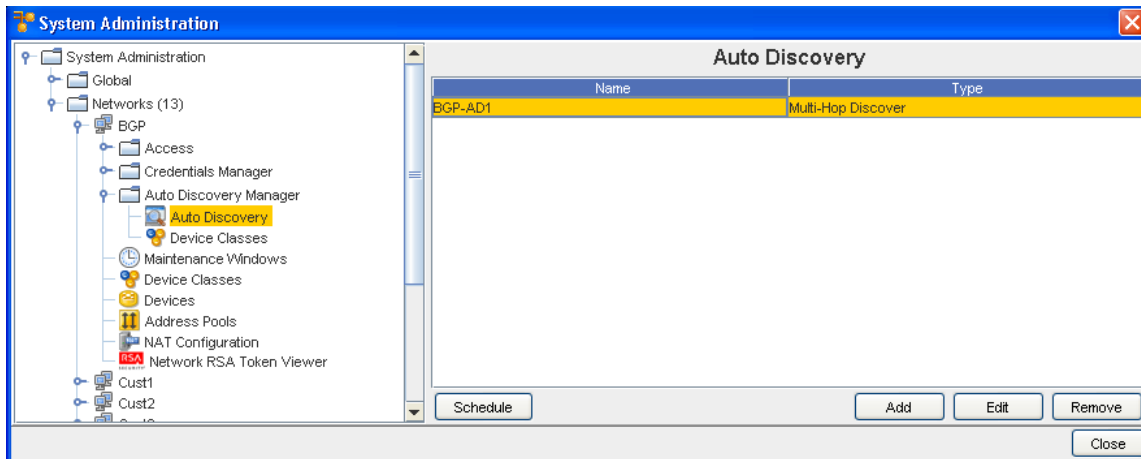
This is attempted based on the order contained in the addev.order file on the device server. Once a device class is determined, the appropriate commands are sent to the device to determine it's model information, which is then cross referenced with Voyence's database to determine the SysObjectID for the device.

Depending on the settings for the discovered device class, the device server now attempts to determine if FTP and/or SCP are enabled. The management mechanism is set for the device, based on the discovered credentials and the ordering options set in the application.

### Assigning Privilege Passwords

You can also assign Privilege Passwords during an Auto Discovery job.

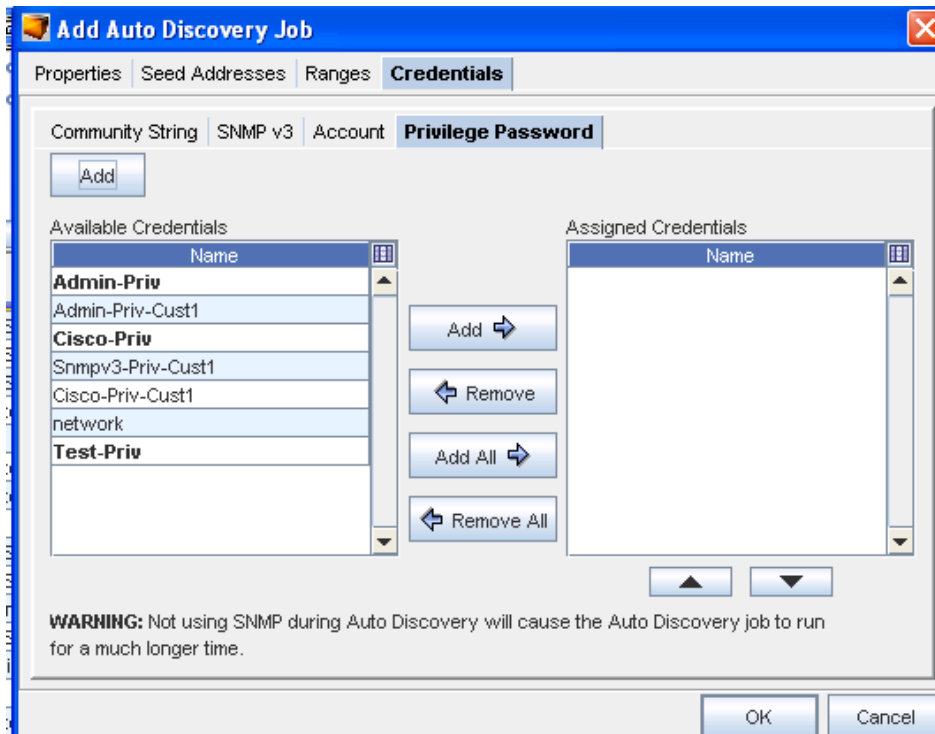
- 1 Select **Add** from the Auto Discovery window.



2 At the **Add Auto Discovery Job** window, click **Credentials**.

To work with the Privilege Password tab,

1 From the **Available Credentials** listing, select a **Credential**, then click the **Add** button to move that credential into the **Assigned Credentials** list. You can also use the **Select All** arrow if needed.



2 To Add a new Credential, click **Add**.

3 The **Add Credential** window displays.

4 Enter the information needed for that window, and click **Ok** when you are finished.

### Editing Auto Discovery Jobs

Editing an Auto Discovery job allows you to edit the details that have been previously set for a job. The tasks completed when editing are the same tasks you go through when the Auto Discovery job was first created.

When a job is edited, it does not have to be scheduled to run immediately. If it is on a recurring run cycle, the next time the run occurs, the changes are in effect.

For more information on the Auto Discovery tabs, see [Creating Auto Discovery Jobs](#).

Depending on the Auto Discovery type, details can be edited on the following tabs:

- Properties
- Seed Addresses
- Ranges
- Credentials

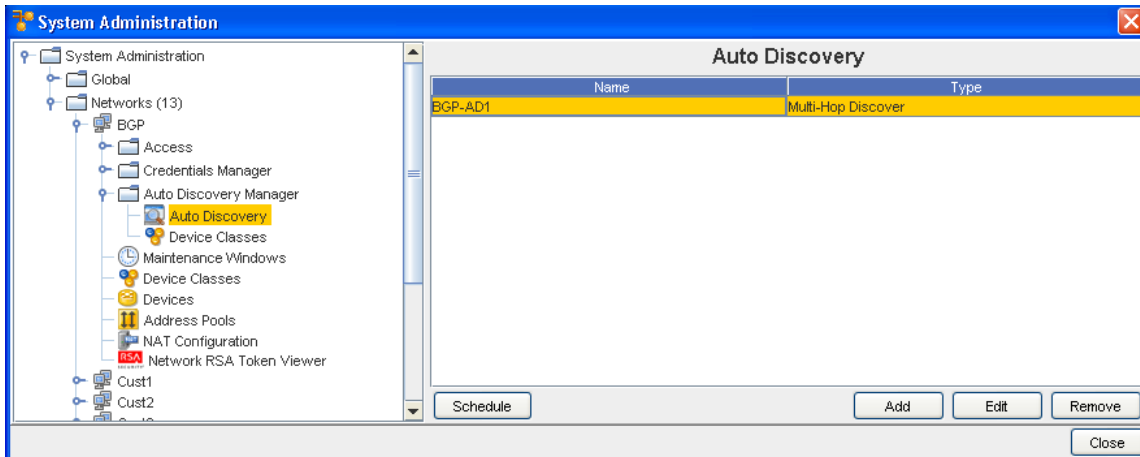
---

**Important** If insufficient details are entered on any tab, the Auto Discovery job may fail, or may not run completely.

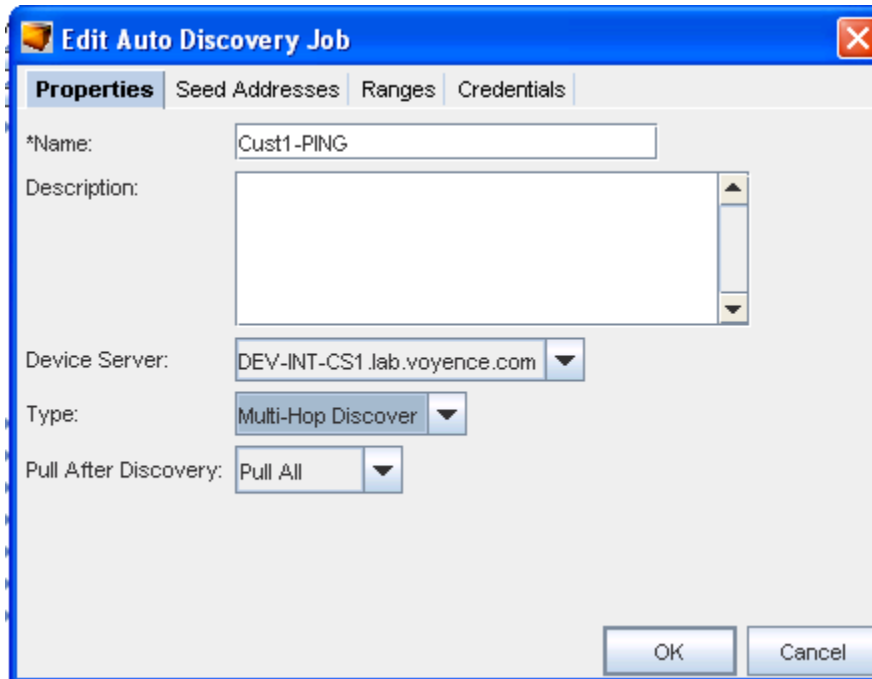
---

To edit an Auto Discovery job,

- 1 From the menu bar toolbar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Networks** folder.
- 3 Open the **Access** folder.
- 4 Click **Auto Discovery**.



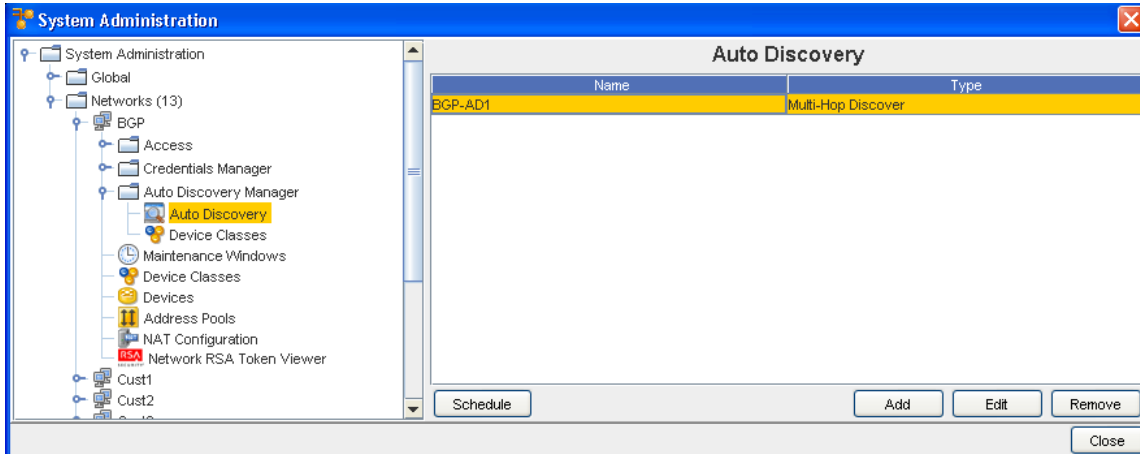
- 5 In the right pane, select the Auto Discovery **job** that you want to edit.
- 6 Click **Edit**. The Edit Auto Discovery Job window opens.



- 7 Make any needed changes to the existing information contained within each one of the tabs.
- 8 Click **Ok** when you have made your changes.

## Removing Auto Discovery Jobs

- 1 From the menu bar, access **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Networks folder**.
- 3 Click **Auto Discovery** .
- 4 The right pane populates with any Auto Discovery jobs that have been created.
- 5 The Schedule, Add, Edit, and Remove buttons are displayed



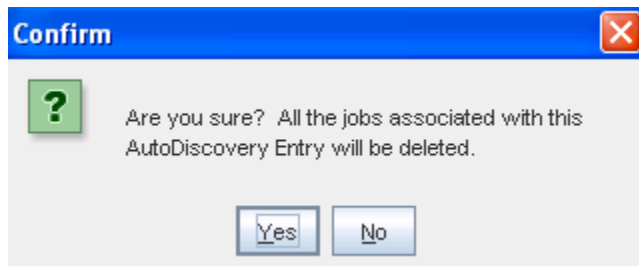
- 6 Select **one or more** Auto Discovery **jobs** to be deleted.
- 7 Click **Remove**. The Confirm window opens asking, "Are you sure?".

---

**Note** All associated jobs with the Auto Discovery entry will be deleted.

---

- 8 If okay, click **Yes**. The Confirm window closes.



The System Administration window refreshes. The selected Auto Discovery job is removed from the right pane.

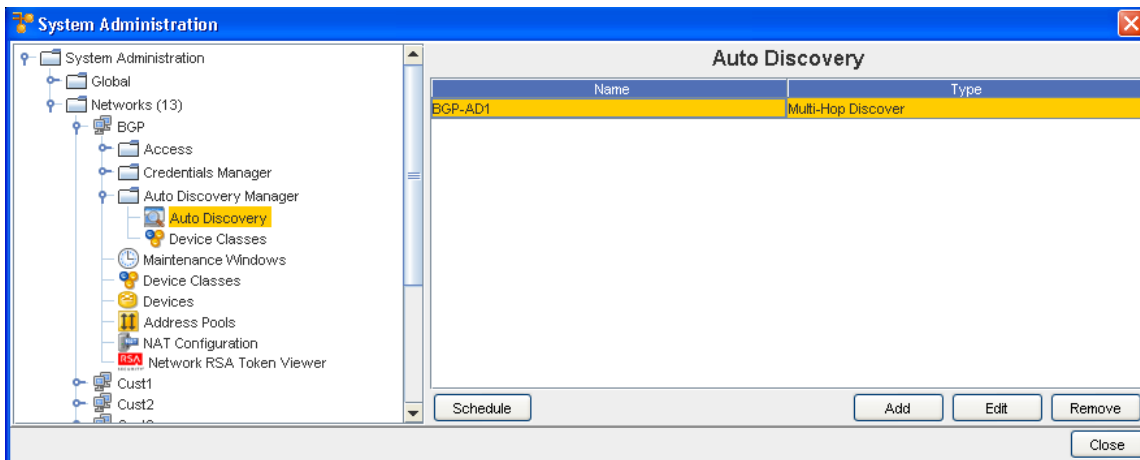
## Scheduling Auto Discovery Jobs



Auto Discovery jobs can be scheduled and then rescheduled. By storing all Auto Discovery jobs that have been created for each network, you are able to select and schedule any existing job. All settings for the stored jobs are saved, and can be edited. For more information, see [Editing Auto Discovery Jobs](#).

To schedule and submit an Auto Discovery job for approval,

- 1 From the menu bar toolbar, select **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, expand the **Networks folder**.
- 3 Click **Auto Discovery**.



- 4 Click **Schedule**. The Schedule Auto Discovery Job window opens.

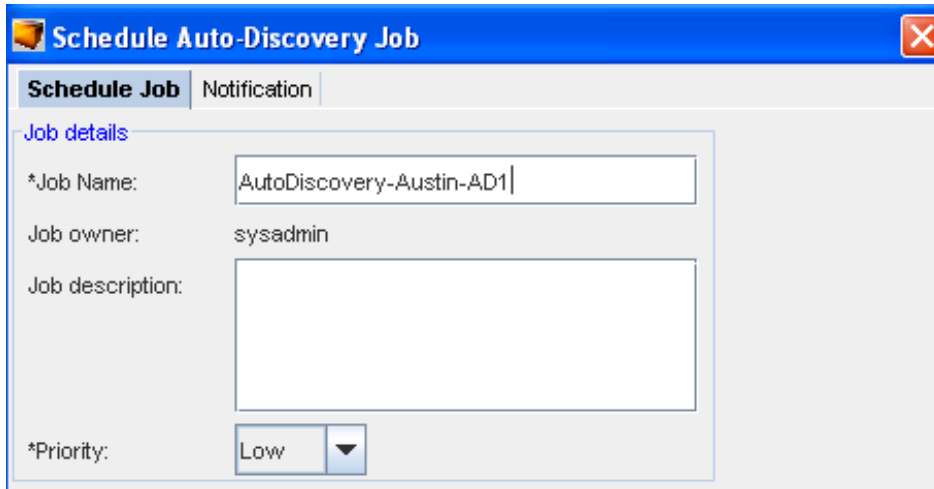
### The Schedule Job Tab

The Schedule Job tab is divided into two sections:

- Job Details
- Schedule Job

There are also two tabs, **Schedule Job** and **Notification**.

### Schedule Job - Job Details



The following fields are available when scheduling a job. The required fields are identified by an asterisk (\*).

Field	Description
Job Name	Required Field. The job name is how you refer to the job in the job history.
Job Owner	System generated, from the user creating the job
Job Description	Optional. Comment area for outlining job significance and other details that other users may find helpful during a review of the job history and tasks.
Priority Setting	Priority Setting priority allows the job to run ahead of other scheduled jobs, depending on the prioritized setting. Priority settings are: Low, Medium, and High. The default is Medium. If you are running a cut-through the priority must be High.

**Note** The priority setting affects the job execution between the device server and the network device.

### Schedule Job

**Note** When the **recurring schedule** is selected, the new time zone drop-down options are available. Make your selection from the drop-down options. The time zone you select must be the **client's time zone**. The new time zone field will be propagated with the client time zone automatically when creating a new Maintenance Window or recurring scheduled job.

The following fields are available when scheduling a job.

Field	Description
Run in next maintenance window	Setting allowing the job to run in the next maintenance window
Run upon approval	Setting allowing the job to run as soon as the job is approved. If you have job approval permissions, when you schedule the job you can also approve it to run immediately.
Run upon operator initiation	Will run when the operator designates the activity
Run at scheduled date/time	Used to set a specific date and time the job will run. This allows you to run jobs when best for your network, or based on planned network changes.
Run as recurring series	Used for pushing updates to the network automatically. Not only allowing you to set the start date, but also the end date for a limited time-span and frequency. If necessary, the update can be set to never end. This option allows the updates to continue, unless manually canceled in the Scheduler.
<b>Recurring Options:</b>	- Frequency (Hourly, Weekly, Monthly) - Start Time - End Time - Interval (Set by hours) The recurring updates do not change unless updated in the Scheduler.

The **Approve & Submit** button, located on the bottom of all tabs, can be used when adequate permissions have been granted. When clicked, the job is immediately sent to the scheduler, based on the defined settings.

- 1 Enter the information needed in the **Job Details** section.
- 2 Make your selections in the **Notifications** tab.
- 3 Make your selections in the **Schedule Job** section, then click the appropriate button (**Approve & Submit** or **Submit**) at the bottom of the window.

## Device Types and Objects

Once auto discovery has located a device, the devices are made **available** to the networks.

Depending on the devices servers and the related devices, you might have the following devices types and objects that can be managed by your network:

- Routers
- Generic Switches
- Contivity
- Connectors
- Clouds
- Generic Devices
- VPN Concentrators
- ATM Switches
- Content Switch
- Firewalls
- layer and Switch
- Load Balancer
- Access Points
- Modems

After completing Auto Discovery to locate devices, you must [Managing Network Devices](#) to the appropriate networks. Devices can be assigned to multiple networks. When a device is assigned to a network or networks, the device is classified as *Managed*.

There are **two** ways that a device can be associated with a network:

- Automatically assigned during Auto Discovery
- Using the Mange Devices window

## Networks - Maintenance Windows - Done

## Maintenance Window Overview

When there are large networks involved, downtime - due to changes to the network, can be costly. Network Configuration Manager allows you to set a window of time in which updates to your networks can be scheduled. This can be designated by time of day, days of the weeks, or scheduled to run on a regularly scheduled event until changed basis.

A maintenance schedule can be set for the entire network, or for separate networks that are managed by Network Configuration Manager.

Similar to the Schedule Manager window, the Maintenance window uses the One-time schedule, or a Recurring schedule, that allows you to determine not only when, but how often updates occur to the network.

It is not necessary to create Maintenance schedules for all networks. Networks inherit any System Maintenance window settings. If a System Maintenance is not set, then each network defaults to the individual scheduled times.

Maintenance windows can be overridden at the Network level. When set at the Network level, any Global Maintenance windows must be copied down to the Network. Windows can only be set at either the Global or Network level, but not both,

Maintenance windows can be set for the following:

- Pushes
- Pulls
- Auto-discovery
- Commands
- Quick commands
- Cut-throughs
- OS Updates
- Reports

If more than one of the following types is scheduled, the following priority sequence will be used.

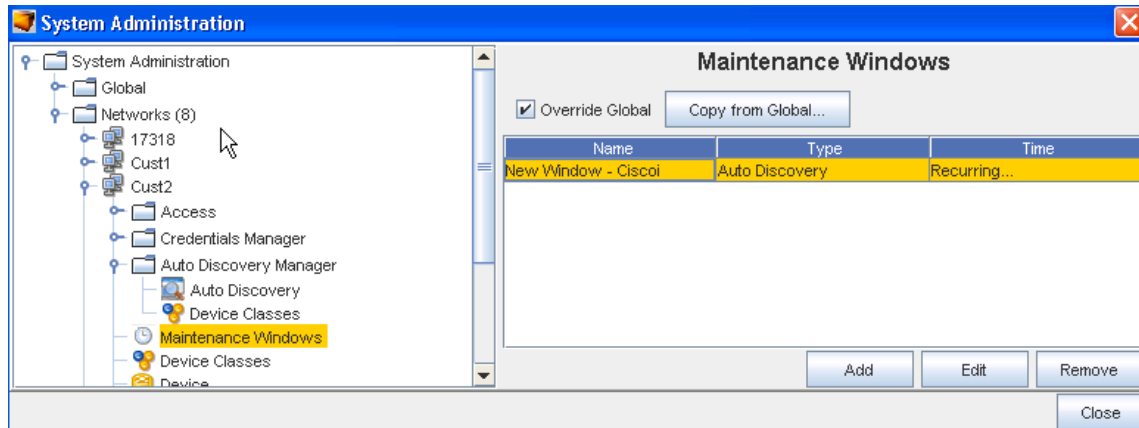
- OS Update
- Config/Configlet Push
- Saved Command
- Auto-Discovery
- Pulls

---

**Note** Quick Commands and Cut-throughs cannot be scheduled. Overlapping schedule times is not allowed.

---

As an added feature, a user with the **appropriate privileges can override a scheduled maintenance (at the Network level)** . This is allowed, for emergency changes to the network for which the schedule change is either unnecessary or harmful.



**Important** Note that you can select to Override Global settings, and then Copy from the Global Settings from this Network window. You must select Yes to continue the copy process.

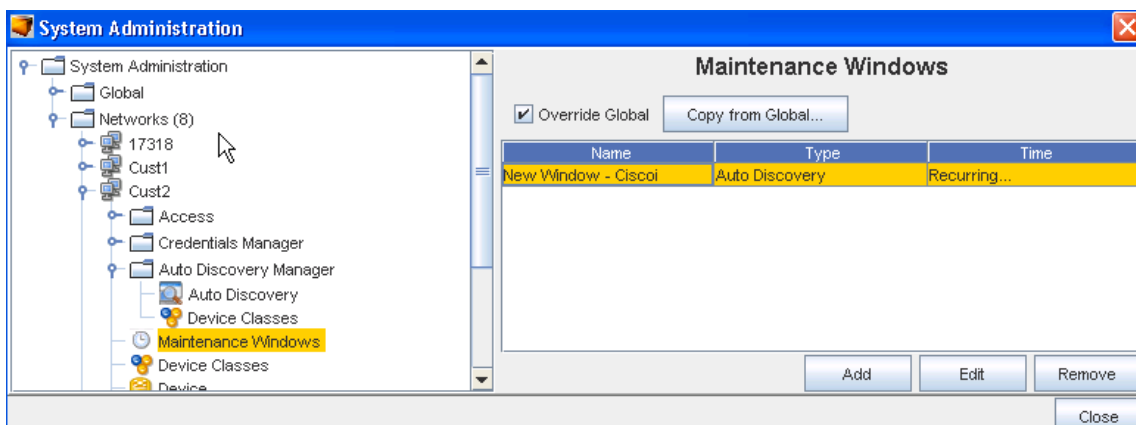
### Networks - Adding a Maintenance Window

A Maintenance window can be added at the System (Global) Level, or at the Network Level.

**Note** You can now define a window for each activity that can be completed against a device, thus ensuring that only those activities can only be completed during that designated window.

To add a scheduled maintenance window,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Networks -> Maintenance Window**.



- 3 Click **Add**.

The Maintenance window uses the same schedule window as the Schedule Manager.

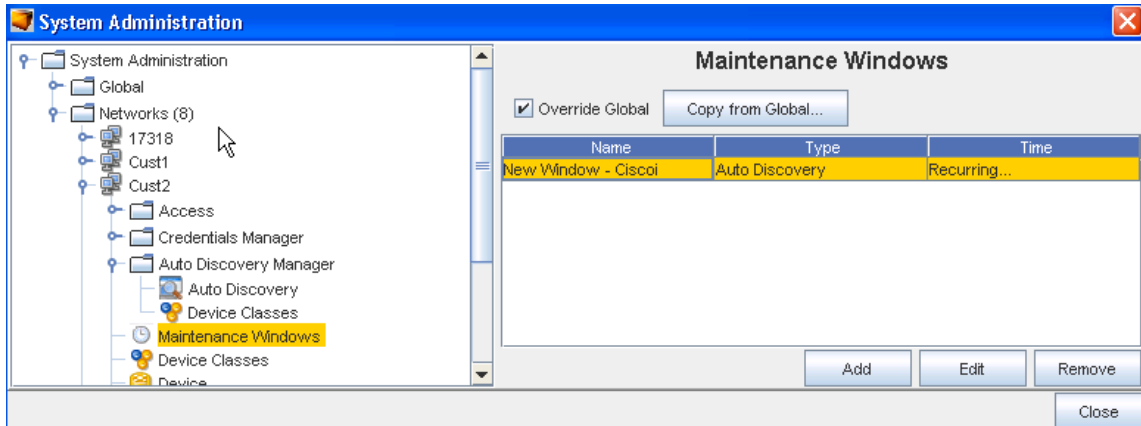
- Set the **exact date** and time for the run to occur.
  - Select a **recurring schedule** using the **Run As Recurring series** option. When the recurring schedule is selected, the new **time zone** drop-down options are available. Make your selection from the drop-down options. The time zone you select must be the **client's time zone** . The new time zone field will be propagated with the client time zone automatically when creating a new Maintenance Window or recurring scheduled job.
- 4 After making your schedule preferences, click **OK**. The maintenance window closes, and the information is now stored within the Maintenance Windows.
- Enter a **unique name** for the maintenance window.
  - From the drop down list, select a **Type**. Remember, you can now schedule a window for each activity.
  - From the next drop down ( **Window Duration**), select the time allocated updates.
  - Next, at the Schedule portion of the window:

### Networks - Editing a Maintenance Window

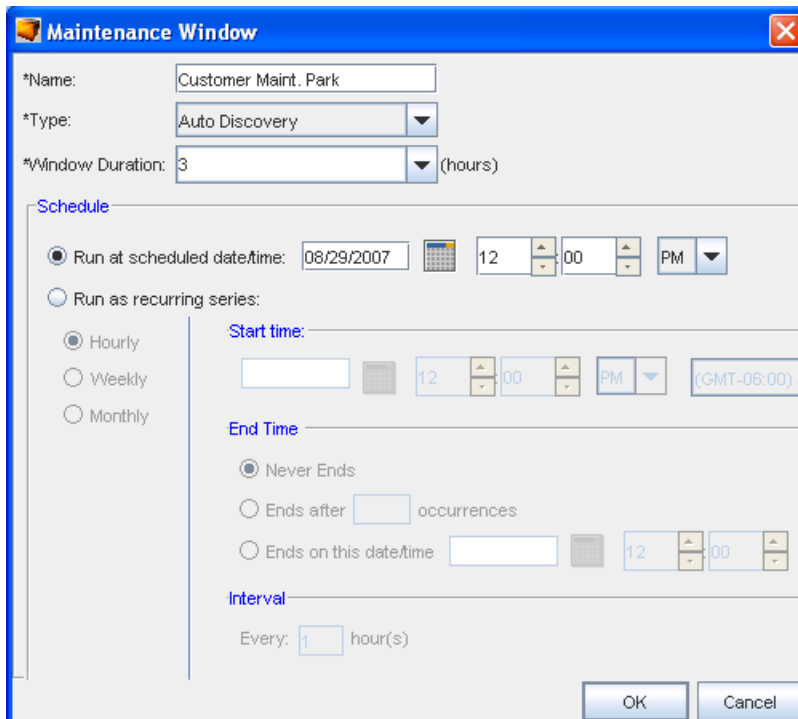
Maintenance windows can be added at the System (Global) Level, or at the Network Level. The date, time, or recurring sequence can be edited, based on the needs of your networks.

To edit a scheduled maintenance window,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Networks -> Maintenance Window**.
- 3 Select the **Schedule** from the list, then click **Edit**.



Or, select the schedule, then click **Edit**. The schedule opens. The current settings are available for edit.



- 4 Make changes to the schedule as needed.
- 5 Click **OK**. The changes are saved and are in effect on the next schedule run. The Maintenance window closes.

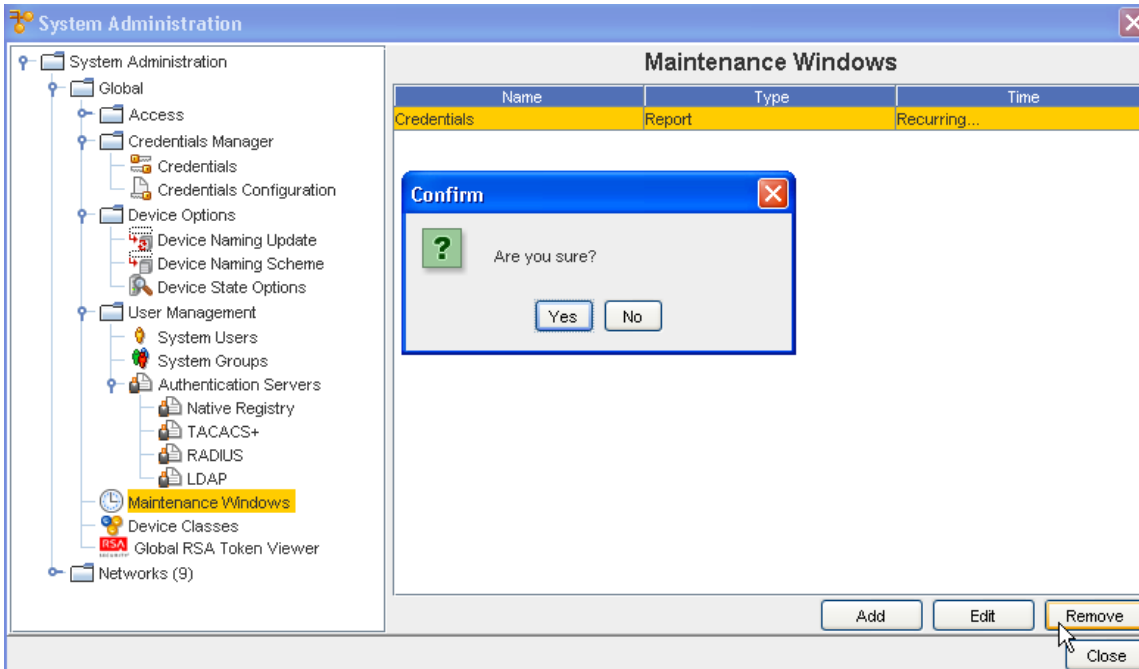
### Networks- Removing a Maintenance Window

When a schedule is no longer needed for your networks it can be deleted from the list. By removing a maintenance schedule, any network with the associated schedule takes on the settings of the System (Global) maintenance schedule (if one has been previously set).



To remove a scheduled maintenance window,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Global -> Maintenance Windows**.
- 3 Select the schedule (maintenance window), then click **Remove**. The confirmation window displays.



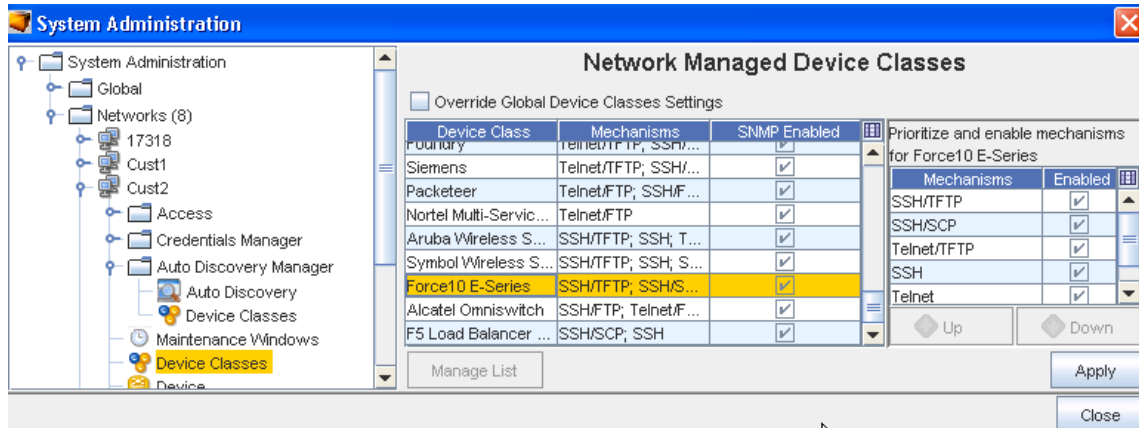
- 4 If okay, click **Yes**. Or, to cancel this action, click **No**.

The Maintenance Window updates with the selected item removed from the list.

## Networks - Device Classes

### Network - Device Classes Overview

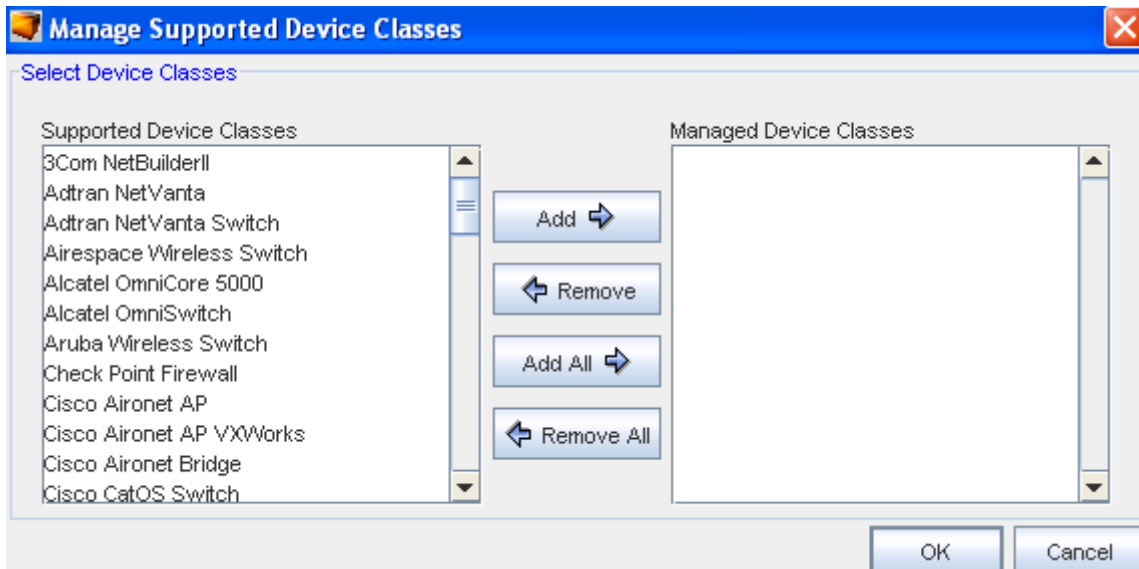
From the System Administration tool, you can access the Device Classes for the various Networks you have created.



From this Network Managed Device Classes window you can work with the Device Classes.

To Manage the Devices Classes list (and override Global Settings),

- 1 From the listing of Device Classes displayed in the Network Managed Device Classes window, select a **Device Class**, then click the **Override Global Settings** check box.
- 2 Next, select the **Managed List** button to view a listing of the Supported Device Classes shown in the Manage Supported Device Classes window.



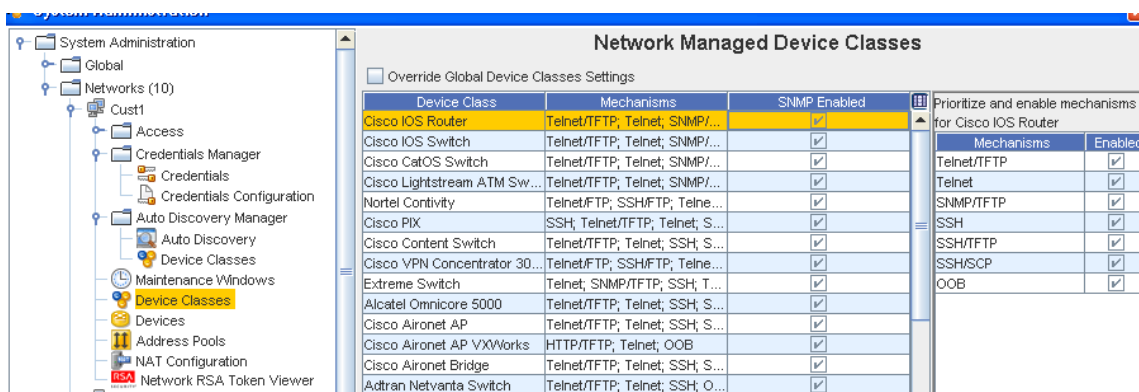
- 3 Make your selections from the **Supported Device Classes** pane, and move them into the **Managed Device Classes** pane using the **Add** or **Add All** buttons. Note that you can also remove any unneeded classes using the Remove or Removal All buttons.
- 4 Click **Ok** when you have made all your additions to the Managed Device Classes pane. The Device Classes you added are now in the listing shown in the Network Managed Device Classes window.

## Networks - Specifying Device Class Protocol

**Important** Your Networks may not be configured to handle certain protocols for supported devices. If you choose, you can enable or disable communications to your network devices using specific communication protocol methods.

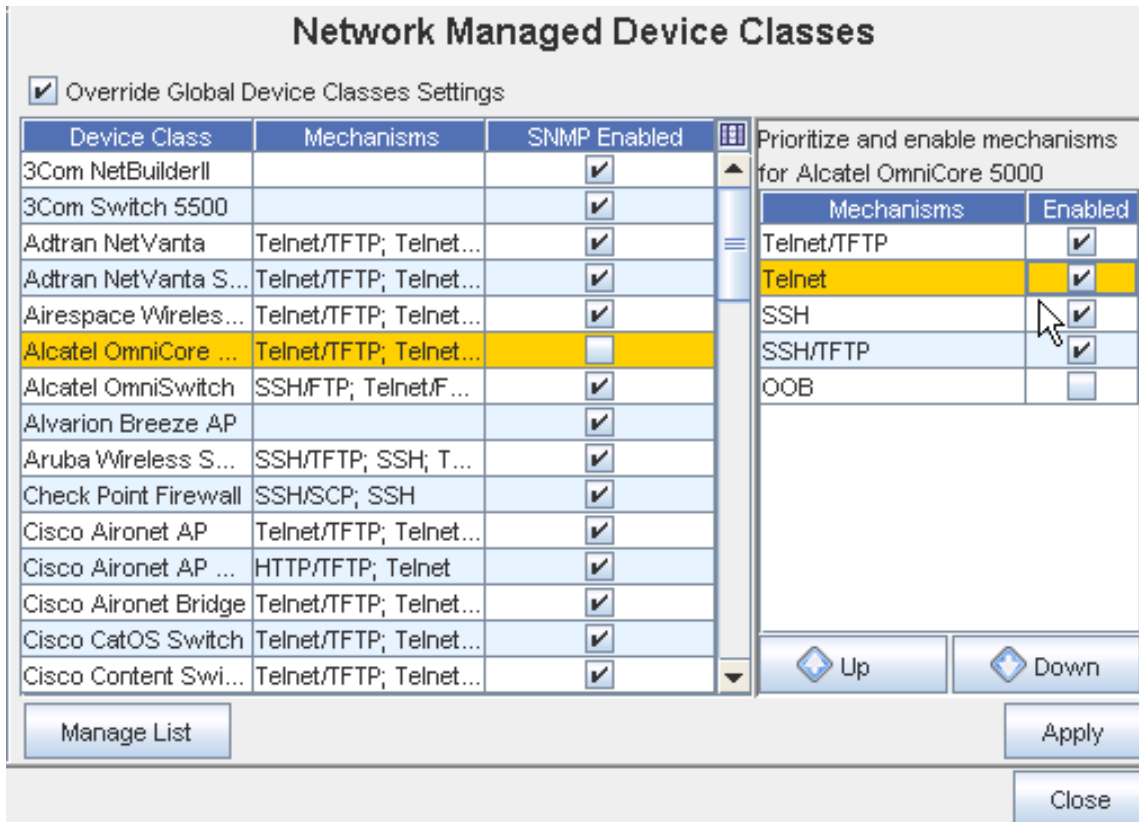
To adjust the device class protocols,

- 1 From the menu bar, select **Tools**.
- 2 From the menu options, select **System Administration**. The System Administration window opens.
- 3 On the tree menu, expand the **Networks -> Access** folders.
- 4 Select **Device Classes**. The Network Managed Device Classes configuration window populates the right pane.
- 5 Select a **row (listing the Device Class and the Primary Protocol)**. When highlighted, the Enable or Disable fields show any protocols that are active/deactivated for the device class.



**Note** By default the Use SNMP check box is selected. If you choose not to use SNMP, un-check this check box.

- 6 To make changes to the Protocols section, **disable** the device class by un-checking the check box, then select another **Mechanism** from the listing to the right.



- Adjust the priority of the protocols
- Enable or Disable protocols

7 Click **Apply** when you have select a Mechanism from the list.

- This window allows you to:

To change the priority of the listed protocols,

- 1 Select a **protocol** from the list. Based on its location in the list, the Up and Down arrows activate.
- 2 Using the Up/Down arrows move the selected protocol to the new location. The top-most protocol is used as the default.
- 3 If you are enabling or disabling protocols, proceed to the next step. Or, if no other changes are required, click **OK**. The Manage Devices - [Device Class Name] window closes.

To enable and disable device protocols,

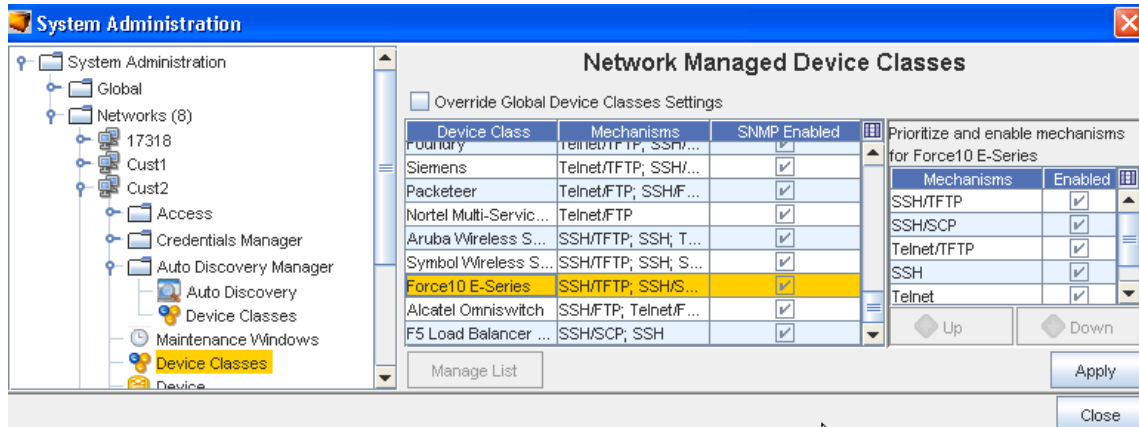
- 1 If you are enabling a protocol, in the Enable column, check the boxes of the **approved protocols**.
- 2 If you are disabling a protocol, in the Enable column, de-select the check box.
- 3 If no other changes are required, click **OK**. The Manage Devices - [Device Class Name] window closes.

- When all changes have been completed on the Network Managed Device Classes window, click **Apply**.

## Override Global Settings

Device Classes and Communication mechanisms can be overridden at the Network level. To do this, the Override Global Settings check box must be selected.

This allows you to use SNMP/TFTP to manage Cisco routers in one Network, and to use Telnet for management in another Network.



## Networks - Devices

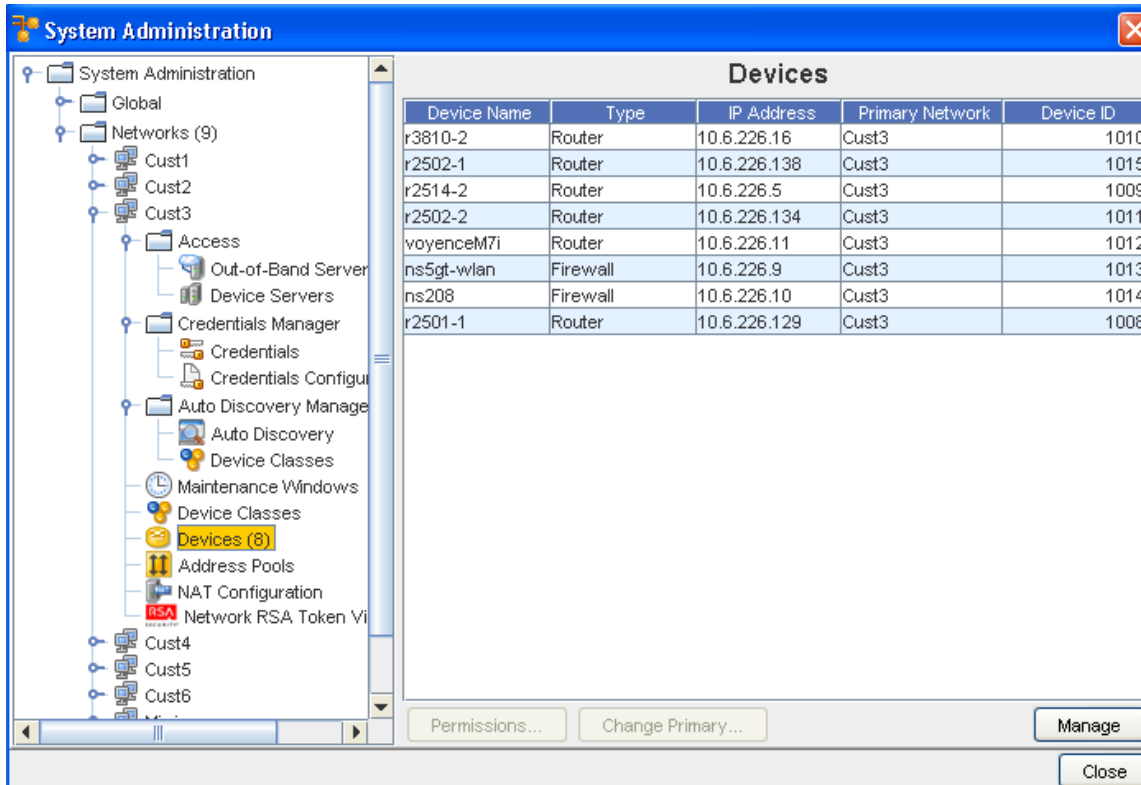
### Managing User and Group Device Permissions

The devices on the device server are edited in two ways:

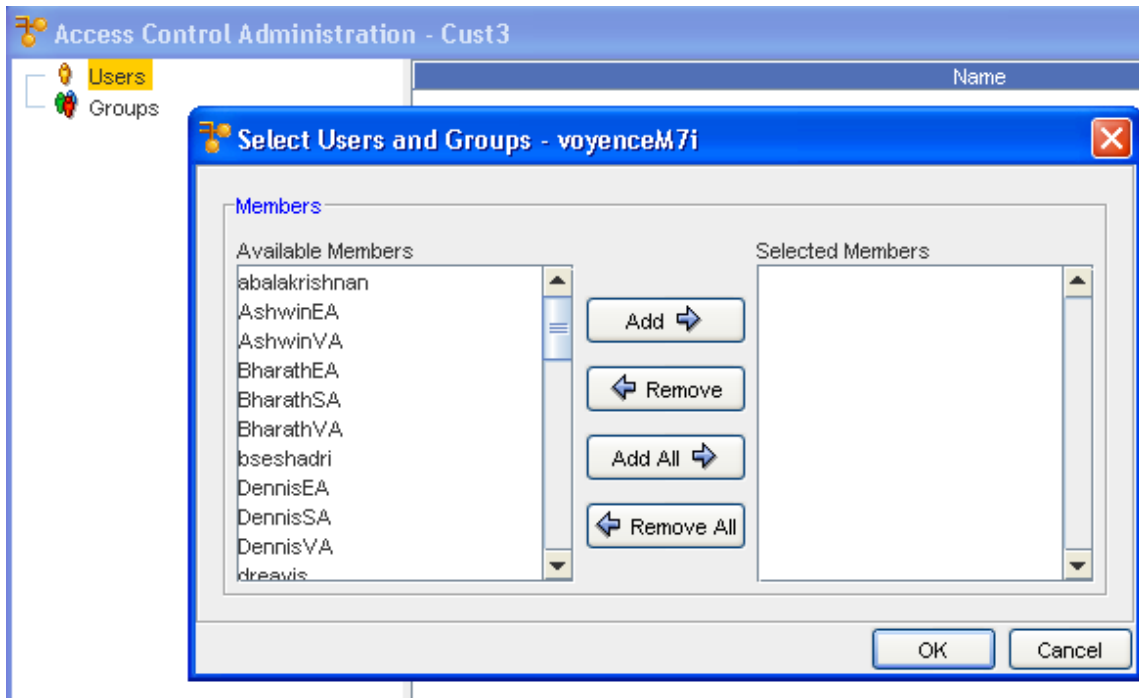
- Editing the device override default settings
- Defining devices level permissions

To designate users permissions at a device level,

- In the navigation pane, open the network where the device is located.
- Expand the **Network** folder, then select **Devices**.
- In the right pane, select one or more devices .



- 4 In the lower portion of the window click **Permissions**. The Access Control Administration window opens. There are two groups:
  - Users
  - Groups
- 5 Select an option, then at the bottom of the window, click **Manage**. The Select Users and Groups window opens.



- Users and groups that do not have permissions are listed in the Available Members column.
  - All users and groups with permissions are listed in the Selected Members column.
- 6 To give users or groups permissions to the workspace, click the **name of the user or group** in the Available Members column.

**Note** A string of users/groups can be selected by holding down the Shift-key while selecting users/groups. Or, select multiple, non-sequential users/groups can be selected by holding the Ctrl key while selecting users/groups.

- 7 Click **Add**. The selected users and groups are moved to the Selected Members column, and have permissions to the workspace. Or, to remove a user or groups permissions, in the Selected Members column, select the name or group.
- 8 Click **Remove**. The selected users and groups are moved to the Available Members column and no longer have permissions to the workspace.
- Clicking **Add All** moves all users and groups listed in the Available Members column to the Selected Members column.
  - Clicking **Remove All** moves all users and groups back to the Available Members. If you complete this action, remember to put your own user name back into the Selected Members column.
- 9 Once you have the needed users and groups to have access to the workspace, click **Ok**. The Select Users and Groups window closes.

The Access Control Administration window refreshes. All users and groups are re-categorized to reflect the changes that were made.

You are now able to set the [Setting User and Group Permissions](#) and Others. (Others are users that have limited access determined by the permission settings for selected devices only.)

### Changing the Device's Primary Network

Device Permissions, Device Status, and Primary Network are all set in the Network level devices area. Since a device can be shared by multiple Networks, and its credentials and communications are set from its Primary Network, the Primary Network name is available in this window.

You can change the Primary Network associations by clicking on Change Primary, and then re-selecting the Primary Network.

---

**Important** Primary Network does not appear by default in the Device table. To view the Primary Network, you must modify the table setting to include this field.

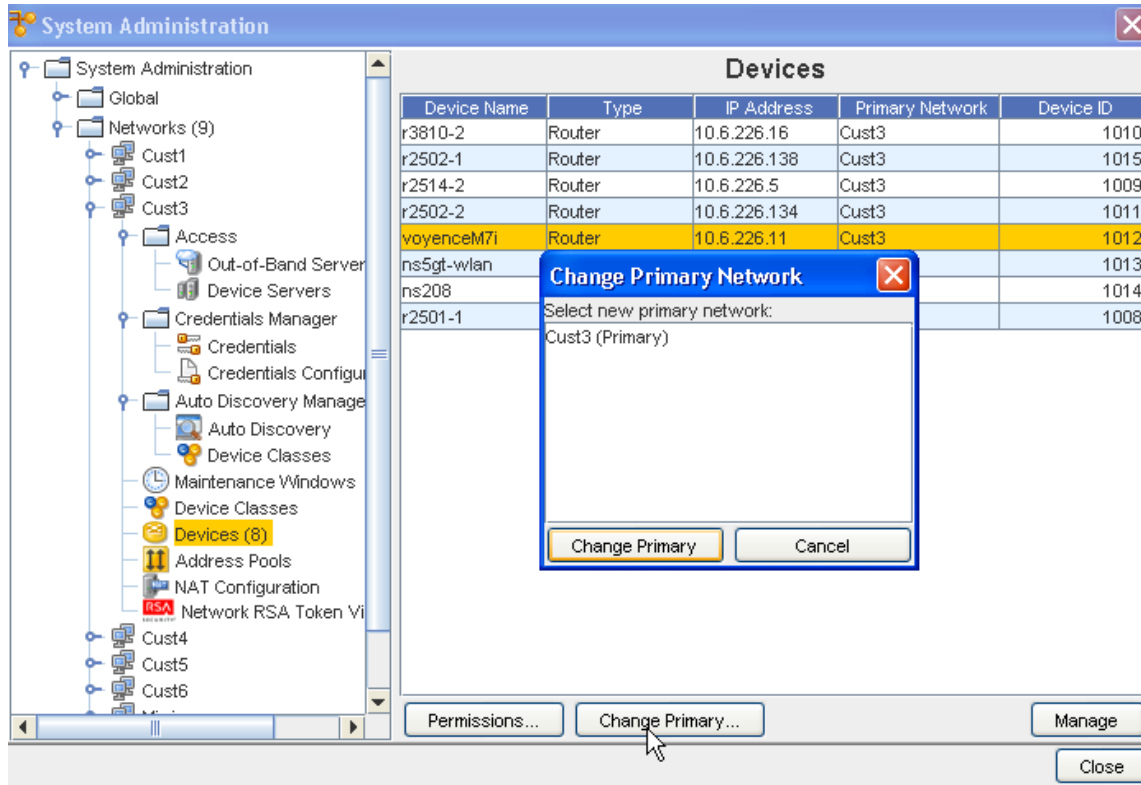
---

Network Configuration Manager allows devices to be managed by multiple networks . The first network that the device is associated with becomes its **primary** network.

To change the primary network of a device,

- 1 From the menu bar, select **Tools -> System Administration**. The System Administration window opens.
- 2 In the navigation pane, click **Networks**.
- 3 Open the device's current primary network.
- 4 Expand the **Network** folder, then select **Devices**. The right pane populates with all devices currently residing in the network. If the network is the primary location of the device, they Primary Network column contains information.
- 5 In the right pane, select one or more devices. The selected devices are affected by the following steps.





- Click **Change Primary** . The Change Primary Network window opens.
- Select a name from the listing, then click **Change Primary** . The Primary Network you selected is now displayed in the Devices list.

## Networks - Address Pools

### Address Pool Overview

The Address pools allow you to setup flat address pools using Network Configuration Manager. You can define address pools for each Network within Network Configuration Manager.

**Note** This feature is also available using the API.

The IP Addressing feature uses a flat topology, but it contains multiple blocks. These flat pools are only seen in the network for which they are created. The pools are then used in the Workspace, Sites, and Views of the network.

There is no limit to the number of IP Addresses that can be set up in the pool. When needed, addresses can be excluded. When a device is pulled into the repository, the device's IP is authenticated to make sure it's IP is defined in the networks pool.

IP Addresses are blocked for each network. Each block can contain as many IP Address as needed for the block. Address blocks can be allocated from pools for use in assigning IP Addresses to new devices and interfaces. Addresses are assigned through the use of insert IPs and Insert Reference Variables within [Editors Overview](#)

When completing cleanup and maintenance on the IP Address blocks, you can [Removing an IP Address Pool](#) or only [Editing an IP Address Pool](#).

### Managing Address Pool Usage

The status of existing Address pools can be checked by clicking **Manage Usages**. Address blocks in each of the four status pools (Used, Ready, Held, and Excluded) can be checked.

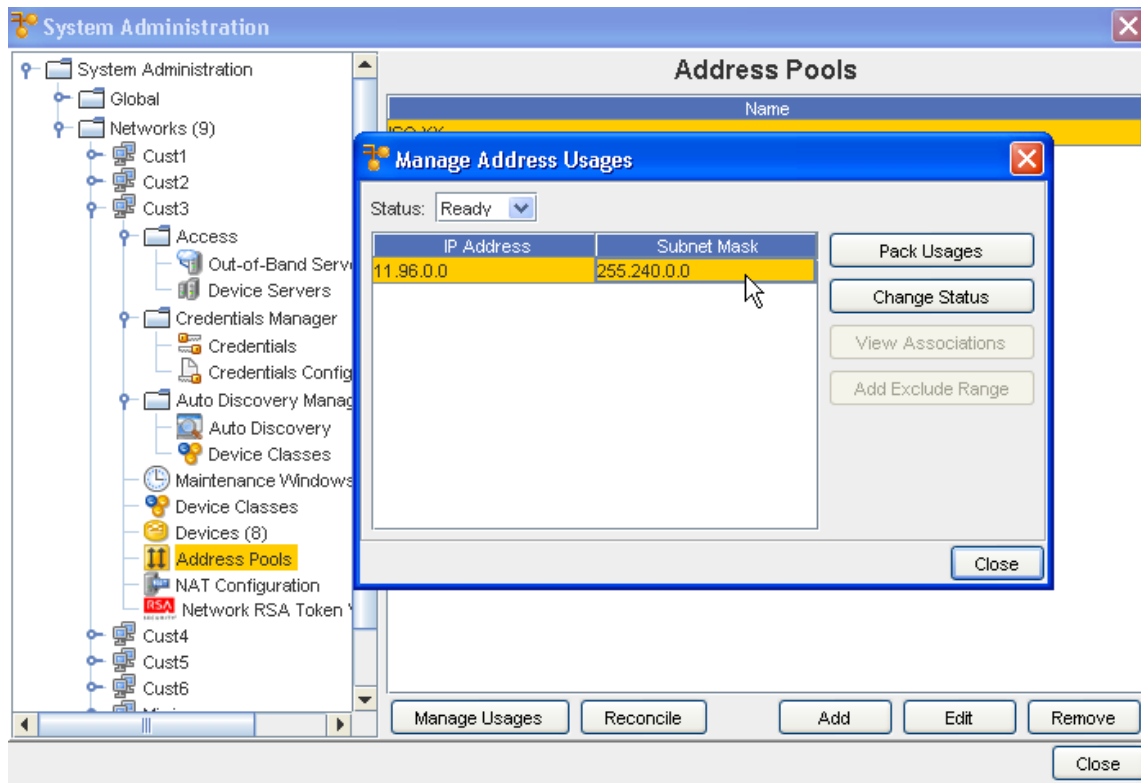
IP associations can be checked, and the status of currently used blocks can be managed.

The ability to manage the usage of IP Addresses has four options:

- Pack Usages
- Change IP Address Status
- View the Associates of the IP Address
- Add Exclude Range

To access the Manage Usage feature,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Address Pool**. The Address Pools List window opens. All existing IP Address Pools are listed.



- 3 Select an address pool, then click **Manage Usages**. The Manage Address Usages window opens.

You can view the **Status** of the range of IP addresses using the drop-down arrow, and making a selection from the list. You can view IP addresses in the Held, Used, Ready and Excluded status. Once you have made a Status selection, the IP addresses within that status are displayed.

The Manage Address Usages window allows to you see the following details about the selected address pool.

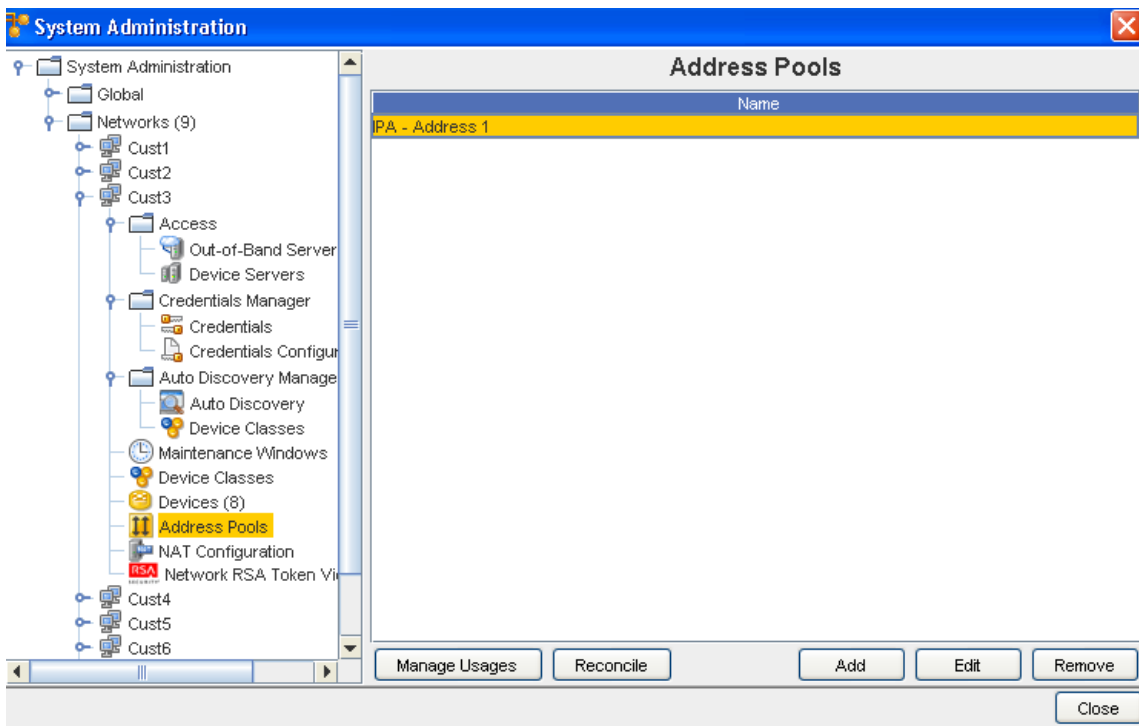
### View IP Address Pool Associates

The ability to manage the usage of IP Address has four options:

- Pack Usages
- Change IP Address Status
- View the Associates of the IP Address
- Add Exclude Tang

To view devices which currently use the selected IP Address,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Address Pool**. The Address Pools List window opens. All existing IP Address Pools are listed.



- 3 Select an Address pool, then click **Manage Usages**. The Manage Address Usages window opens.
- 4 Select the **IP Address row**. If there are devices associated with the IP Address, the View Associations button becomes active.

5 Click **View Associations** . You can now view the associations information.

### Change IP Address Pool Associates

The ability to manage the usage of IP Address has four options:

- Pack Usages
- Change IP Address Status
- View the Associates of the IP Address
- Add Exclude Range

The Change Status features allows you to modify the status of an IP address range without deleting the range.

---

**Note** Changing the status only affects the status for the specified range, not the entire address pool.

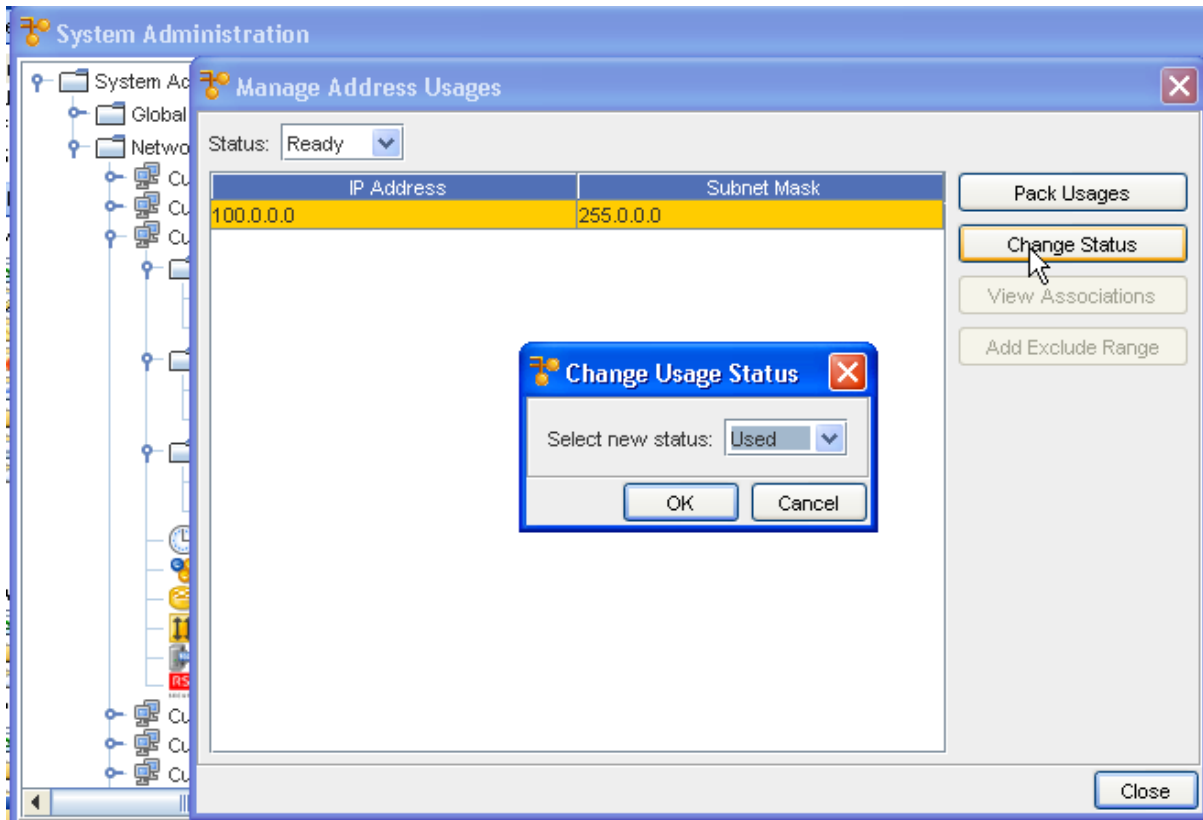
---

The current status options are:

- **Ready** - Identifies the IP address ranges that can be used for device IP address comparison or inserted in an editor
- **Used** - Identifies the IP address ranges that are currently being utilized
- **Held** - Identifies IP address ranges that have been assigned by Network Configuration Manager -- but not yet deployed to a device
- **Excluded** - Identifies address ranges that are currently excluded from use in Network Configuration Manager.

To change the status of an IP Address range,

- 1 From the menu bar, select **Tools -> System Administration** .
- 2 Next, select **Network -> Address Pool**. The Address Pools List window opens. All existing IP Address Pools are listed.
- 3 Select an Address pool, then click **Manage Usages**. The Manage Address Usages window opens.



- 4 Select the **IP address row**, then click **Change Status**. The Change Usage Status window opens.
- 5 From the drop-down list, select the new status for the IP Address.
- 6 Click **OK**. The Change Usage Status window closes, and the Manage Address Usages window updates.

### Reconcile Address Pools

IP Address pools may need to be **reconciled** if there have been changes made to the pools that are no longer in-sync. Reconciling IP Address pools permits you to see those address ranges within your pool already allocated to devices within the Network.

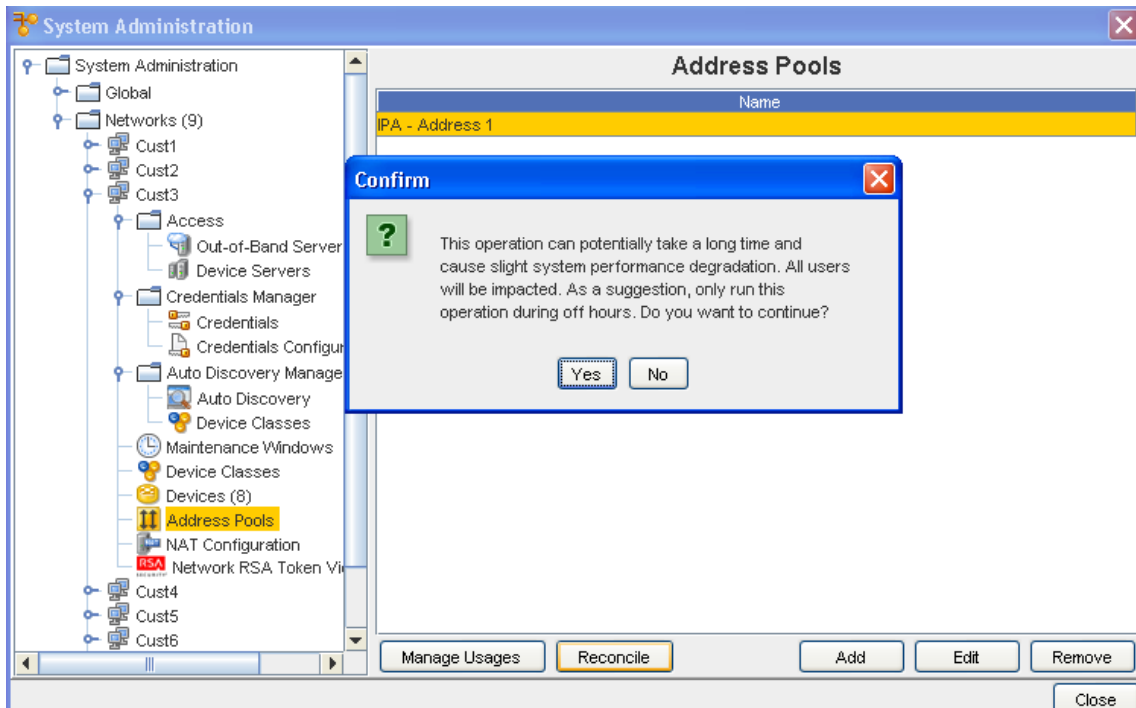
---

**Important** Take care in using Reconcile, as it is an application-intensive process.

---

To reconcile an out-of-sync IP Address pool,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Address Pools**. The Address Pools List window opens. All existing IP Address Pools are displayed.
- 3 Select the Address Pool that is out-of-sync, then click **Reconcile**.



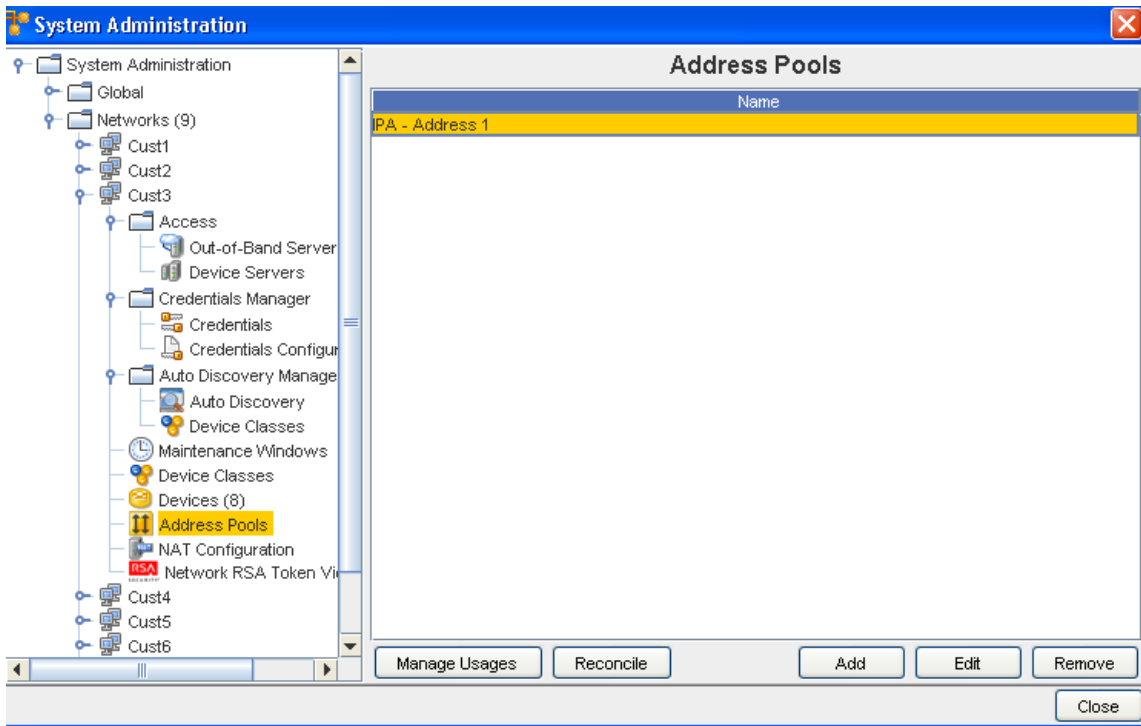
- Carefully read the Confirm message, then select **Yes** to complete the task, having been made aware of the effects, or select **No** to end this activity.

### Adding an IP Address Pool

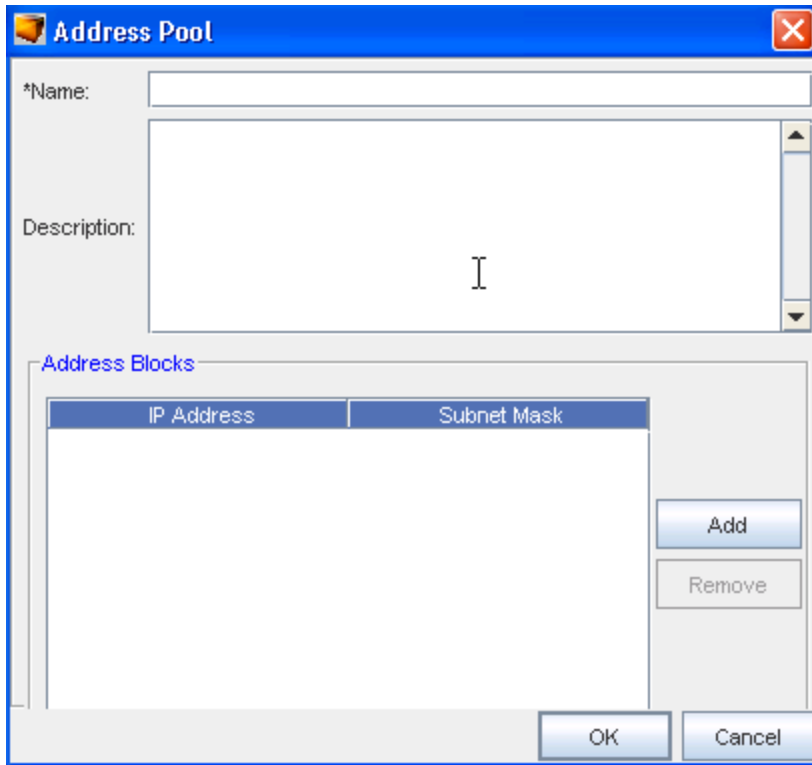
IP Address pools are added in a flat topology, and can only be used with the network in which it is created. Voyence does not allow you to create an overlapping IP Address block.

To add an IP Address to the network pool,

- From the menu bar, select **Tools -> System Administration**.
- Next, select **Network -> Address Pools**. The Address Pools List window opens. All existing IP Address Pools are displayed.

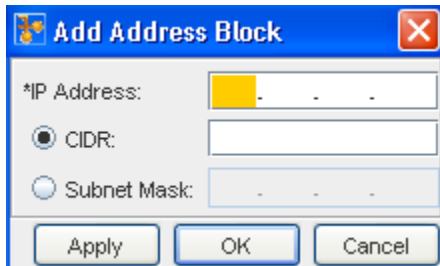


3 At the bottom of the window, click **Add**. The Address Pool window opens.



4 At a minimum, you must enter a **name for the pool**. Once the IP Address Pool has been named, the name cannot be modified.

- To define the IP addresses, click **Add**. The Add Address Block window opens. At a minimum, the **IP Address** must be defined in this Add Address Block window. A **CIDR** or **Subnet** for the IP Address must also be entered.




---

**Note** When the CIDR and Subnets are defined, and when the IP Address matching is queried, the specified details must also match.

---

- If you are entering more than one IP Address pool, click **Apply**. Both the IP Address List and Add Address Block window refreshes. Or, if you are entering a single block, click **OK**.

The Add Address Block window closes, and the IP Address is added to the IP Address List window.

### Editing an IP Address Pool

With the current design of IP Address Pools, you can:

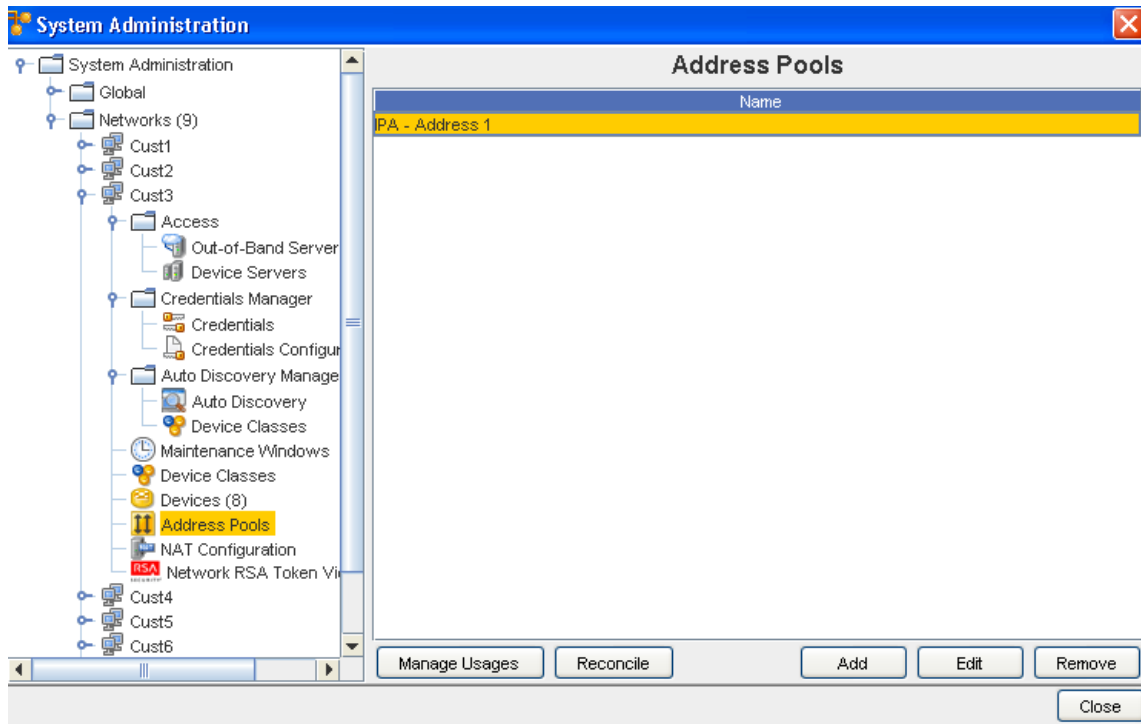
- Add IP Addresses to a block
- Insert a description of the pool
- Delete an existing IP Address from the block

The ability to add an IP Address to an existing block uses the same instructions as provided in the [Adding an IP Address Pool](#) topic.

To edit the IP Address Pool description,

- From the menu bar, select **Tools -> System Administration**.
- Next, select **Network -> Address Pools**. The Address Pools List window opens. All existing IP Address Pools are listed.
- At the bottom of the window, click **Edit**.





The Address Pool window opens.

- 4 Make any changes needed, then click **OK**.

To remove an IP Address Pool from a block,

- 1 Open the Network IP Address Pool list.
- 2 At the bottom of the window, click **Edit**. The Address Pool window opens.
- 3 From the list of IP Address within the pool, select the **pool** you want deleted.
- 4 Click **Remove**. The window updates.
- 5 When finished, click **OK**. The Address Pool window closes.

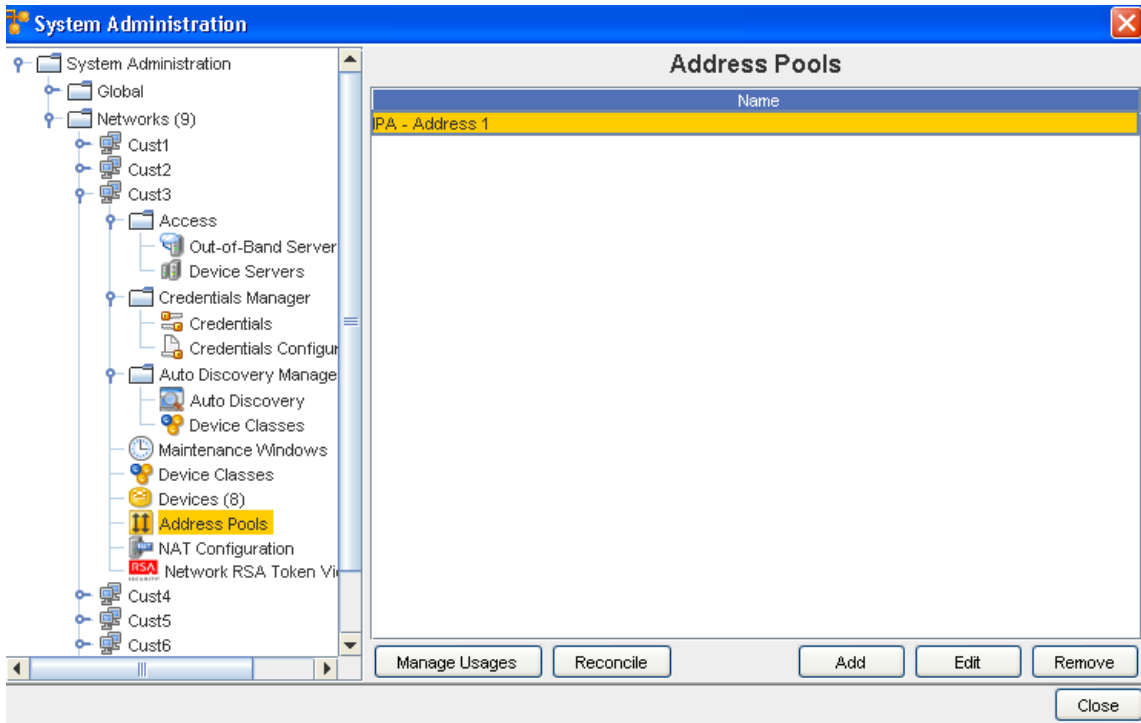
### Excluding IP Addresses

The ability to manage the usage of IP Address has four options:

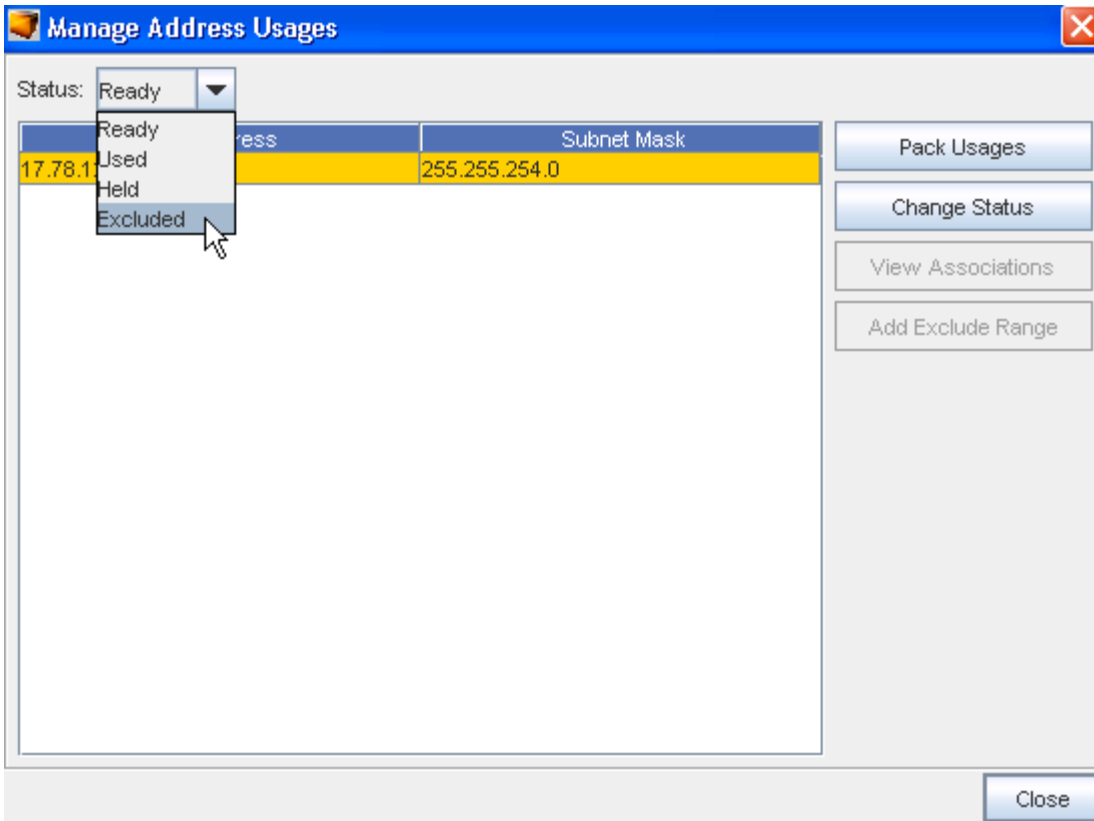
- Pack Usages
- Change IP Address Status
- View the Associates of the IP Address
- Add Exclude Range

To excluded ranges within an IP Address range,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Address Pool**. The Address Pools List window opens. All existing IP Address Pools are listed.



- 3 Select an Address pool, then click **Manage Usages**. The Manage Address Usages window opens.



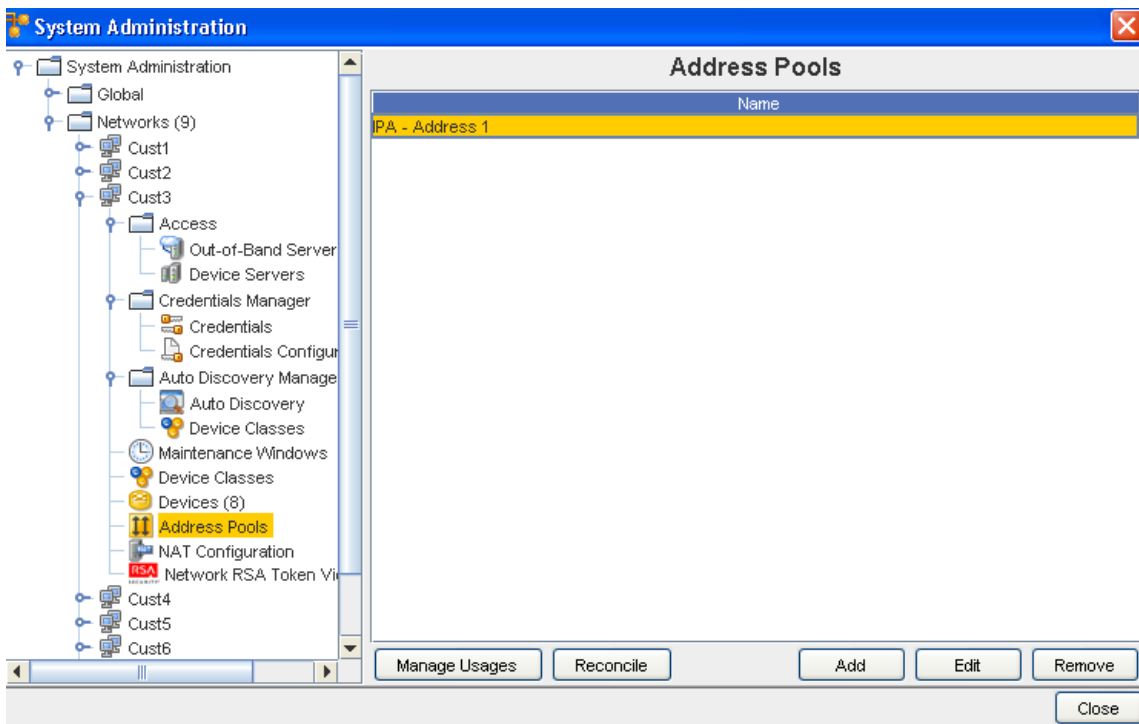
- 4 From the Status drop-down select **Excluded**. The Add Exclude Range window opens.
- 5 From the drop-down list, select an **Address Block**.
- 6 In the IP Address field, enter the **IP** that will be excluded.
- 7 Enter the **CIDR**.
- 8 Optionally, enter a **Subnet** if needed.
- 9 When finished, click **OK**. The Add Exclude Range window closes. The Manage Address Usages window updates.

### Pack IP Address Pool Usage

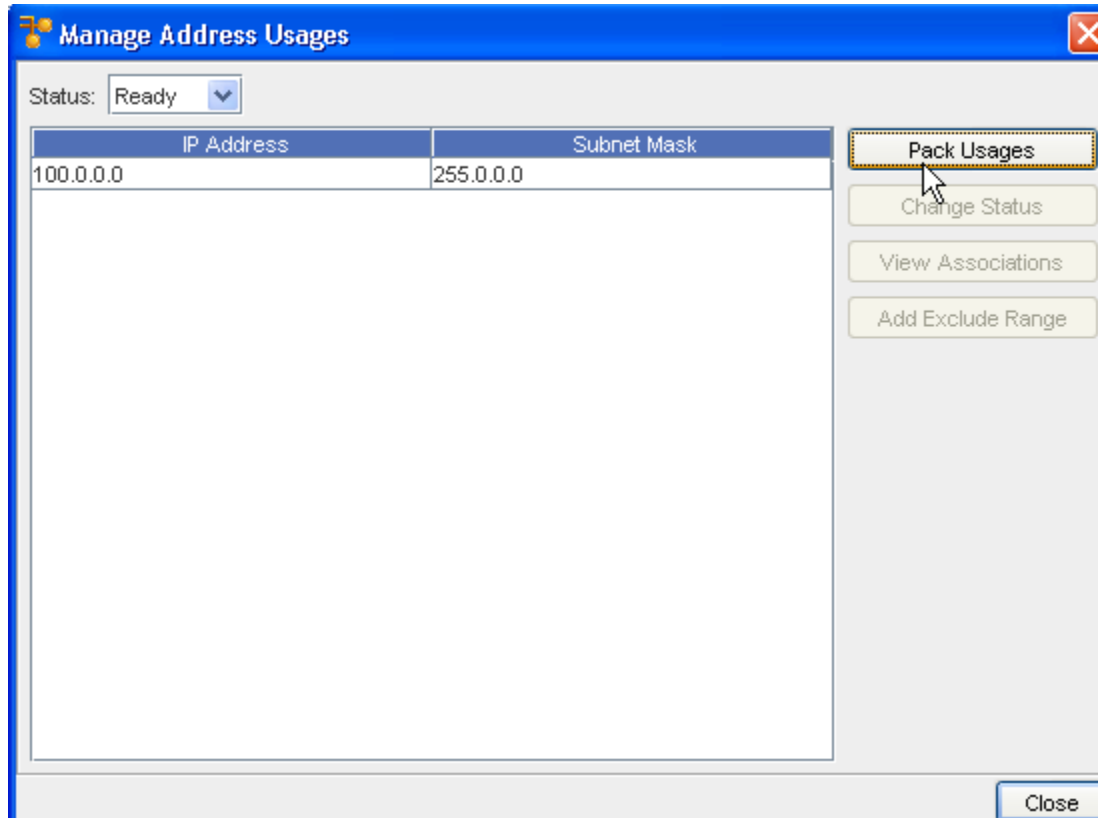
The Pack Usages feature activates a system review of devices to summarize the use of the IP address. Once summarized, the other options are updated with current IP address details on each device.

To access and use the Pack IP Address Pool Usage,

- 1 From the menu bar, select **Tools -> System Administration** .
- 2 Next, select **Network -> Address Pool**. The Address Pools List window opens. All existing IP Address Pools are listed.



- 3 Next, click **Manage Usages**.
- 4 Click **Pack Usages** . From here, you can then use the Pack feature to allocate, or re-allocate IP addresses as requested.



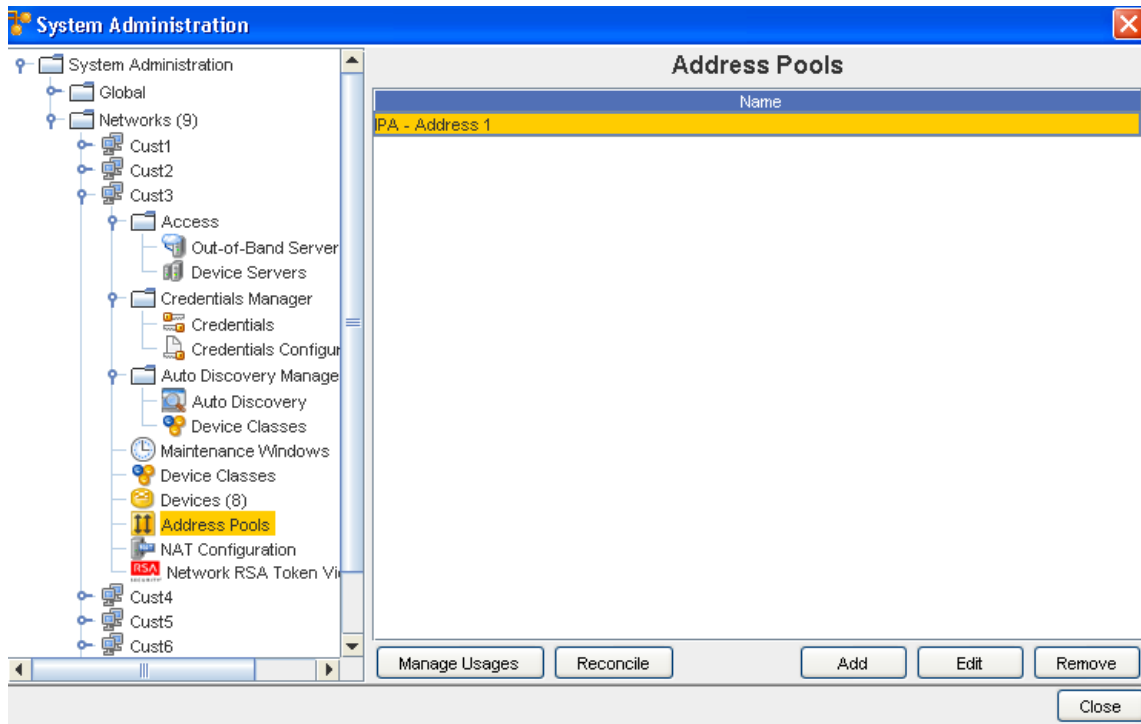
### Removing an IP Address Pool

**Note** This feature is also available using the API.

IP address blocks can be deleted when they are no longer useful to the network. When deleting address blocks, all IP addresses defined for the block are also deleted.

To delete Address blocks defined for a network,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Address Pools**. The Address Pools List window opens. All existing IP Address Pools are listed.
- 3 Select the IP Address block that needs to be removed.



**Note** For added integrity, address blocks can only be deleted one at a time.

- 4 Click **Remove**.
- 5 At the Confirm message, click **Yes** to continue and remove this Address Pool. Note the information within the confirmation message. Click **No** to cancel this removal action.

## Networks - NAT Configuration

### NAT Configuration - Overriding Device Server IPs

Network Address Translation (NAT) configuration allows both the System Administrator and the Network Administrator to define an IP address for each Device Server to **override** the existing IP address of that Device Server.

- 1 From the menu tool bar, select **Tools**, then **System Administration**.
- 2 Expand the **Network** section, and go to **NAT Configuration**.

### Network-Specific NAT Setup

Administrators can define an IP address for each Device Server within a network that will then be the **Device Server IP Address** for that network.

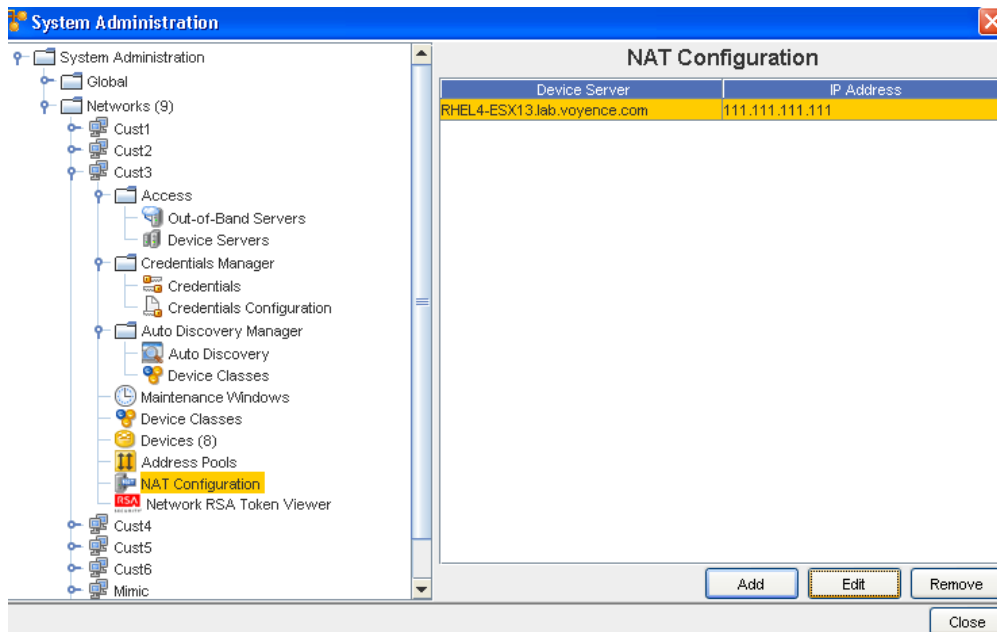
**Note** Only One IP Address is allowed for each Network-Device Server combination.

The new IP Address then affects all devices that consider that network to be the "primary" network. The new IP Address will be the address the Server uses to communicate to the devices.

For example, in a Telnet/TFTP managed device, when the Network Configuration Manager Device Server telnets to the device, it sends the configured NAT IP address needed for the device to TFTP to its configuration. This is used for any communication originating from the device back to the Device Server, including event-based pulls (which is also cached on the device server).

To add a NAT IP Address,

- 1 From the NAT Configuration window, select a **Device Server** from the listing, then click **Add**.
- 2 At the Add NAT IP window, select a **Device Server** from the options shown in the drop-down arrow.
- 3 Enter the **NAT IP Address** you want to use to for the selected Device Server.
- 4 Click **Ok** when you have entered the IP Address. You can also use Cancel to leave this window without saving any new text.



### Additional Tasks - Editing and Removing NAT IPs

- You can Select to **Edit** any existing Device Servers in the NAT Configuration window by first selecting the Device Server from the list, clicking **Edit**, then making the needed IP Address changes. Once your changes are make, click **Ok**.
- To **remove** (delete) existing Device Servers from the list in the NAT Configuration widow, first select the Device Server, then click **Remove**. At the confirmation window, select **Yes**.

## Device-Specific NAT Setup

A Network Administrator can **override** the Device Server IP Address for a specific device. This can be completed using two Quick Commands.

- **View NAT Setup** : View NAT Setup shows only device-specific Device Server NAT IP, and not the network-wide NAT setting.
- **Setup NAT** : If there is no IP Address provided at the time of Setup, the existing setup is to be cleaned. This is provided as a method of re-setting a previous configuration (if any exists). If the device override is set, then that server address is used, regardless of any other configuration setting.

To setup a Device-Specific NAT - from the Devices View,

- 1 From the **Devices View**, select a device with an existing Device Server IP Address that you want to override.

State	Device Name	IP	Device Class
	Switch	172.22.2.73	Cisco IOS Switch
	Nortel-450	172.22.2.80	Nortel Baystack
	<b>VPN-3000-2</b>		<b>Cisco VPN Con...</b>
	Cat190		Cisco CatOS S...
	lansw	Compliance Audit...	Alcatel OmniSw...
	netvar	Enforce Policy	Adtran NetVanta
	Lab-4	Cut-Through ▶	Nortel BoSS Sw...
	Tasma	Editor ▶	Tasman Router
	Adtran	Edit Device ▶	Adtran NetVant...
	LAB-4	Pull ▶	Nortel Baystack
	ASN-1	Quick Commands ▶	Nortel Router
	netvar	Saved Commands	Test Credentials
	350t	Save To...	<b>Setup NAT</b>
	Passp	Update OS Image	View NAT Setup
	Nortel-	Wizards ▶	OSUpgrade
	NetVa	Navigations ▶	Clear Cache
	Tasma	Compare Configs	Cisco PIX
	pix1	Properties	Nortel BoSS Sw...
	bps20		Cisco VPN Con...
	Cisco3		Cisco IOS Router
	r1841-		Tasman Router

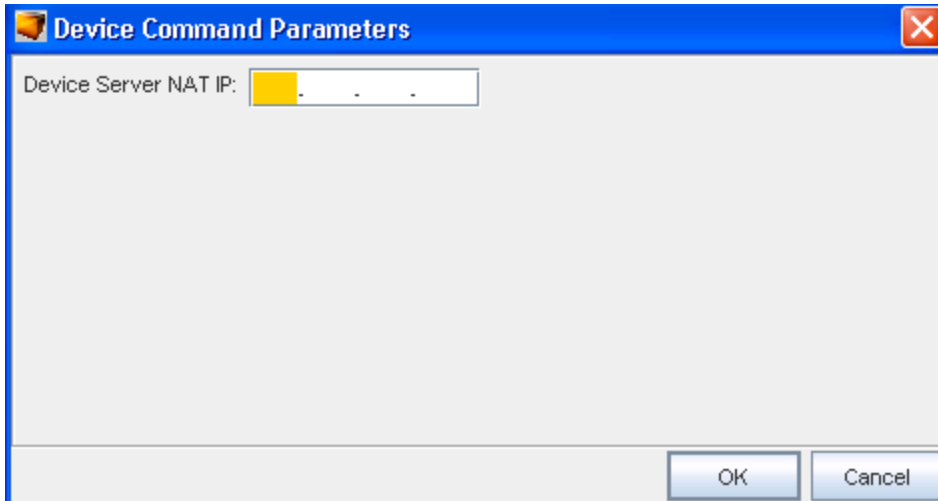
- 2 **Right-click** on the selected device to view the right-click options, then select **Quick Commands** from the list. Now, select **Setup NAT** from the Quick Commands list.

---

**Note** You can also select **View NAT Setup** from this Quick Commands option.

---

The Device Command Parameters window now displays.

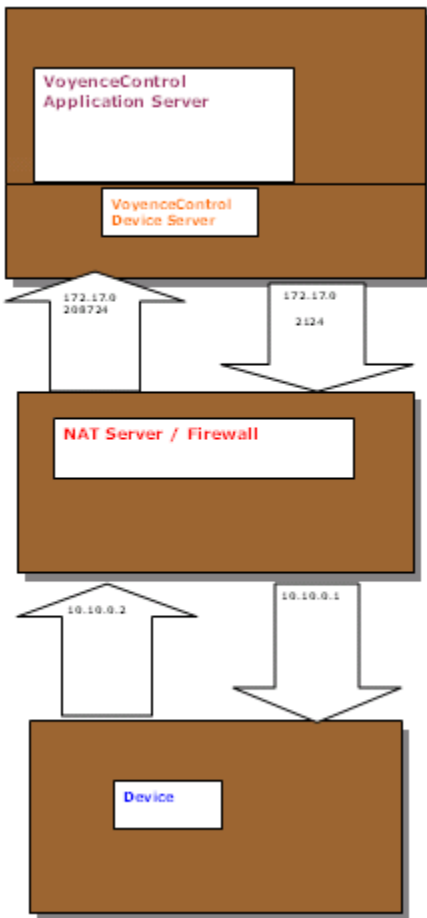


3 Enter the **Device Server NAT IP Address** into the field provided, then click **OK**.

Review the [NAT Setup - Example](#).

### NAT Setup - Example

Following is an example of a Network Address Translation (NAT) setup.





## Working with Change Audit

### Working with Change Audit

To access the Change Audit report, use one of these methods:

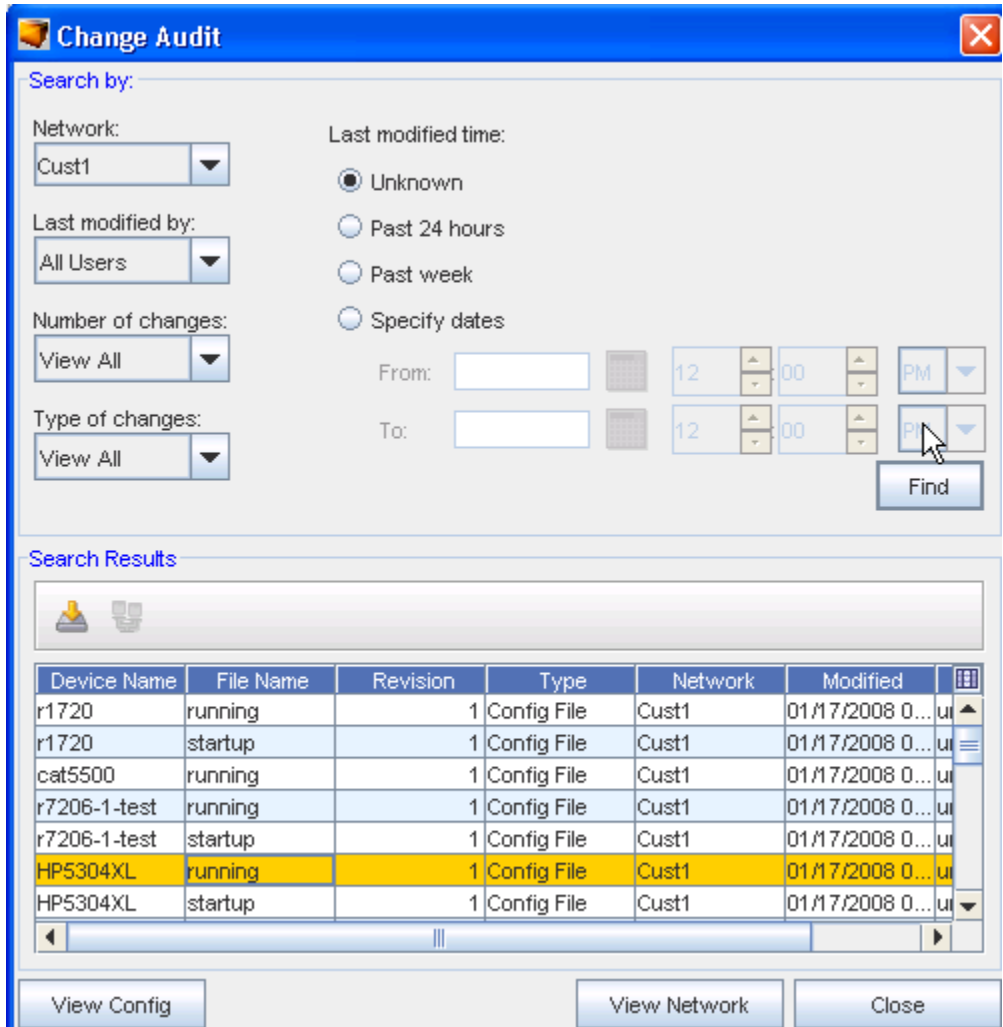
To generate a Change Audit report,

- Click the drop-down arrow on **Network:** to see that specific customer listing, and to make a selection from the list.
- Click the drop-down arrow on **Last modified by:** to make your filter selection based on who last modified the devices information. You have the All User's, EXTERNAL, System, and Voyence options to select from.
- Click the drop-down arrow on **Number of Changes:** to make your filter selection based on the number of changes you want to display. You can View All changes, or select 10, 20, 30, 40 or 50 as the number of changes to display.
- Click the drop-down arrow on the **Type of Changes:** to make your filter selection based on the type of changes you want to display. You can select from View All, Config (to view configuration changes only), or Hardware (to view hardware changes only).
- Make a selection from the **Last modified time:** options. You can select from:

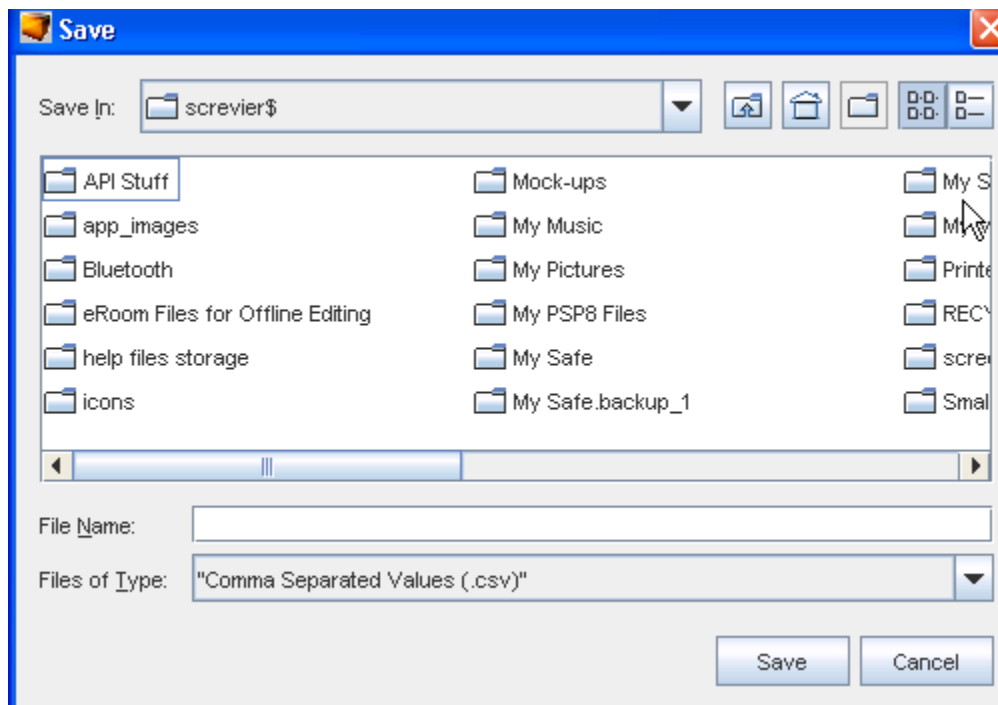
### Search Results - Save

In the Search Results, you have several options to select from:

- Save
- Compare



When Save is selected, the Save window opens.

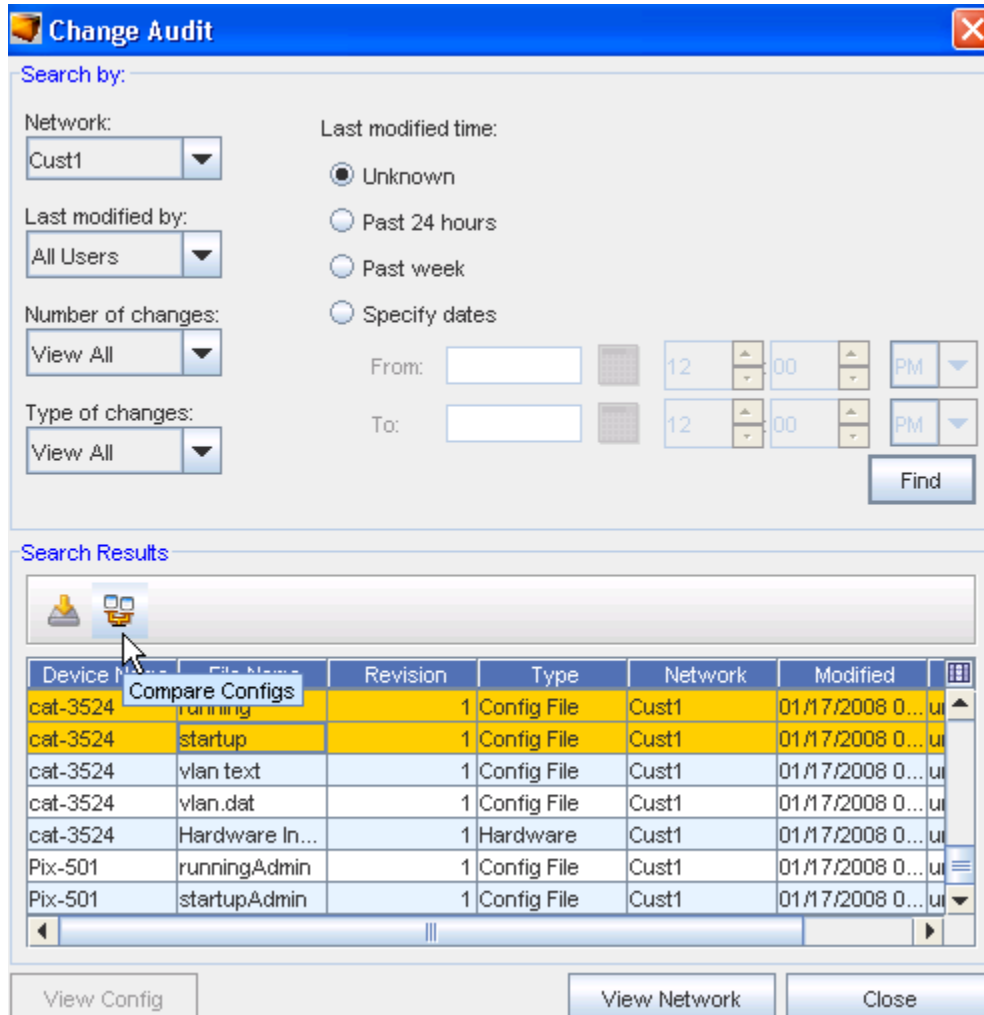


- 1 Continue to go through the **Save** windows, until you select the Save location.
- 2 Click **Close** to leave this window.

## Search Results - Compare

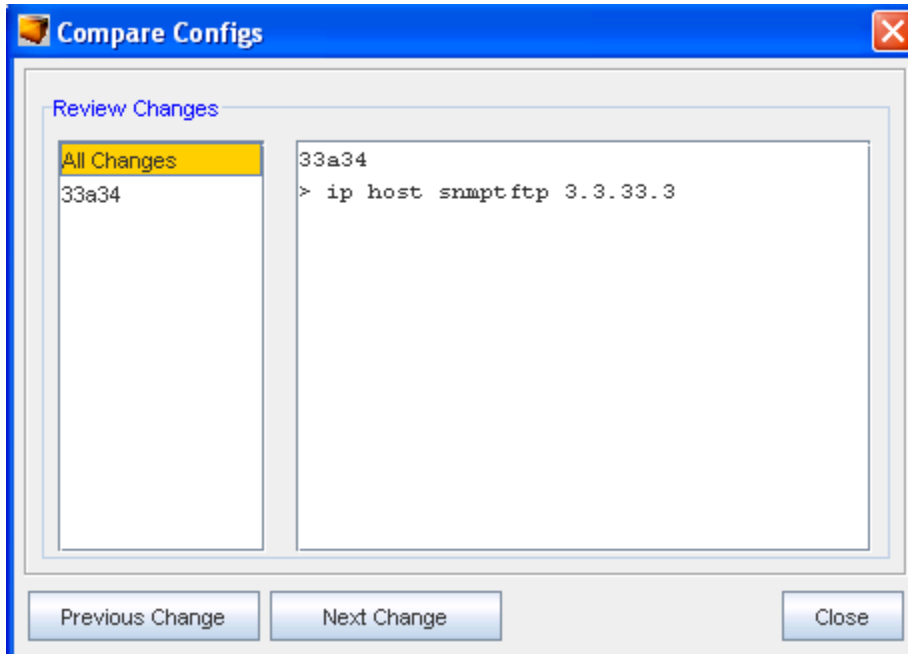
In the Search Results, you have several options to select from:

- Save
- Compare



- 1 You must first **select two separate configurations** from the listing, then select the **Compare Configs** icon.

Once the Compare icon is selected, the two configs are displayed.

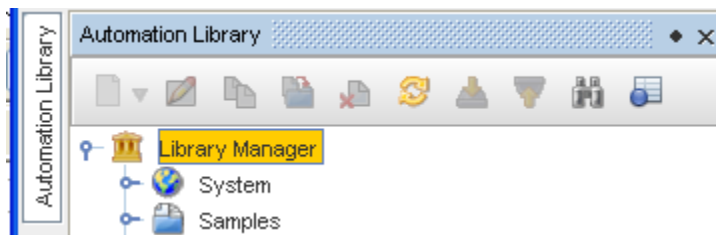


- 2 You can then select to see the **Previous Change** (if applicable) or go to the **Next Change** (if applicable) to compare the Configs.

## Automation Library

### Working in the Automation Library

From the menu bar, access **Tools -> Automation Library** .



At the top level, the Library Manager contains:

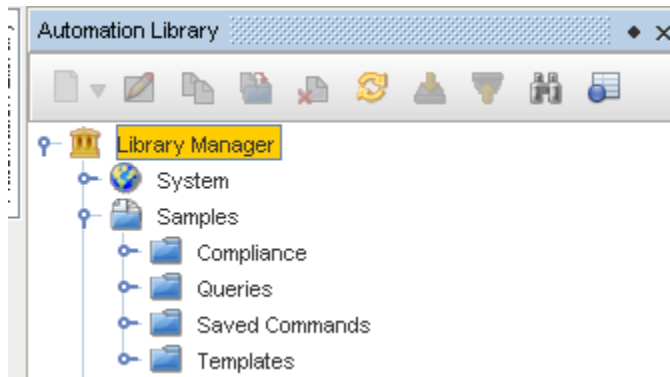
- A **System** folder, which is accessible only to users with System Administration privilege

The system folder is read-write by a user (or System Admin) with System-level **Manage Compliance**, and read-only privileges, as well as access to all other users.

- A **Samples** folder, which is accessible to all users but whose (recursive) content is read-only

- A **folder** for each network defined in the system, where the user has (at a minimum) **View Access** , such as Network1, where that name corresponds to the name of a network. This folder is writable if the user has Manage Compliance privileges, otherwise this folder is read-only.

Within these folders, which are create by the application and cannot not be deleted or modified, other folders can be created, allowing a complex path hierarchy to be developed. Each folder can hold any type of automation library object .






The Samples section contains:

- **Compliance**, including:
  - **RegEx Compliance Tests** – is a compliance test, constructed using regular expression matching and substitutions, applied to a textual configuration file or diagnostic output
  - **Attributed Compliance Tests** – is a compliance test, based on a Query of the Attributed Model, and a set of rules to determine if the result set is compliant
  - **Queries** – Attributed Model queries are templates that define database searches of the Data Model objects
  - **Saved Commands** – is a body of text (containing variables), which can be pushed to the device as a set of commands
  - **Templates** – is a body of text (containing variables), which can be pushed to the device to make a configuration change


### Automation Library - Tool bar




Icon	Action
	Edit - opens the editor for the item you have selected
	Copy - copies the item you have selected, and allows you to designate the copy to destination

-  Move - moves the item you have selected, and allows you to designate the move to destination


---

-  Delete - allows you to delete a selected item


---

-  Refresh - refreshed your current view after any changes


---

-  Export - allows you to export an item from your system or network


---

-  Import - allows you to import an item you have previously exported into your system or network

---

-  Search - opens a Search window for you to enter information for your search criteria

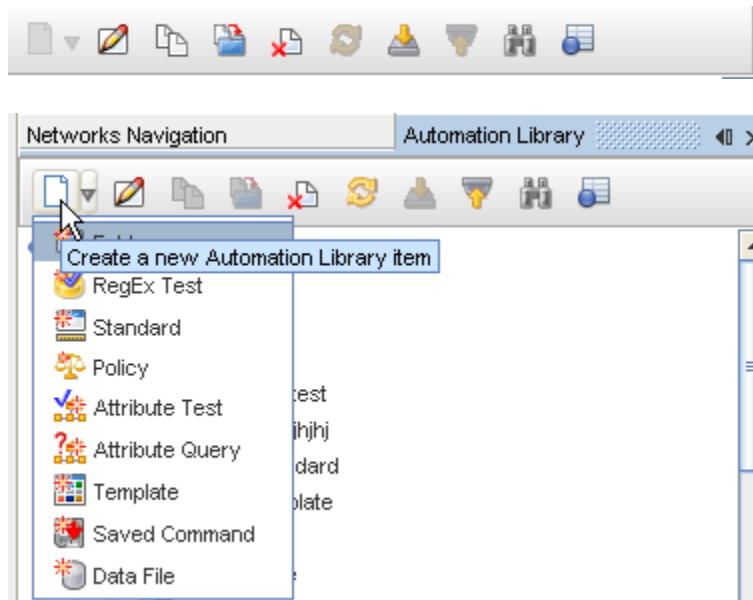
---











-  Automation Library Properties View - opens another window to detail the item name and the path

## Automation Library - Tool bar

The Automation Library tool bar helps you work with the items contained within the System and Sample sections.

Once opened, the following tool bar icons can be accessed to complete actions.



Icon	Action
	When the down arrow is clicked, you can select to create a new library item from the options displayed (as shown in the above graphic).
	Edit - opens the editor for the item you have selected
	Copy - copies the item you have selected, and allows you to designate the copy to destination
	Move - moves the item you have selected, and allows you to designate the move to destination
	Delete - allows you to delete a selected item
	Refresh - refreshes your current view after any changes
	Export - allows you to export an item from your system or network
	Import - allows you to import an item you have previously exported into your system or network
	Search - opens a Search window for you to enter search criteria
	Automation Library Properties View - opens another window to detail the item name and the path

## Using Search in Library Manager

One of the first things you may want to do is **locate an item** within the Automation Library. This feature saves you valuable time when searching for any of the following:

- Attributed Query
- Attributed Test
- Data File
- Policy
- RegEx Test
- Saved Command
- Standard

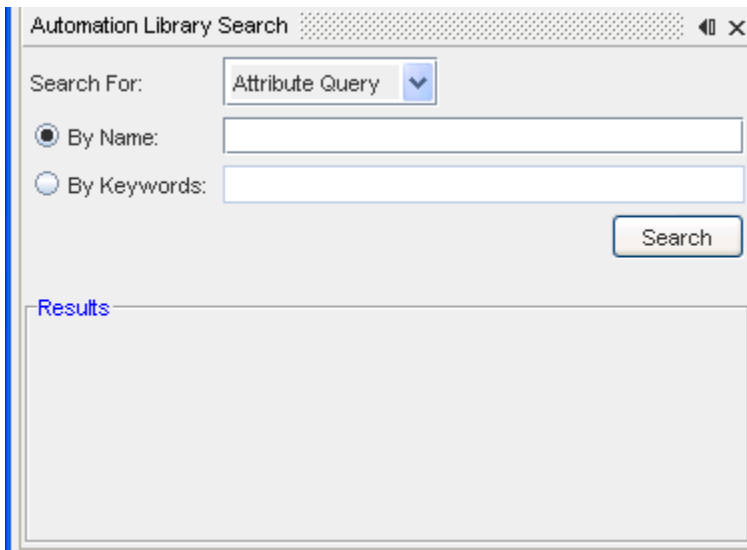


- Template

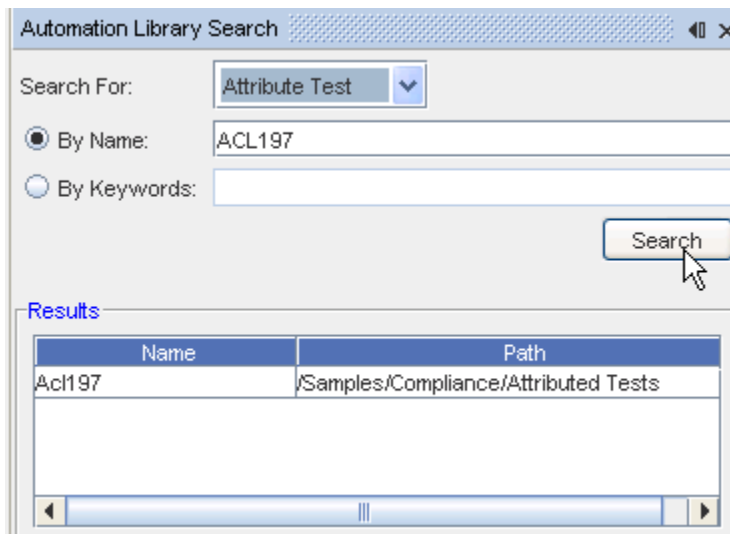
- 1 With the Automation Library displayed, right-click the **Library Manager** to get to the **Search** option.

**Important** The System right-click menu also includes the **Refresh feature** . Use the Refresh when changes have been made to the Automation Library.

- 2 The Automation Library Search window opens in the lower section of the Automation Library tree. From here, you can click the **Search For:** drop-down arrow, and make a selection from the listing. You can also enter a **Name** or enter **keywords** to use as search criteria.
- 3 Once your search filtering is selected or entered, click **Search**.



Your search Results are now displayed.



- 4 To view the actual **ACL197 Attributed Test** (or the results of your search criteria), double-click on the item in the Results.

## Attributed Model

### Introducing the Attributed Model (AM)

#### About the Attributed Model

The AM allows you to interactively view data within it from within the Network Configuration Manager User Interface, using a facility called a **Query**. Queries are similar to reports displayed in a spreadsheet-like manner. The AM also allows you to construct Attributed Compliance Tests (ACT) against the results of Queries.

---

**Note** The AM facilities do not replace the textual, configuration-based, model of Devices within Network Configuration Manager. Rather, the AM facilities are an extension to the existing facilities, allowing you to use the most appropriate tool for the task.

---

### Introducing the Data Model

#### Understanding the Data Model

The Data Model is comprised of **Objects** that are represented in **Database tables**. This allows the contents of the Objects to easily be searched, displayed by the User Interface, formatted into Reports, and subject to Compliance Tests.

Each of these **Objects** has a set of **Attributes** that may be present. Some Attributes are required to be present, whereas others are optional.

While most of the Attributes in an Object typically represent information collected about the Device's configuration or operational state, all Objects in the Database have some additional Attributes that are used to facilitate their storage in the database, such as database keys.

The **Attributes** may be of various types. Here are the currently supported primitive types.

Type	Description
Boolean	A true or false value.
ByteArray or byte[]	An array of bytes. This is used to represent certain Database keys (OIDs).
Date	A date value.
GenericString	A string field which may have unusual sorting properties. This type is appropriate for strings that might represent different types, as Access List Names, that might be numeric on some routers and alpha-numeric on others.
Integer	A signed, 32-bit numeric value.
InetAddressString	A string that represents an IP Address.
ListObject	A list of values, typically numeric values, or strings representing numeric values. For example, a list of service types in an access list rule, e.g. "telnet ftp". Spaces should be used as separators between items in the list.
Long	A signed, 64-bit numeric value.
String	A string value.
Time	A time value.
Timestamp	A date and time time-stamp, for example in a log entry.

The external representation of the Data Model is defined by an XML schema known as the DeviceConfigurationState.xsd, and other associated **Metadata** maintained in Network Configuration Manager's Database, and in the Device Packages.

The schema is subdivided into Configuration Units, which represent a unit of information that Device drivers know how to **pull or push** .

Each Device Package may have its own unique set of supported Configuration Units, however a Configuration Unit must be configured in the **Metadata** to be accessible by Network Configuration Manager.

The Metadata used by the application is visible within the application, by selecting **Tools** then **Metadata**.

See: **Object Types**

## Object Types

The **Object types** currently supported are shown in the following table, along with the **Configuration Unit** they are derived from, and a **description of the Object** .

Details of each Object Type, and its Attributes is provided in the following sections.

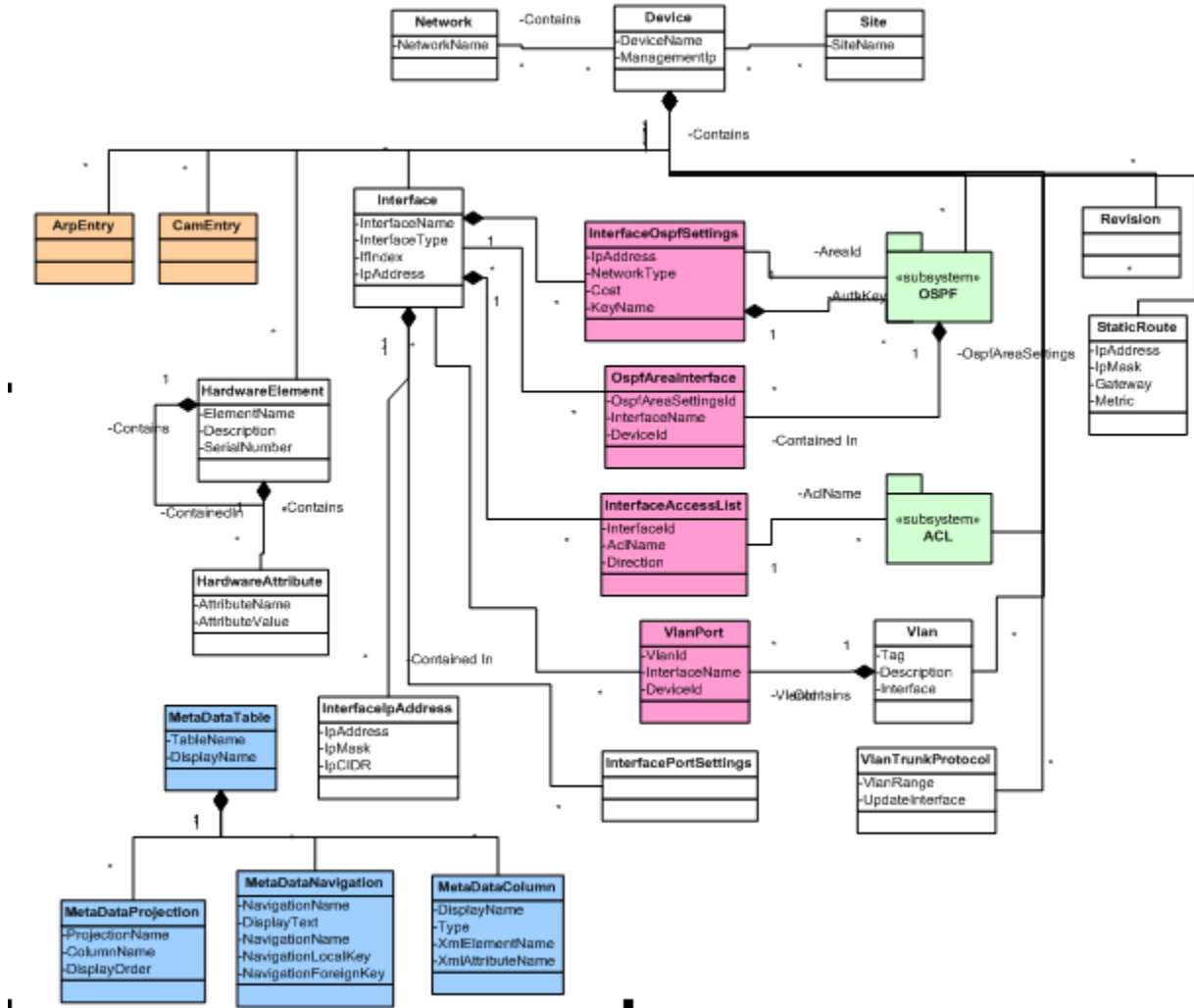
Object	Configuration Unit	Object Description
<a href="#">AccessList</a>	Access Control Lists	<a href="#">Access Control List</a> . These can be of various types such as basic or extended.
<a href="#">AclDstNetworkGroup</a>	Access Control Lists	Destination Address of a host in a Network Group
<a href="#">AclDstPortGroup</a>	Access Control Lists	Source Port for a transmission protocol in a Port Group
<a href="#">AclExtendedRule</a>	Access Control Lists	Access List Extended Rule used for Cisco IOS like devices
<a href="#">AclGroupedRule</a>	Access Control Lists	Access List Grouped Rule used for Juniper, PIX, Linux
<a href="#">AclOption</a>	Access Control Lists	Uninterpreted (device package specific) options for an access control list.
<a href="#">AclSrcNetworkGroup</a>	Access Control Lists	Source Address of a host in a Network Group
<a href="#">AclSrcPortGroup</a>	Access Control Lists	Source Port for a transmission protocol in a Port Group
<a href="#">ArpEntry</a>	ARP Table	<a href="#">Arp Table</a> . This is operational data, not data specified in the Device's configuration.
<a href="#">AuthKey</a>	Interfaces, OSPF Settings	<a href="#">Authentication Key for OSPF Interfaces and Virtual Interfaces</a> .
<a href="#">CamEntry</a>	CAM Table	<a href="#">MAC address to Port Table</a> . This is operational data, not data specified in the Device's configuration.
<a href="#">Device</a>	Device Identity, System Properties	<a href="#">A discovered Device in Vovence Control</a> . The model does not display information on Virtual or Workspace devices
<a href="#">HardwareAttribute</a>	Physical Hardware	Extensible attributes of a Hardware Element. Can be any property discovered by the Device Driver.
<a href="#">HardwareElement</a>	Physical Hardware	<a href="#">Hardware elements (components) and their properties</a> . Examples would be Chassis, Card, Bus.
<a href="#">Interface</a>	Interfaces	<a href="#">A Device's Interfaces</a> .
<a href="#">InterfaceAccessList</a>	Interfaces	The Access Lists applied to an Interface.
<a href="#">InterfaceIpAddress</a>	Interfaces	The IP addresses for an Interface
<a href="#">InterfaceOspfSettings</a>	Interfaces	These are the <a href="#">OSPF settings</a> for a particular interface.
<a href="#">InterfacePortSettings</a>	Interfaces	These are the feature settings for a particular Port or Interface
<a href="#">InterfaceVlanSettings</a>	Interfaces	<a href="#">An interface's VLAN settings</a> .
<a href="#">Network</a>	<none>	<a href="#">A Network container in Vovence Control</a> .

<a href="#">NetworkGroup</a>	Access Control Lists	A group of network addresses used for ACL rule source or destination addresses.
<a href="#">NetworkGroupEntry</a>	Access Control Lists	A particular entry in the Network Group table that represents one Network Address.
<a href="#">OspfAdminDistance</a>	OSPF Settings	Configuration of Administrative Distances of OSPF (metric compared with other routing protocols)
<a href="#">OspfAreaInterface</a>	OSPF Settings	OSPF Area of the interface
<a href="#">OspfAreaNetwork</a>	OSPF Settings	OSPF Networks associated with an Area
<a href="#">OspfAreaRange</a>	OSPF Settings	Maps a group of network area ranges to an OSPF area settings entry.
<a href="#">OspfAreaSettings</a>	OSPF Settings	Configuration for an OSPF area.
<a href="#">OspfDistributeList</a>	OSPF Settings	Configuration of the OSPF Distribute List.
<a href="#">OspfNeighbor</a>	OSPF Settings	Configuration of OSPF neighbors.
<a href="#">OspfRedistributeList</a>	OSPF Settings	Configuration of the OSPF Redistribute List.
<a href="#">OspfRestrictList</a>	OSPF Settings	Configuration of the OSPF Restrict List, which indicates IP Networks that are restricted from advertisement to other routers
<a href="#">OspfRouterSettings</a>	OSPF Settings	Configuration settings for an OSPF routing instance.
<a href="#">OspfSummaryNetwork</a>	OSPF Settings	Configuration of IP Networks Summarized in OSPF.
<a href="#">OspfVirtualLink</a>	OSPF Settings	Configuration of an OSPF virtual link within an OSPF Area.
<a href="#">PortGroup</a>	Access Control Lists	A group of Ports specified as a named entity in an Access List rule.
<a href="#">PortGroupEntry</a>	Access Control Lists	A single port entry in a Port Group.
Revision	<none>	A table of configuration unit revisions in Vovence Control per device.
Site	<none>	Properties of a physical Site that may contain Devices in Vovence Control.
<a href="#">StaticRouteEntry</a>	Routes	A static route table entry that is in the Device's configuration.
<a href="#">ValidationError</a>	<none>	A table of Validation Errors that may be associated with a Device (indicating there were data inconsistencies detected when the Device's Modeled Configuration was pulled).
<a href="#">Vlan</a>	VLANs	The configuration settings for a VLAN.
<a href="#">VlanInterfaces</a>	VLANs	A table showing what interfaces are a member of each VLAN.
<a href="#">VlanTrunkProtocol</a>	VLANs	Configuration settings for the protocol used for the exchange of VLAN tags on a trunk

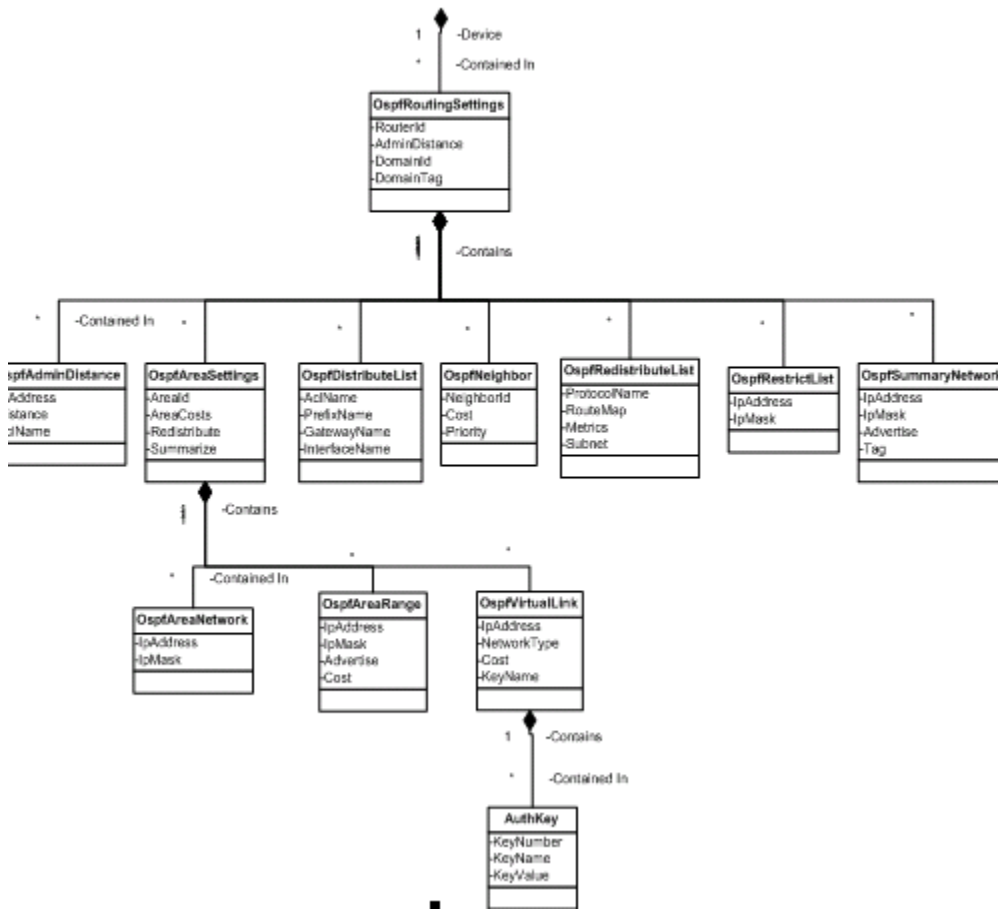
The different Object types have hierarchical relationships, which are also described in the Metadata. For example, a Network contains Devices, which in turn contains Interfaces, each of which, in turn, may have one or more Interface IP Addresses associated with it. A pictorial relationship of the Object types is depicted in the UML drawings below.

In the Model UML diagrams, boxes represent **Object classes**, and lines represent **relationships between classes**. The existence of a line extending between two boxes on the diagram (usually) implies there will be one or more relationships (referred to as Navigations) defined between the two Object classes. As an example, there is a Navigation from Device to AccessList, and from AccessList to AclExtendedRule or AclGroupedRule.

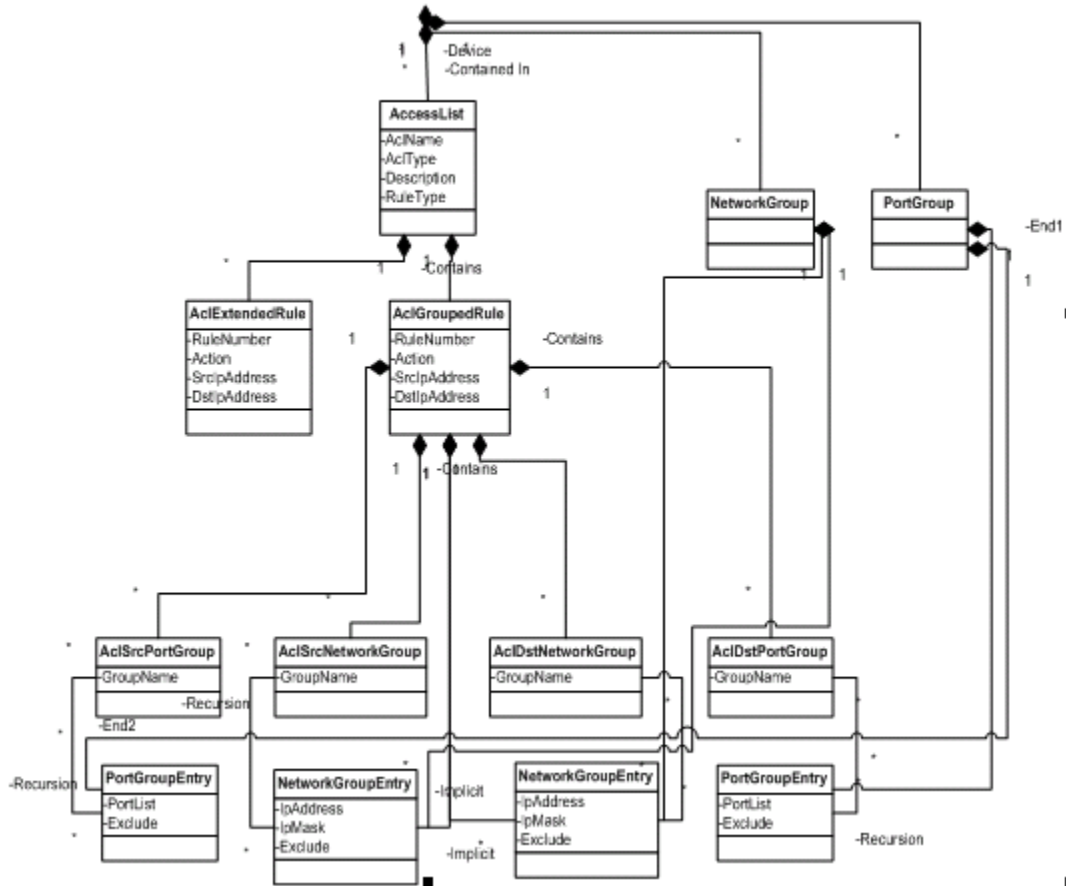
Device properties, Interfaces, Hardware, Arp entries, CAM entries.



The OSPF sub-system



### The Access List (ACL) Subsystem



See: [Model Object Types](#)

## Model Object Types

A detailed description of each Object Type in the model is presented in this section.

### AccessList

**Description:** Represents an Access Control List on the Device. AccessLists are represented in the model by two distinct flavors, each having a different type of rule. Cisco style access lists have rules of type AcIExtendedRule (which allow only one source and destination address per rule); Juniper, PIX, Linux, and some other devices have access lists that use rules of type AcIGroupedRule (which allow multiple source or destination addresses per rule).

**Parent Object Type(s):** Device

**Child Object Type(s):** AcIExtendedRule, AcIGroupedRule

**Ordered By:** AcIName

Sample config text:

```
r2621(config)#access-list 100 ?
deny Specify packets to reject
```

dynamic Specify a DYNAMIC list of PERMITs or DENYs

permit Specify packets to forward

remark Access list entry comment

#### Attributes support in Access List:

Display Name	Type	Description
AclName	String	Access list name (or number for ACLs without names).
AclType	String	Type of Access List, e.g. Extended, Standard, Juniper, Pix, or Rate-Limit.
Description	String	User description of ACL.
DeviceId	Long	ID of device containing ACL.
RuleType	String	Rule entry type: AclExtendedRule or AclGroupedRule

### AclDstNetworkGroup

**Description:** A NetworkGroup used for Access List destination addresses

**Parent Object Type(s):** AclGroupedRule

**Child Object Type(s):** NetworkGroupEntry

**Ordered By:** GroupName

See NetworkGroup for a list of attributes.

### AclDstPortGroup

**Description:** A PortGroup used for Access List destination ports

**Parent Object Type(s):** AclGroupedRule

**Child Object Type(s):** PortGroupEntry

**Ordered By:** GroupName

See PortGroup for a list of attributes.

### AclExtendedRule

**Description:** A Cisco type Access List rule within an AccessList. This can be a Standard or Extended rule. The extended rule is used to capture a full set of extended attributes and may be sparsely populated only as needed to collect the attributes of the rule.

**Parent Object Type(s):** AccessList

**Child Object Type(s):** none

**Ordered By:** RuleNumber

Sample configuration text:

```
r2621(config)#access-list 100 permit ip ?
```

A.B.C.D Source address

any Any source host



host A single source host

r2621(config)#access-list 100 permit ip

% Incomplete command.

r2621(config)#access-list 100 permit ip ?

A.B.C.D Source address

any Any source host

host A single source host

r2621(config)#access-list 100 permit ip host 1.1.1.0 ?

A.B.C.D Destination address

any Any destination host

host A single destination host

r2621(config)#access-list 100 permit ip host 1.1.1.0 any ?

dscp Match packets with given dscp value

fragments Check non-initial fragments

log Log matches against this entry

log-input Log matches against this entry, including input interface

precedence Match packets with given precedence value

time-range Specify a time-range

tos Match packets with given TOS value

<cr>

⊕ Attributes supported in AclExtendedRule:

Display Name	Type	Description
<u>Ack</u>	Boolean	ACK tcp-flag.
<u>AclRuleDescription</u>	String	User description of rule. (Most devices do not implement this.)
<u>Action</u>	String	Action to take on packet if the rule matches.
<u>Dscp</u>	Integer	Diff-serv code point. Small integer value.
<u>DstIpAddress</u>	<u>IpAddressString</u>	Destination IP address (IPV4 or IPV6).
<u>DstIpCIDR</u>	<u>IpAddressString</u>	Constructed IP conglomerate used for comparisons.
<u>DstIpNetMask</u>	String	Destination IP Net Mask. (These are true Net Masks, not Wildcard entries).
<u>DstMac</u>	String	Destination MAC for layer 2 packets.
<u>DstMacMACADDR</u>	String	Constructed destination MAC for comparisons.
<u>DstPortList</u>	<u>ListObject</u>	Destination port low range or single port value.
<u>DynamicName</u>	String	Name of dynamic ACL.
<u>EspSpi</u>	String	Value of IPSEC Security Parameter Index
<u>EthernetType</u>	Integer	Ethernet type code.
<u>Fin</u>	Boolean	Fin tcp-flag.
<u>ForwardingClass</u>	String	Current forwarding class of packet.
<u>FragOffsetRange</u>	String	Frag offset range.
<u>IcmpCode</u>	Integer	ICMP code for ICMP packets.
<u>IcmpMessage</u>	String	ICMP message for ICMP packets.
<u>IcmpType</u>	Integer	Type code for ICMP packets.
<u>IgmpTypeList</u>	<u>ListObject</u>	IGMP type code for IGMP packets.
<u>IpPrecedence</u>	Integer	IP precedence value.
<u>IpProtocolList</u>	<u>ListObject</u>	Ip protocol list or range
<u>IsEstablished</u>	Boolean	Boolean indication a TCP connection is established.
<u>IsFragment</u>	Boolean	Boolean indicating packet is a fragment.
<u>LogInput</u>	Boolean	Enable the logging of input interface
<u>LogPackets</u>	Boolean	Boolean indicating packets should be logged.
<u>MacPrecedence</u>	Integer	MAC precedence value.

<a href="#">MatchCount</a>	Long	The device rule counter for this rule.
<a href="#">PacketCounter</a>	String	Name of packet counter associated with ACL rule.
<a href="#">PacketLength</a>	Integer	Packet length of IP packet.
<a href="#">Psh</a>	Boolean	<a href="#">Psh tcp-flag</a> .
<a href="#">RedirectPort</a>	Integer	Port number packets matching packets should be redirected to
<a href="#">ReflexiveEvaluate</a>	String	Evaluate the indicated reflexive ACL.
<a href="#">ReflexiveName</a>	String	Name of Reflexive Acl.
<a href="#">RejectCode</a>	Integer	ICMP reject code that should be sent when packets match rule.
<a href="#">Rst</a>	Boolean	Reset tcp-flag
<a href="#">RuleNumber</a>	Integer	Rule number with the ACL.
<a href="#">SetForwardingClass</a>	String	Set matching packet's forwarding class to specified field.
<a href="#">SetLossPriority</a>	String	Set matching packets loss priority to specified field.
<a href="#">SetRateLimiter</a>	String	Set matching packets rate limiter to specified field.
<a href="#">SrcIpAddress</a>	<a href="#">IpAddressString</a>	Source IP address in rule (IPV4 or IPV6).
<a href="#">SrcIpCIDR</a>	<a href="#">IpAddressString</a>	Constructed IP/mask conglomerate for address comparisons.
<a href="#">SrcIpNetMask</a>	String	Source IP Net Mask. (These are true Net Masks, not Wildcard entries).
<a href="#">SrcMac</a>	String	Source MAC for layer 2 packets.
<a href="#">SrcMacMACADDR</a>	String	Constructed source MAC operator for comparisons.
<a href="#">SrcPortList</a>	<a href="#">ListObject</a>	List of source ports or port ranges
<a href="#">Syn</a>	Boolean	<a href="#">Syn tcp-flag</a> .
<a href="#">TimeRange</a>	String	Name of time range association. (Cisco)
<a href="#">TypeOfService</a>	Integer	IP type of service value
<a href="#">Urg</a>	Boolean	<a href="#">Urg tcp-flag</a> .

## AclGroupedRule

**Description:** A Juniper style Access List rule within an AccessList. The ACL Grouped rule extends the basic rule settings allowing lists of attribute values and groups of IP addresses, Subnets, and Ports. The ACL Grouped Rule is only supported by certain classes of equipment allowing list and dynamically created attributes to be assigned to rules. The rule will usually be associated with one or more Network Groups or Port Groups specifying the network IP addresses, Network Masks, and Ports.

**Parent Object Type(s):** AccessList

**Child Object Type(s):** AclOption, DstNetworkGroup, DstPortGroup, SrcNetworkGroup, SrcPortGroup

**Ordered By:** RuleNumber, SrcIpAddress, DstIpAddress, SrcPortList, DstPortList (in that order). (Note that if a Device does not supply rule numbers, the Device driver will generate them automatically so as to keep the rules in proper order).

Attributes supported in AclGroupedRule:

Display Name	Type	Description
<a href="#">Ack</a>	Boolean	ACK tcp-flag.
<a href="#">AclRuleDescription</a>	String	User description of rule. (Most devices do not implement this.)
<a href="#">Action</a>	String	Action to be taken if the rule matches.
<a href="#">ActionTarget</a>	String	Device package specific target for the action that was specified.
<a href="#">AhSpiExceptList</a>	ListObject	Except these AH SPI values
<a href="#">AhSpiList</a>	ListObject	Ah Spi values.
<a href="#">DscpExceptList</a>	ListObject	Except these dscp values
<a href="#">DscpList</a>	ListObject	Diff-serv code point. Small integer value.
<a href="#">DstAddressTypeList</a>	ListObject	List of possible destination address types.
<a href="#">DstInterface</a>	String	Destination (egress) interface
<a href="#">DstIpAddress</a>	IpAddressString	Destination IP address (IPV4 or IPV6).
<a href="#">DstIpCIDR</a>	IpAddressString	Constructed IP conglomerate used for comparisons. To be implemented.
<a href="#">DstIpNetmask</a>	String	Destination IP Net Mask (not a wild card).
<a href="#">DstMac</a>	String	Destination MAC for layer 2 packets.
<a href="#">DstMacMACADDR</a>	String	Constructed destination MAC for comparisons.
<a href="#">DstNetworkGroup</a>	String	A Network Group name that contains a list of Network Addresses to be used for destination address matching in this rule.
<a href="#">DstPortGroup</a>	String	A Port Group name that contains a list of Ports to be used for destination matching in this rule.
<a href="#">DstPortList</a>	String	Destination port range or single port value.
<a href="#">DynamicName</a>	String	Name of dynamic ACL.
<a href="#">EspSpiExceptList</a>	ListObject	Except these esp spi values
<a href="#">EspSpiList</a>	ListObject	IP SEC ESP SPI List.
<a href="#">EthernetTypeList</a>	ListObject	Ethernet type code.
<a href="#">Fin</a>	Boolean	FIN tcp-flag.
<a href="#">ForwardingClassExceptList</a>	ListObject	Except these forwarding classes.
<a href="#">ForwardingClassList</a>	ListObject	Current forwarding class of packet.
<a href="#">FragOffsetExceptList</a>	ListObject	Except these fragment offsets
<a href="#">FragOffsetRangeList</a>	ListObject	Fragment offset range.
<a href="#">IcmpCodeList</a>	ListObject	ICMP code for ICMP packets.
<a href="#">IcmpMessage</a>	String	ICMP message for ICMP packets.
<a href="#">IcmpTypeExceptList</a>	ListObject	Except these ICMP types.
<a href="#">IcmpTypeList</a>	ListObject	Type code for ICMP packets.

<a href="#">IcmpTypeExceptList</a>	<a href="#">ListObject</a>	Except these ICMP types.
<a href="#">IcmpTypeList</a>	<a href="#">ListObject</a>	Type code for ICMP packets.
<a href="#">IgmptypeList</a>	<a href="#">ListObject</a>	IGMP type code for IGMP packets.
<a href="#">IpPrecedenceExceptList</a>	<a href="#">ListObject</a>	Except these ip precedence values
<a href="#">IpPrecedenceList</a>	<a href="#">ListObject</a>	IP precedence list
<a href="#">IpProtocolExceptList</a>	<a href="#">ListObject</a>	Except these IP protocol values.
<a href="#">IpProtocolList</a>	<a href="#">ListObject</a>	IP protocol list range or single value.
<a href="#">IsEstablished</a>	Boolean	Boolean indication a TCP connection is established.
<a href="#">IsFragment</a>	Boolean	Boolean indicating packet is a fragment.
<a href="#">IsInitial</a>	Boolean	Is this an initial fragment in the packet
<a href="#">LogInput</a>	Boolean	Boolean indicating input should be logged.
<a href="#">LogOptions</a>	String	Logging options for this rule.
<a href="#">LogPackets</a>	Boolean	Boolean indicating packets should be logged.
<a href="#">MacPrecedence</a>	Integer	MAC precedence value.
<a href="#">MatchCount</a>	Long	The match count for the rule in the Device.
<a href="#">PacketCounter</a>	String	Name of the packet counter associated with this ACL rule.
<a href="#">PacketLengthExceptList</a>	<a href="#">ListObject</a>	Except these packet lengths
<a href="#">PacketLengthList</a>	<a href="#">ListObject</a>	Packet length of IP packet.
<a href="#">Psh</a>	Boolean	PSH tcp flag.
<a href="#">RedirectPortList</a>	<a href="#">ListObject</a>	Port number packets matching rule should be redirected to.
<a href="#">ReflexiveEvaluate</a>	String	Evaluate the indicated reflexive ACL.
<a href="#">ReflexiveName</a>	String	Name of the Reflexive ACL.
<a href="#">RejectAsDest</a>	Boolean	Boolean to reject packet as if from the destination address
<a href="#">RejectCode</a>	Integer	ICMP reject code that should be sent when packets match rule.
<a href="#">Rst</a>	Boolean	RST tcp flag.
<a href="#">RuleName</a>	String	The name of the rule, for Device classes that support named rules.
<a href="#">RuleNumber</a>	Integer	Rule number with the ACL
<a href="#">SetForwardingClass</a>	String	Set matching packet's forwarding class to specified field.
<a href="#">SetLossPriority</a>	String	Set matching packets loss priority to specified field.
<a href="#">SetRateLimiter</a>	String	Set matching packets rate limiter to specified field.
<a href="#">SrcAddressTypeList</a>	<a href="#">ListObject</a>	List of possible source address types.
<a href="#">SrcInterface</a>	String	Source (ingress) interface
<a href="#">SrcIpAddress</a>	<a href="#">IpAddressString</a>	Source IP address in rule (IPV4 or IPV6).
<a href="#">SrcIpCIDR</a>	<a href="#">IpAddressString</a>	Constructed IP/mask conglomerate for address comparisons.
<a href="#">SrcIpNetmask</a>	String	Source IP Net Mask (not a Wildcard).
<a href="#">SrcMac</a>	String	Source MAC for layer 2 packets.
<a href="#">SrcMacMACADDR</a>	String	Constructed source MAC operator for comparisons.
<a href="#">SrcNetworkGroup</a>	String	The name of a Network Group that contains a list of IP network addresses to be used for source matching.
<a href="#">SrcPortGroup</a>	String	The name of a Port Group that contains of list of ports used for source matching.
<a href="#">SrcPortList</a>	<a href="#">ListObject</a>	A list of source ports matched against the packet's source port.
<a href="#">Syn</a>	Boolean	SYN TCP flag.
<a href="#">TcpMssList</a>	<a href="#">ListObject</a>	List of possible TCP MSS values matching this rule.
<a href="#">TcpOptionList</a>	<a href="#">ListObject</a>	List of possible TCP options matching this rule.
<a href="#">TimeRange</a>	String	Name of time range association.
<a href="#">TypeOfServiceList</a>	<a href="#">ListObject</a>	List of IP Type of Service values.
<a href="#">Urg</a>	Boolean	URG TCP flag.

## Metadata Information

The data describing the Data Model's Objects and Attributes is itself a part of the model, and is accessible via the standard facilities used to query the model. In addition, there is a model browser within the application that allows you to **navigate** through the model and see the Objects and their attributes.

For example, a device has a **ManagementIp address** , and a collection of **Interface objects** , each of which contains an **InterfaceName**. Each Interface object may contain one or more InterfaceIpAddress objects, which have IpAddress as one of their attributes.

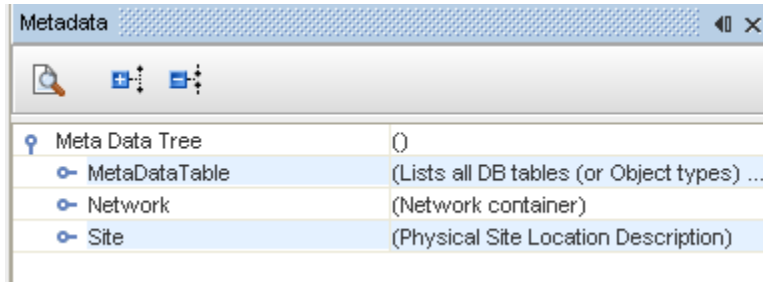
Within Network Configuration Manager, device information (metadata) is offered within the Automation Library. A Device is represented as a collection of Objects, each with certain attributes that describe the current state of the Object.

You can view the Metadata by accessing the **Meta Data tree** .

- 1 Click **Tools** in the Network Configuration Manager main Launch window.
- 2 Next, select **Metadata**.

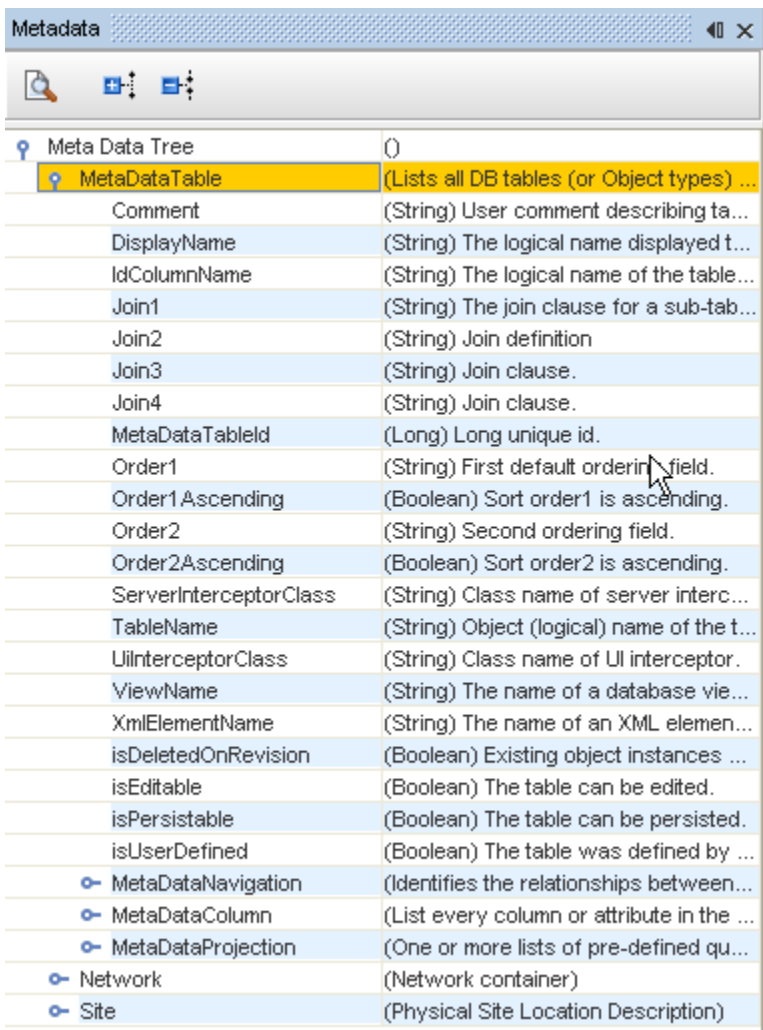


Once opened, you can **expand** the sections (Metadata Table, Network, and Site) to view the information contained within each location.



For example, when the **Meta Data Table** is expanded, the following selections are available. The left side lists the column name within a table, and the right side of the information lists the description of the information contained within that column .

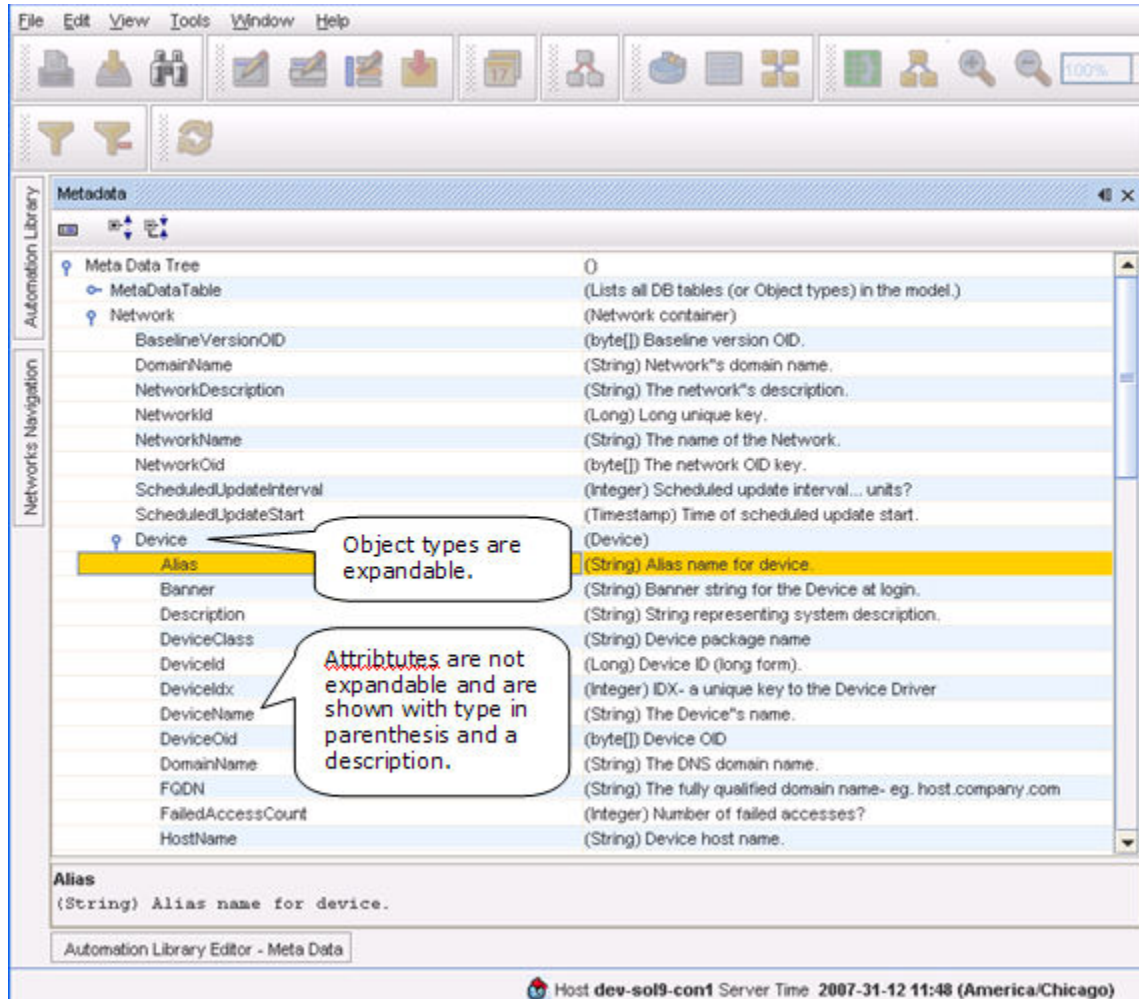
Also, notice that there are other tables available you can expand within this MetaData Table option for more information. For example, from the MetaData Table you can also expand **MetaDataTableColumn** and **MetaDataTableProjection**. Continue to expand on the available information.



A sample browser diagram of part of the Metadata is shown below. Object classes (such as Device or Interface) can be identified because they are expandable to show the Attributes that Object class contain, as well as any Object classes that are contained in the Object that is expanded.

From the example below, Network is expanded to see it contains Device objects, and attributes such as NetworkDescription and NetworkName, and the Device object is expanded to show that it has attributes of Alias, Banner, Description, DeviceClass, etc.

Attributes are shown with their **type in parenthesis** followed by a description of the attribute.





The Meta Data information itself is stored in multiple database tables. These include:

Table DisplayName	Description
MetaDataTable	Contains an entry describing each Object class, such as Device, Network, or Interface. The entry contains information such as the primary key name, default sorting order, and how to construct objects from one or more database tables.
MetaDataColumn	Contains an entry for each attribute of an Object that gives the attributes of that attribute, such as their database column name, type, and information about their XML representation. Each entry in the MetaDataColumn table is associated with a single MetaDataTable entry.
MetaDataProjection	Contains one or more entries for each defined projection of an Object. A projection is a set of columns that may be referenced by a logical name. All objects in the model contain a projection named "basic". Other projections could be defined by adding additional entries. Each entry in the MetaDataProjection table is associated with a single MetaDataTable entry and a single projection name.
MetaDataNavigation	Contains entries that define relationships between objects, such as Object A contains Object B, or Object B is contained in Object A. The MetaDataNavigation table is used to construct relationships from one part of the model to another; for example to find the Interfaces within a Device. Each entry in the MetaDataNavigation table is associated with a single MetaDataTable entry, and it defines one relationship for the Object represented by that entry.
Translation Tables (named md_XXX_translation)	Translation tables are used to translate enumerated values (either integers or internal string representations) to their external string value used for display purposes. For example, the md_protocol_number_translation table contains the information that "tcp" is ip protocol number 6. There are many translation tables defined in the model, each of which translates a set of values for an attribute to their displayable string representation.

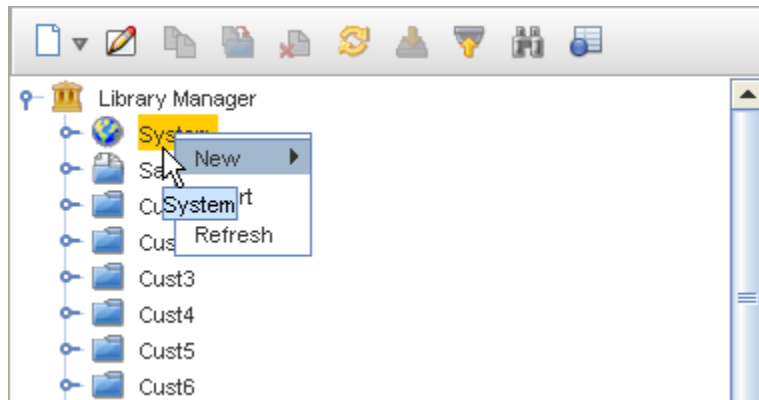
## Library Manager - System

### Working with System in the Automation Library

- 1 First, access **Tools** from the menu bar, then select **Automation Library**.
- 2 Once the Automation Library is displayed, select **System**.

From the **System** link (which is defined as **Global**) within the Library Manager, you can right-click to get the following options:

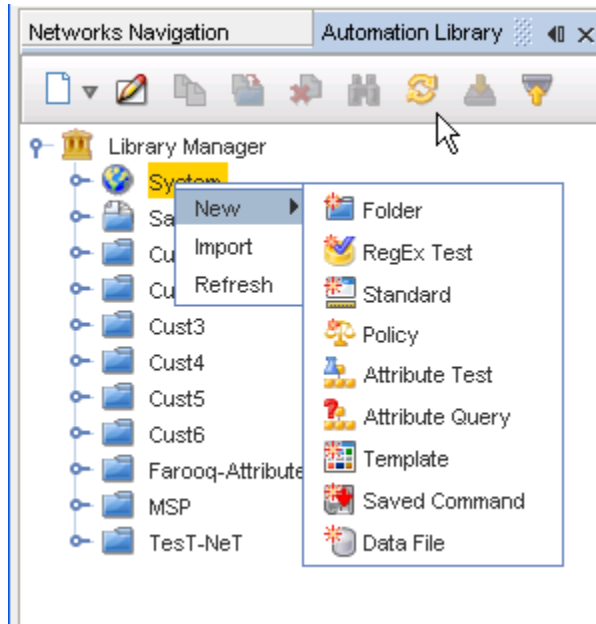
- New
- Import
- Refresh



## New Option

### Creating New Items

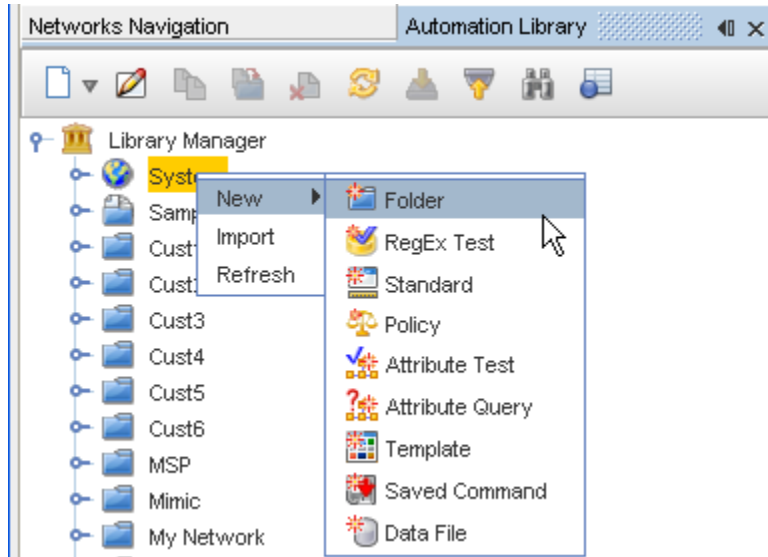
- From the **System** option, you can right-click and select the **New** Option. From this option, the following new items can be created:
  - Folder
  - RegEx test
  - Standard
  - Policy
  - Attribute Test
  - Attribute Query
  - Template
  - Saved Command
  - Data File
- Click **each link** to get the steps needed to create these **New** items.



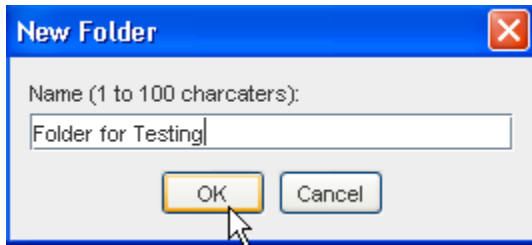
- [Creating System Folders](#) - that resides in the System View
- [Creating a New RegEx Compliance Test](#) - that can be linked to Standards
- [Creating a New Standard](#) - that can be linked into Tests
- [Creating a New Policy](#) - that can be linked to a Standard
- [Creating a New Attributed Test](#) - to be used for testing Compliance
- [Creating a New Attribute Query](#) - used within an Attributed Test
- [Best Practices when using Templates](#) - save reusable configuration commands (known as templates)
- [Creating a New Saved Command](#) - that can be accessed and used from the Devices View
- [Creating a New Data File](#) - created from a template's variables

### Creating System Folders

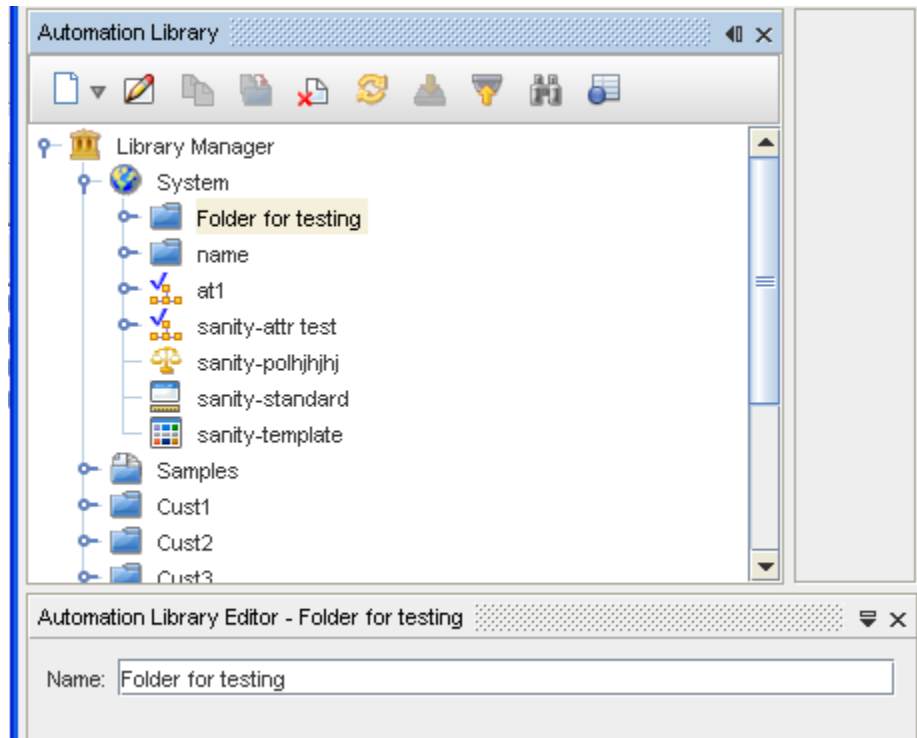
- 1 To create a **New System folder**, you must first select the **Automation Library**.
- 2 When the **Library Manager** opens, right-click on **System**, then select **New -> Folder** .



3 At the New Folder window, enter a **Folder name**, then click **Ok**.



A folder is created under the System folder. If the Automation Library Editor is already open, it displays the folder name.




---

**Important** You can make any changes to the existing name if needed, and then click **Save** while in the Editor.

---

Once a Folder is created, you can complete tasks using the right-click options.

- Click on the Folder name, then:
- Click **Edit** to edit the name of the Folder.
- Click **Delete** to delete a Folder. Click **Ok** at the confirmation message.
- Click **Import** to go to the Open window, and select an item to import into the Folder.
- Click **Refresh** to refresh the list of Folders after changes.

## Import Option

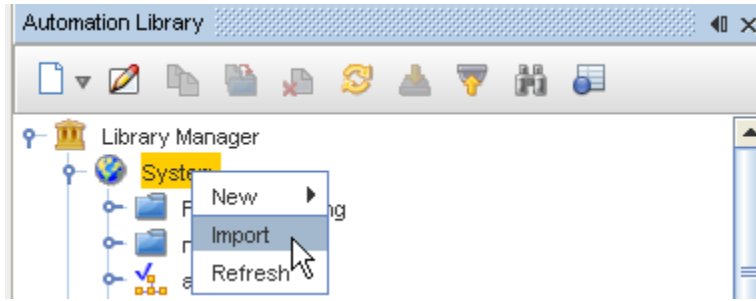
### Importing Items

While working in the Automation Library, **System** has right-click options. You can **Import** items and bring them into the Global System.

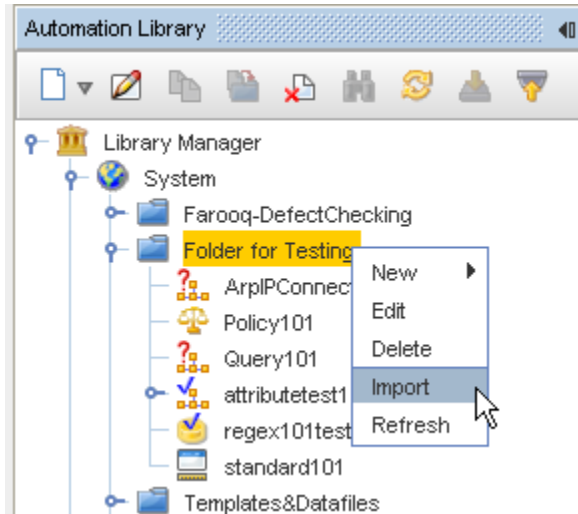
---

**Important** Import can only be completed on those items that have been Exported.

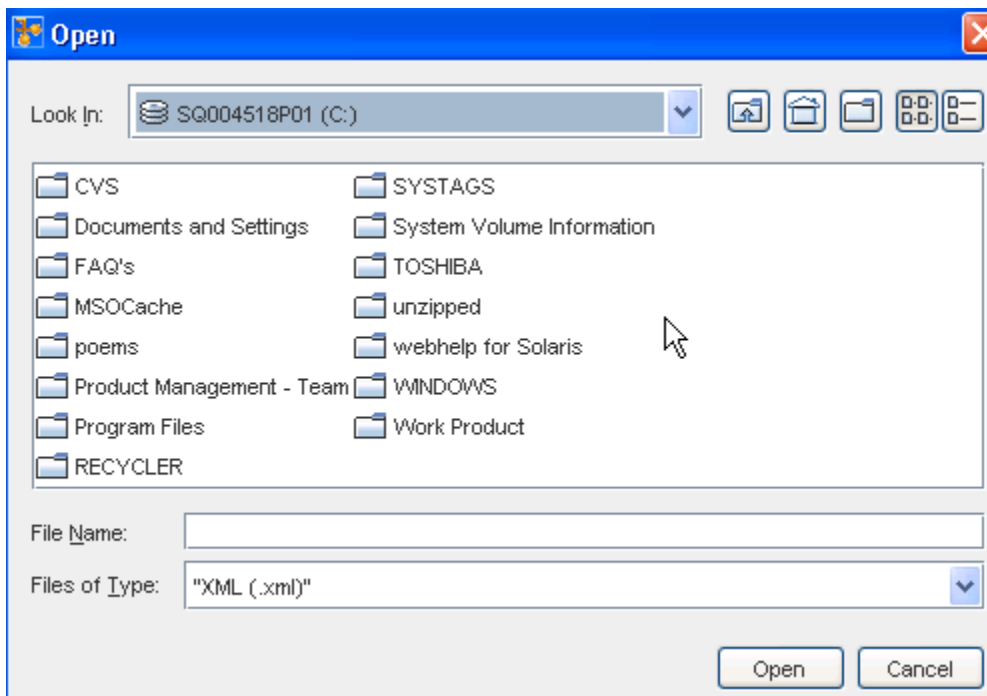
---



You can also import items and bring them into any **Folder** you have within the Global System.



- 1 Once **Import** is selected from the right-click menu, the Open window displays, allowing you to select the item to import.



- 2 Go through the various windows to locate the item you want imported, then click **Ok**.
- 3 In the Files of Type section, select **XML** for importing Attribute Tests, Attribute Queries, RegEx Tests, Templates and Saved Commands.
- 4 Select **CSV** for importing Data Files.

## Refresh Option

### Refreshing the System View

- 1 When you have made changes within System, right-click on the **System**.
- 2 Select **Refresh**.

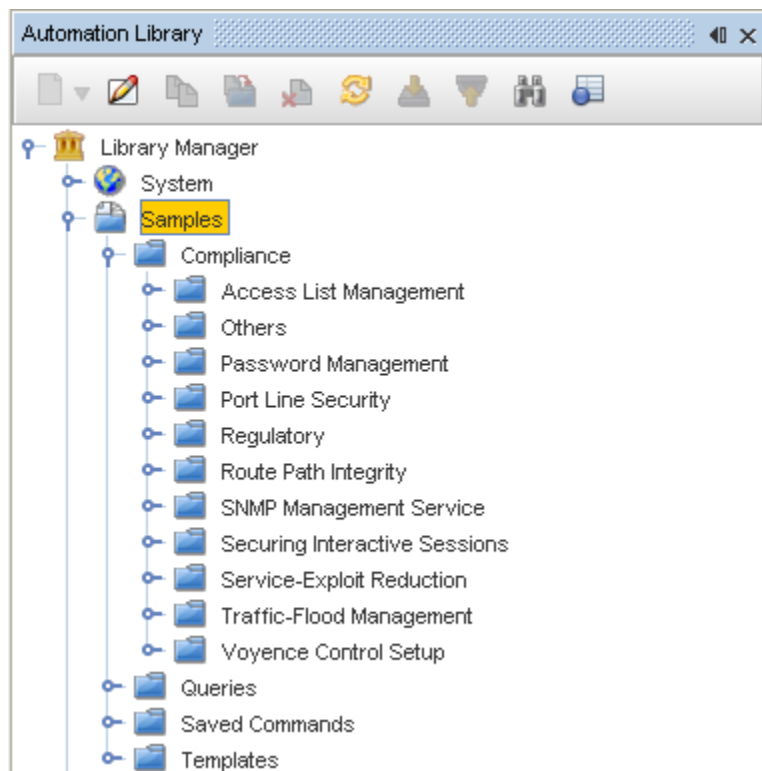
This refresh action ensures your view is the latest and most up-to-date, and includes the most recent changes.

## Library Manager - Samples

### Introducing Test Samples

#### Sample Categories - Available Samples

The following Sample **categories** have been added to the Library Manager **Compliance** section of the Automation Library.



For information on how to begin working with these samples, see [Copying Samples](#).

Each of these categories contains sample RegEx Compliance tests.

---

**Important** The Others category lists the available Attributed Tests.

---

For a more detailed description of each test within these new categories, take time to review the following:

[Compliance - Access List Management Samples](#)

[Others - Samples](#)

[Password Management Samples](#)

[Port Line Security - Samples](#)

[Regulatory](#)

[Route Path Integrity](#)

[SNMP Management Service](#)

[Securing Interactive Sessions](#)

[Service-Exploit Reduction](#)

[Traffic-Flood Management](#)

[Network Configuration Manager Setup](#)

### **Compliance - Access List Management Samples**

The following are some of the samples available under Compliance, **Access List Management** in the Library Manager.

Move your cursor over each sample to view a description of the samples within this category.

NEED GRAPHIC

#### **ACL Ends In Deny Any Any**

This test is for a simple egress Access Control List (ACL), and ensures the ACL ends with a Deny Any Any. To customize this test for a specific network, edit the check pattern to specify permit.

#### **Extended ACL to Disallow Permit of Any Destination Regardless Of Source**

This test ensures that Permit of Any Destination is not in the configuration, regardless of source.

#### **Extended ACL to Disallow Permit of Any Source Any Destination**

This test ensures that Permit of Any Source, and Permit of Any Destination is not in the configuration.

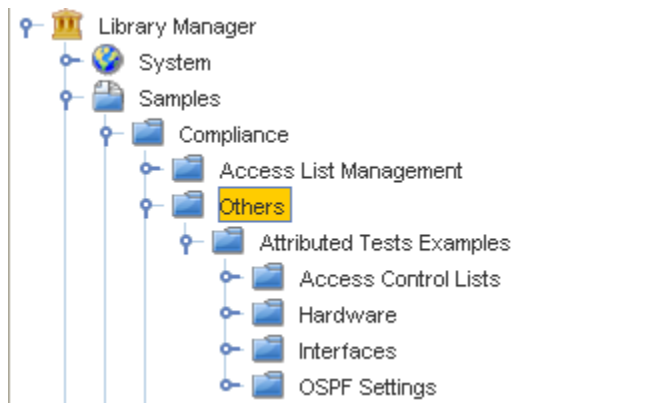
#### **Extended ACL to Disallow Permit of Any Source Regardless Of Destination**

This test ensures that Permit of Any Source is not in the configuration, regardless of destination.



## Others - Samples

This section of the Samples in the Automation library lists other types of samples. For example, here is where the **Attributed Tests Examples** are stored.

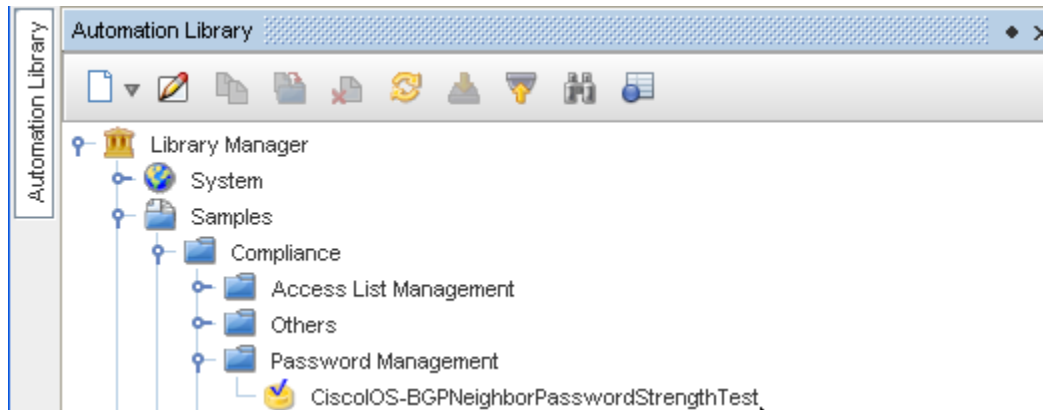


This is also where the Access Control Lists, Hardware, Interfaces and OSPF Settings samples reside.

## Password Management Samples

The following is just one the samples available under Compliance, **Password Management** in the Library Manager.

Move your cursor over each sample to view a description of the samples within this category.



### CiscoIOS-BGPNeighborPasswordStrengthTest

This tests the strength of unencrypted BGP Neighbor Passwords. Passwords must contain at least one lower-case letter, one upper-case letter, one number, and one special character. Passwords must also be at least eight characters long.

---

**Note** There is no remedy supplied.

---

## Port Line Security - Samples

The following is just one of the samples available under Compliance, **Port Line Security** in the Library Manager.

Move your cursor over each sample to view a description of the samples within this category.



### CiscoIOS-Enable Switchport Security per Specified Interface

This test ensures that switch port security is configured correctly on user-specified Non-Shutdown, Non-Loopback, and Non-VLAN interfaces. The device is flagged as non-compliant, if the switch port security is not configured correctly.

### Regulatory

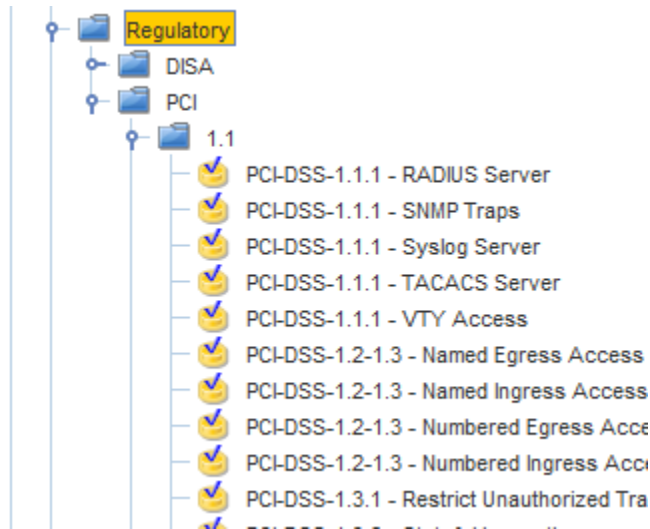
The following are some of the samples available under Compliance, **Regulatory** in the Library Manager.

Move your cursor over each sample to view a description of the samples within this category.

---

**Note** The compliance reporting capability of NCM is enhanced to support DISA/NSA compliance testing. The DISA STIG compliance reports are separate reports that can be run from within the Report Advisor. The PCI Compliance tab in the Report Advisor (RA) is now replaced with Compliance and DISA STIG samples are included in the Automation Library. The DISA STIG compliance reports are now accessible through the "Compliance" tab. The compliance reports are now updated to include DISA Compliance requirements. The required definitions and compliance definitions are available at: <http://iase.disa.mil/stigs>.

---



### PCI-DSS-1.1.1 – RADIUS Server

This test ensures that a user-specified server is setup as a RADIUS server with proper authentication, and also ensures there are no other RADIUS servers other than the specified server.

### PCI-DSS-1.1.1 – SNMP Traps

This test ensures that SNMP Traps are enabled, have been directed at the specified host, and will not be sent to any other location. This sample test only works for SNMPv1 and SNMPv2.

### PCI-DSS-1.1.1 – Syslogs

This test ensures that Syslogs are enabled, pointed at the correct IP address for the Network Configuration Manager Device Server, and ensures that Syslogs will not be sent to any other location.

### PCI-DSS-1.1.1 – TACACS Server

This test ensures that the specified server is configured as the only TACACS+ server, and ensures authentication is setup correctly.

### PCI-DSS-1.1.1 – VTY Access

This test ensures that the specified local account is setup on a device for VTY access, and ensures no other local account is active. This test also deletes all usernames that are not specified by the user, if they exist.

### PCI-DSS-1.2-1.3 – Named Egress Access List – By ACL Name

This test ensures that only valid IP addresses are allowed to exit the network, and ensures that the simple egress access list ends with a Deny Any Any.

### PCI-DSS-1.2-1.3 – Named Ingress Access List – By ACL Name

This test ensures that only valid IP addresses are allowed to enter the network, and ensures that the simple ingress access-list ends with a Deny Any Any.

**PCI-DSS-1.2-1.3 – Named Egress Access List**

This test ensures that only valid IP addresses are allowed to enter the network, and ensures that the numbered egress access-list ends with a Deny Any Any.

**PCI-DSS-1.2-1.3 – Named Ingress Access List**

This test ensures that only valid IP addresses are allowed to enter the network, and ensures that the numbered ingress access-list ends with a Deny Any Any.

**PCI-DSS-1.3.1 – Restrict Unauthorized Traffic**

This test ensures that a specified access list is configured on the identified interface. The specified access list denies unauthorized traffic from the internet into the DMZ, and allows only traffic that is explicitly permitted.

**PCI-DSS-1.3.3 – Stateful Inspection of Firewall**

This test ensures stateful packet inspection is enabled on a firewall, and turned on for UDP and ICMP traffic.

**PCI-DSS-1.3.7 – Test That Denies Traffic on All Ports Other Than Port 23**

This test ensures that a user-specified access list denies all traffic connections that are open, except for the traffic that is coming in on Port 23.

**PCI-DSS-1.3.7 – Test That Allows Traffic on No Other Open Port Other Than Port 23**

This test ensures that a user-specified access list denies all traffic connections that are open, except for the traffic that is coming in on Port 23.

**PCI-DSS-1.4.1 – Approved Routes Re-Distribution**

This test ensures that only specified routes are redistributed from RIP into a neighboring OSPF or BGP domain. If not, the device is flagged as non-compliant, and the remedy pushes the user-specified distribute list in the appropriate direction. Distribute lists serve as the basic form of network security.

The Access Control List identified by the user ensures:

- Only approved routes from RIP are redistributed into OSPF
- Only approved routes from RIP are distributed in the appropriate direction
- No other routes are being distributed into the OSPF domain

**PCI-DSS-1.4.1 – Check for Approved Static Routes Only**

This test checks for the existence of approved static routes, as specified by the user, and no other static routes.

**PCI-DSS-1.5 – Inside NAT Setup**

This test checks that Network Time Protocol has been setup correctly on the inside interface of the device.

**PCI-DSS-1.5 – Outside NAT Setup**

This test checks that Network Time Protocol has been setup correctly on the outside interface of the device.

#### **PCI-DSS-10.4 – Test for Network Time Protocol**

This test checks if Network Time Protocol authentication is MD5.

#### **PCI-DSS-2.1 – Detecting Default Username**

This test ensures the default username cisco does not exist in the configuration. If it does contain the default username, then it removes it ,and adds a username defined by the user.

#### **PCI-DSS-4.1 – VPN Encryption**

This test ensures that an IpSec VPN is configured to use strong encryption.

##### **PCI-DSS-4.1.1 – WAP Encryption**

This test ensures that WAP is configured to use strong encryption.

Block cipher encryption techniques are designed to disguise plain text patterns that might otherwise generate patterns of encrypted cipher text. Any repeated sequences can facilitate cracking of the algorithm. The WAP gateway can be configured to operate all the encryption algorithms, or a list specifying one or more of the options.

To decide which encryption algorithms to configure, you must consider several factors. A shorter key length is easier to compute, and will impose less overhead on the processor than a longer key length, but a shorter key length can compromise security.

The level of security you need to configure is also determined by the type of information that can be accessed through the gateway. Confidential corporate information often requires a high level of security

Use the WAP WTLS encryption command in conjunction with the WAP WTLS hash global configuration commands to help establish and operate a secure WAP session.

##### **PCI-DSS-4.1.1 – WAP Hash Algorithm**

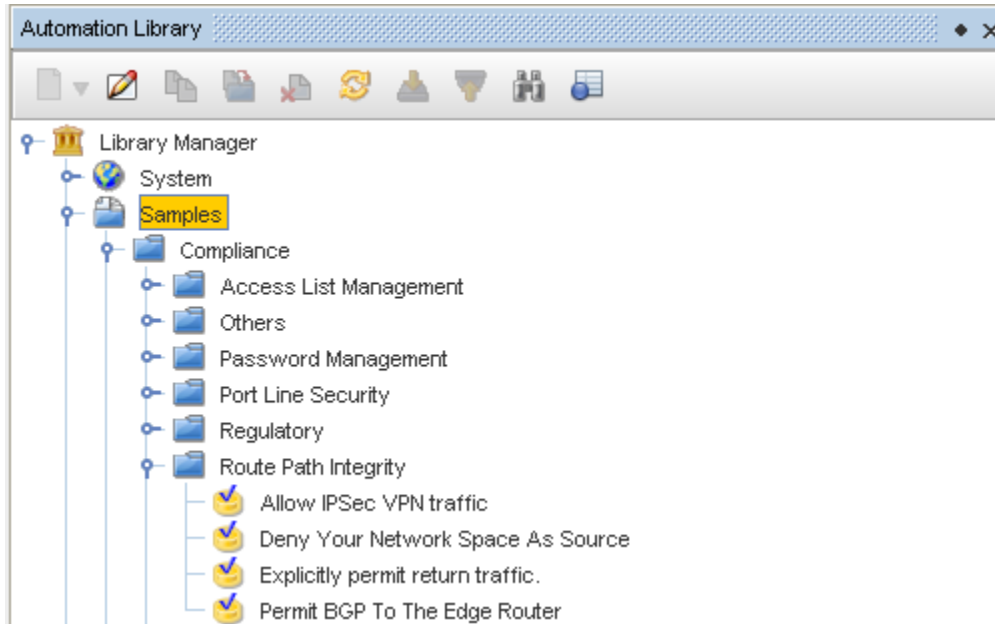
This test ensures that WAP is configured to use strong hash algorithm. Hash algorithms are used to construct a digital signature for encrypted text to prevent attempts to modify the original encrypted text. The WAP gateway can be configured to operate all the hash algorithms or a list specifying one or more of the options.

The level of security you need to configure is determined by the type of information that can be accessed through the gateway. Confidential corporate information often requires a high level of security.

#### **Route Path Integrity**

The following are some of the samples available under Compliance, **Route Path Integrity** in the Library Manager.

Move your cursor over each sample to view a description of the samples within this category.



### Deny Your Network Space as Source

This test ensures that all packets which use the specified Source Subnet as a source address, are dropped if the source address does not reside within a range of legitimately advertised prefixes. If not, the device is flagged as non-compliant.

The Access Control List (ACL) identified by the user ensures that any packet coming in from the specified Source Subnet as the source address is denied access, regardless of where it is comes from.

If an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering is used to prohibit traffic which claims to have originated from outside of these aggregated announcements.

By implementing this type of filtering, it enables the originator to be easily traced to its true source, since the attacker would have to use a valid and legitimately reachable source address.

### Explicitly Permit Return Traffic

This test ensures that specific Internet Control Message Protocol (ICMP) types are explicitly permitted in an ACL specified by the user.

This test allows for return traffic, and flags the device as non-compliant if the device is not explicitly permitted.

The ACL defined by the user ensures the following specific ICMP types:

- Permit Echo-Reply
- Permit Unreachables
- Permit Time-Exceeded
- Deny All Other ICMP Types

## Permit BGP to the Edge Router

This test ensures that unauthorized traffic at the edge of the network is dropped by using ingress filtering, if not, the device is flagged as non-compliant.

This test also ensures that Border Gateway Protocol (BGP) is explicitly permitted on the specified ACL to the edge router by:

- Permitting TCP connections from the ISP Router on ports greater than 1023 for BGP to the Edge Router
- Permitting TCP connections from the ISP Router for BGP on ports greater than 1023 from the Edge Router

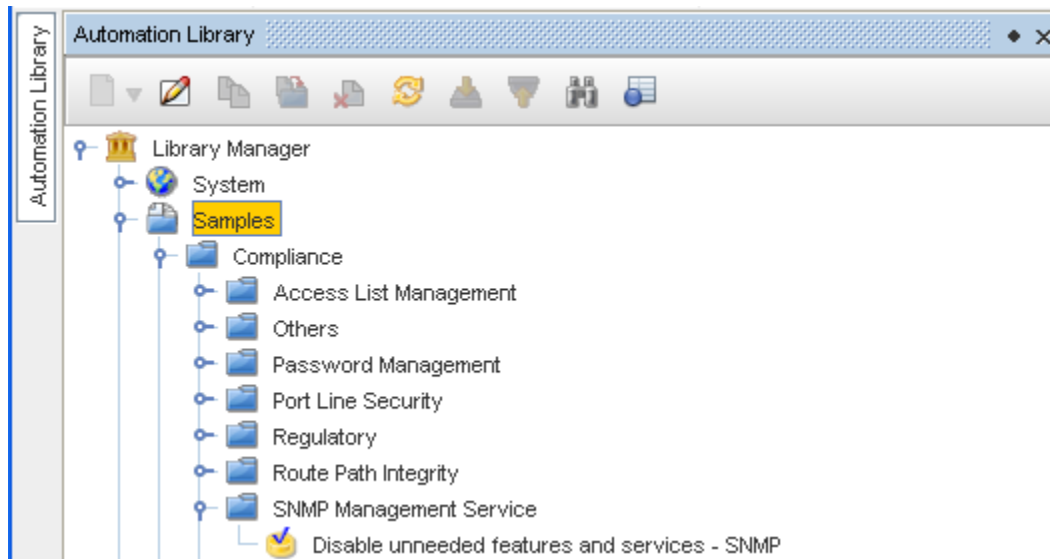
This form of edge (or transit traffic filtering) can be used effectively to limit the flow of transit traffic to and from customers to specific permitted protocols only.

This is done by using Transit Access Control Lists (tACL). As a best practice, it is important that you explicitly permit BGP to the edge router, so when an explicit Deny is configured at the end of the tACL, you do not drop genuine traffic.

## SNMP Management Service

The following is just one of the samples available under Compliance, **SNMP Management Service** in the Library Manager.

Move your cursor over each sample to view a description of the samples within this category.



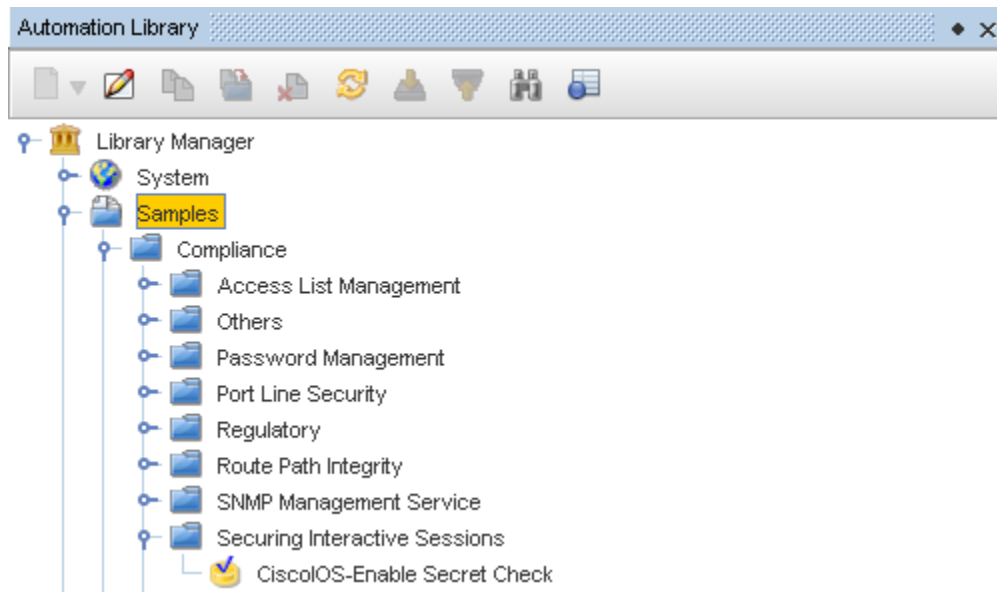
## Disable Unneeded Features and Services - SNMP

This test checks for and removes public and private SNMP community strings.

## Securing Interactive Sessions

The following is just one of the samples available under Compliance, **Securing Interactive Sessions** in the Library Manager.

Move your cursor over each sample to view a description of the samples within this category.



### CiscoIOS-Enable Secret Check

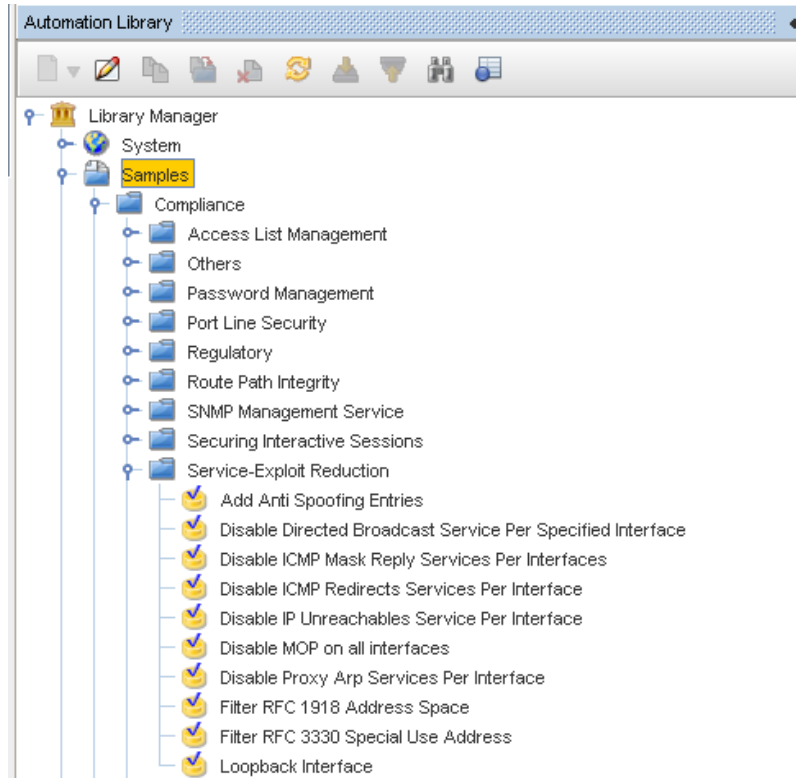
This test ensures that Enable Secret is configured on the device, if not, the device is flagged as non-compliant.

### Service-Exploit Reduction

The following are some of the samples available under Compliance, **Service Exploit Reduction** in the Library Manager.

Move your cursor over each sample to view a description of the samples within this category.





## Add Anti Spoofing Entries

Need information

### Disable Directed Broadcast Service per Specified Interface

This test ensures IP Directed Broadcast is disabled, and if not ,IP Directed Broadcast is disabled.

An IP Directed Broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet, but which originates from a node that is not itself part of that destination subnet.

If directed broadcast is enabled for an interface, incoming IP packets, whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached, are exploded as broadcasts on that subnet.

Since directed broadcasts, and particularly Internet Control Message Protocol (ICMP) directed broadcasts, have been abused by malicious persons, it is advisable that security-conscious users disable the IP Directed Broadcast command on any interface where directed packets are not needed, and use Access Control Lists to limit the number of exploded packets.

### Disable ICMP Mask Reply Services per Interfaces

This test ensures ICMP Mask Reply is disabled, and if not, ICMP Mask Reply is disabled.

ICMP Mask Reply allows the Cisco IOS software to respond to Internet Control Message Protocol (ICMP) mask requests by sending ICMP mask reply messages.

### Disable ICMP Redirects Services per Interface

This test ensures the ICMP Redirects Services are disabled, and if not, the ICMP Redirects Services are disabled.

An ICMP redirect message can be generated by a router when a packet is received, and transmitted on the same interface. In this situation, the router forwards the original packet, and sends an ICMP redirect message back to the sender of the original packet.

This behavior allows the sender to bypass the router, and forward future packets directly to the destination or to a router closer to the destination. Previously, if the Hot Standby Router Protocol (HSRP) was configured on an interface, ICMP redirect messages were disabled (by default) for the interface.

With Cisco IOS Release 12.1(3)T, ICMP redirect messages are enabled by default, if HSRP is configured.

#### **Disable IP Unreachable Service per Interface**

This test ensures the IP Unreachable Services are disabled, and if not, the IP Unreachable Services are disabled.

IP unreachable messages can be used to map out the network topology. It is advisable to disable the IP Unreachable Services on all interfaces.

#### **Disable MOP on all interfaces**

This test ensures an interface does not have a Maintenance Operation Protocol (MOP) enabled, and if it does, it disables it.

#### **Disable Proxy Arp Services per Interface**

This test ensures Proxy Arp Services are disabled, and if not, Proxy Arp Services are disabled.

If Proxy Arp Services are enabled, a machine can claim to be another, to intercept packets; an act called spoofing.

#### **Filter RFC 1918 Address Space**

This test checks if the defined RFC 1918 Restricted Addresses are denied, and if not, the device is flagged as non-compliant.

#### **Filter RFC 3330 Special Use Address**

This test checks if the defined RFC 3330 Special Use Address is denied, and if not, the device is flagged as non-compliant.

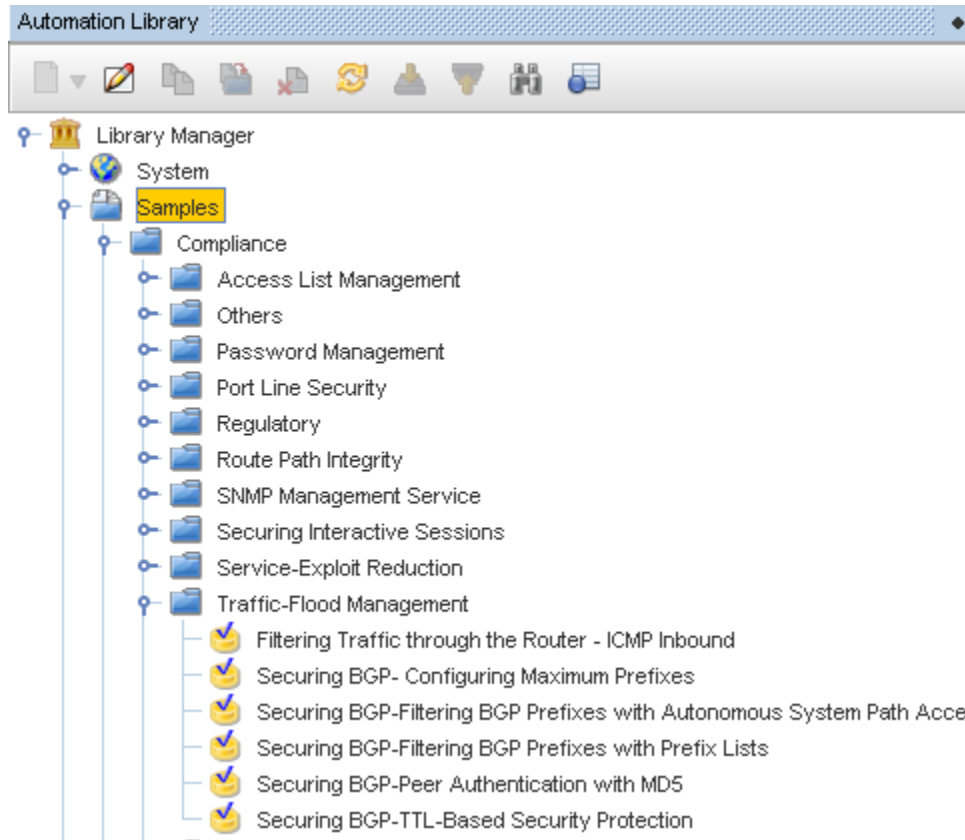
#### **Loopback Interface**

This test ensures there is at least one loopback interface. If no loopback interface is found, it is flagged as non-compliant, and the remedy pushes a loopback interface specified by the user.

#### **Traffic-Flood Management**

The following is just one of the samples available under Compliance, **Traffic-Flood Management** in the Library Manager.

Move your cursor over each sample to view a description of the samples within this category.



### Filtering Traffic through the Router - ICMP Inbound

This test ensures a device has an Access Control List (ACL) that denies ICMP echoes, redirects, and mask replies. If the device does not contain this ACL, it flags the device as non-compliant.

### Network Configuration Manager Setup

The following is one of the samples available under Compliance, **VMware Smart Assurance Network Configuration Manager Setup** in the Library Manager.

Move your cursor over each sample to view a description of the samples within this category.

#### CiscoIOS-SetSyslogHost

This test checks if Cisco IOS Devices are setup to send configuration Syslog messages to the Network Configuration Manager Device Server.

### Working with Network Configuration Manager Samples

An extensive category of Samples for **Compliance Tests** , **Queries**, **Saved Commands** , and **Templates** are shipped in the **Samples** folder.

You can use these samples "as is", or copy and then edit the samples to produce **customized** Compliance Tests, Attributed Queries, Saved Commands, and Templates. You can also select to Export or Move these samples anywhere within your network.

---

**Note** All samples are **read only**, and cannot be modified or linked into Standards or Tests until they are copied to a folder outside the Samples folder hierarchy. This allows the Samples library to be updated independently of the application release, by invoking a button in the JMX-console to reload the samples. This facility does not require a Network Configuration Manager server restart.

---

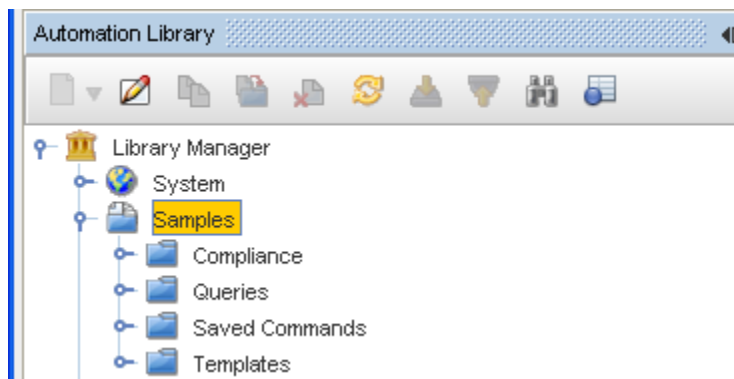
Become familiar with the Samples in this Samples section. By going through the samples, you can see what information is contained within each one, and what columns are contained within each Query.

These samples have been provided to save you time in creating and running your compliance tests, and in determining the information that is displayed as **results** when you run the compliance tests. For the most part, you have sufficient samples to run, or to copy, and make small changes to address your compliance testing needs.

Beginning with an established sample of a query, test, standard, policy, etc., helps to quickly view compliance results, and just as quickly determine what actions need to be taken to bring devices **back** into the compliance state.

First, start by reviewing the contents of the tests (detailed by the actual name of the test), and then run the associated Main Query to view the results.

After you have become familiar with the Tests and Queries, you can copy any sample into another folder, then edit the test and query for customization.

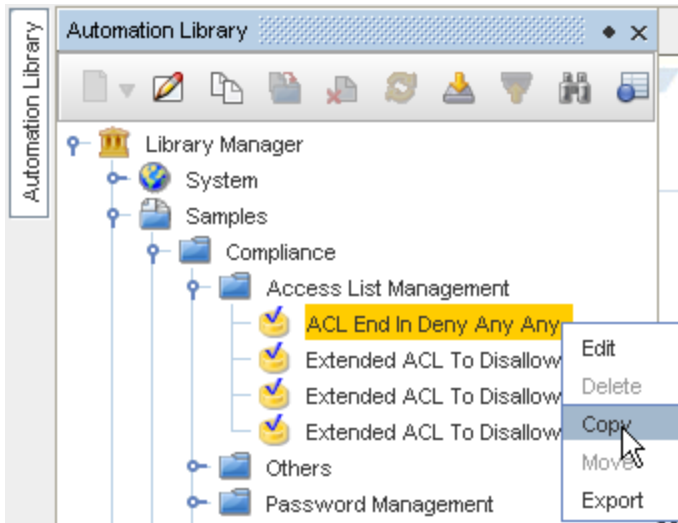


When opened, this link provides several options; Compliance, the associated samples of the (RegEx) tests, Queries, Saved Commands, and Templates.

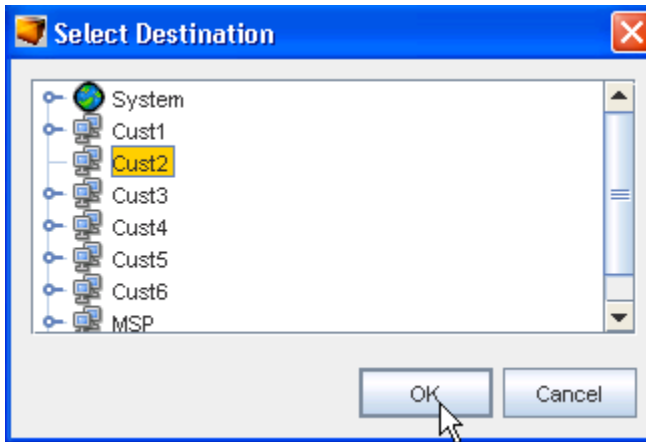
### [Copying Samples](#)

## Copying Samples

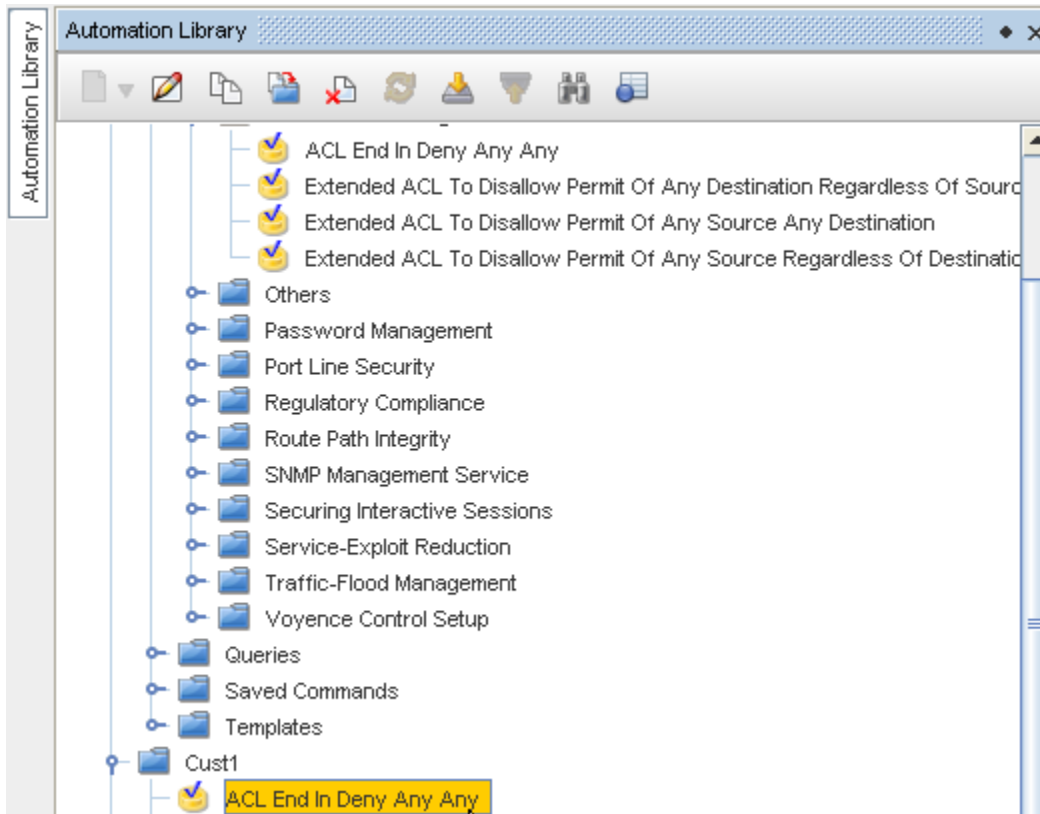
- 1 To copy an Automation Library item into a new or existing folder, first highlight the item, then **right-click**. In the following example, an Access List End in Deny Any Any test is selected from the Compliance Samples.
- 2 Next, select **Copy**.



- 3 At the Select Destination window, select the **location** where the copy of the compliance is to reside, and then click **OK**.



- 4 Now, open the folder, and check to ensure that the destination for the copy was successful.



- 5 You can now double-click to **open the copy of the sample**, and make any needed changes (through the Editor) to customize the Compliance test.
- 6 To run the test now, using all the contents within the Sample test, go to [Running Compliance Tests](#). Your Compliance results are displayed. Viewing the results help you determine if you need to customize the Sample test to better fit your testing requirements.

## Customizing Sample Tests

To modify any item in the **Samples** folder hierarchy, or to link a Compliance Test in the hierarchy to a standard, you must **first copy the sample to another folder** in either the System folder hierarchy, or one of the network folder hierarchies.

---

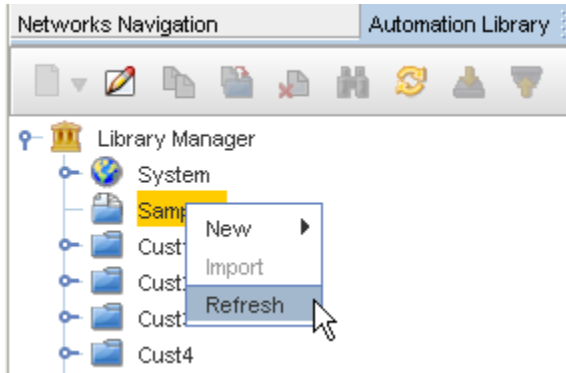
**Important** Requesting that you copy a sample before you can customize the contents isenforced by VMware so the Sample Library can be updated without impacting any changes or dependencies introduced by users. An updated Sample Library can be installed without re-installing or updating Network Configuration Manager, or even restarting the Network Configuration Manager server.

---

Select one of the following Related Topics to continue with customizing samples!

## Right-Click Samples Options

When you right-click on the **Samples** option, you can only use the **Refresh** action at this time. All other options (New and Import) are **not** selectable options.



Selecting **Refresh** ensures that you have the latest view of the Samples.

## Working with a RegEx Compliance Test

### Using Samples to Create a RegEx Compliance Test

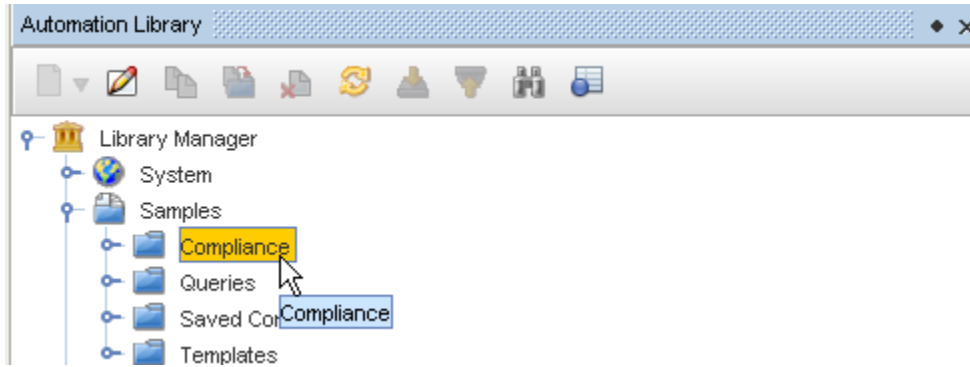
The most convenient way to create a Compliance Test is to use a **Sample Compliance Test** as the template. You can then Copy that test, Edit the test contents, Save the test, then Run the test to view device compliance results.

To begin creating a customized Compliance Test from a sample, follow these steps.

- 1 Access the **Automation Library** by selecting the library from the **Tools** menu bar.



- 2 Next, expand the Samples link, then select **Compliance** from the library Manager.



- 3 Expand the Compliance listing and review the various sample categories. Each category has distinctive sample tests, complete with filters and parameters. Move your cursor over the samples in this category for a quick overview of each sample test.
- 4 Select a **Compliance Test** (from the listing of samples) that is most similar to a test you want to run for device compliance.

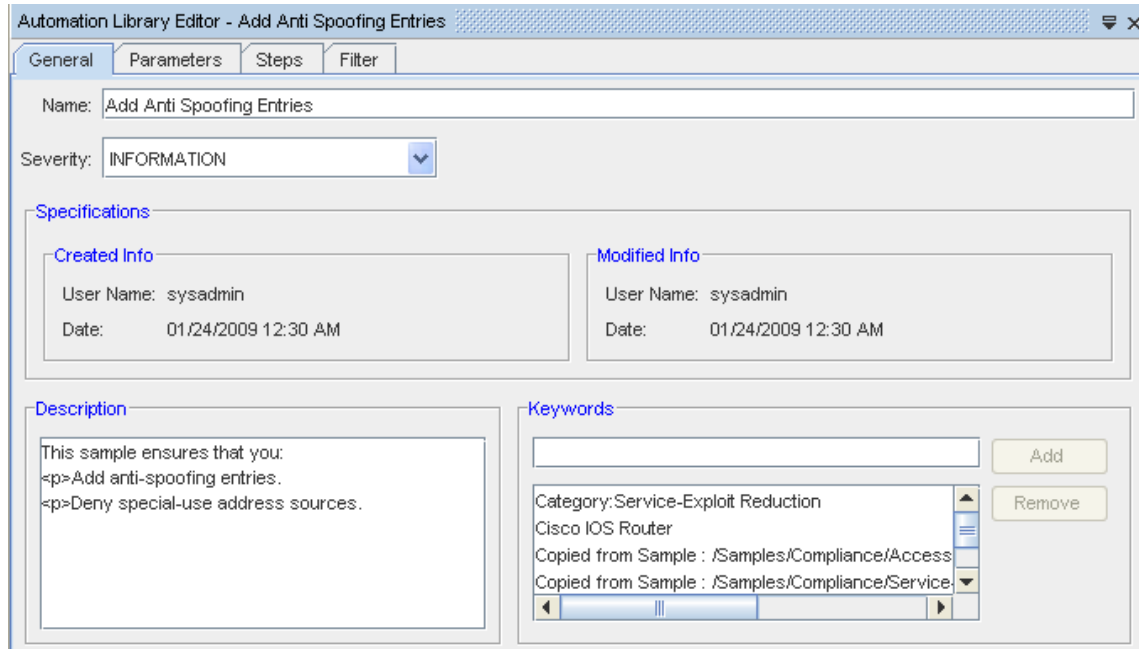
**Note:** See the listing of [Sample Categories - Available Samples](#).

- 5 Click to highlight the sample, then **right-click** on the sample test name.
- 6 Select **Copy** from the options.
- 7 At the **Select Destinations** window, select the destination location for the copy (Network or System).
- 8 Click **Ok** when you have made your save location selection.
- 9 Select that **sample** (from the saved location) then right-click, and select **Edit**, to open the Automation Library Editor, and view the information contained within the sample test.

The **Automation Library Editor** is now open, with all contents of the sample test included in the editor.

- 10 Beginning with the **General** tab, review the information contained within each tab.





General tab,

- 1 To keep a portion of the sample name, but add something to differentiate it from the original sample test name, you can add additional content to the Name, or delete the existing name altogether, and enter a completely new name.
- 2 Review the test **Description** pane.
- 3 You must select the **Severity** of this test by clicking the drop-down arrow, then making a selection from the options.
- 4 You can add or change the **Keywords**. If there are no Keywords, and you want to add keywords, first enter a keyword, then click **Add**. Keywords are helpful to the application when searching for items during a test.
- 5 Click **Save** when you have made your changes to the information in this General tab.

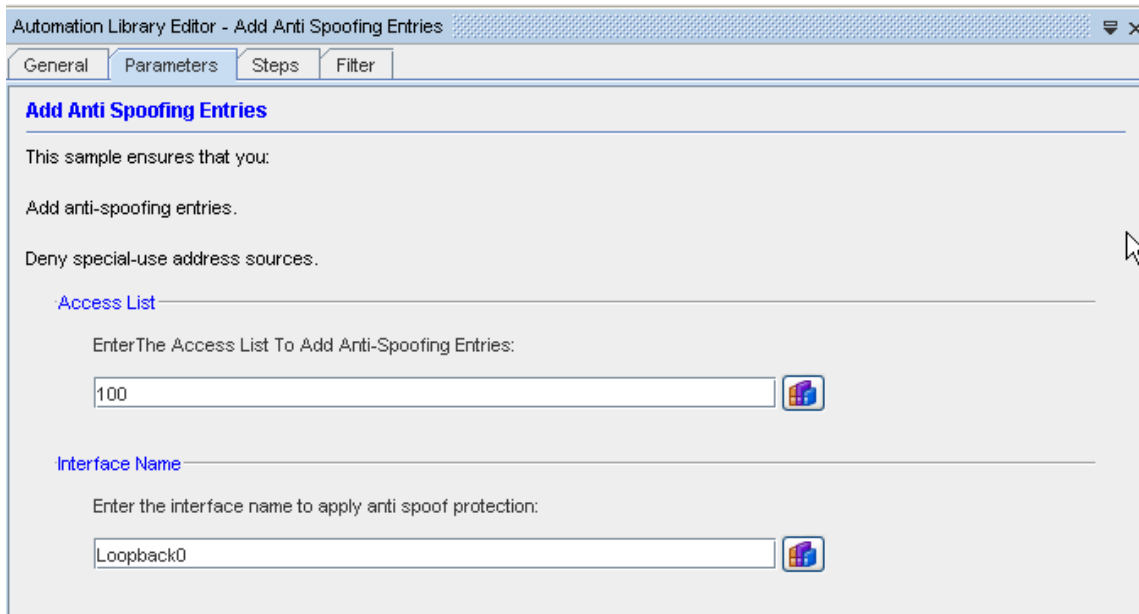
If you have made all the changes you are going to from this Sample test to create your own new test, (for example, you have just made a name change) and have clicked Saved, go to [Running Compliance Tests to run the test](#).

- 6 To view the parameters (if applicable) for this copy of the Sample test, continue with the [Parameters tab - Automation Library Editor for Tests](#) tab on the Automation Library Editor.

---

**Note** If there are Parameters associated with this test, they are displayed in this tab. If not, the Parameters tab does not display. Descriptive Information contained within the Parameters tab is read-only.

---



- 7 Continue on to the [Introducing Chained Steps](#) to make additional changes to the test before running it.

### Creating a New RegEx Compliance Test

Previously, Preconditions and Check Patterns tabs were used in the Automation Library Editor when creating or customizing a RegEx Compliance test. Now, the **Chained Compliance** feature offers General, Scope, and Rule tabs contained within the **Steps** tab.

These new tabs take the place of the previous tabs. Using the **Scope** and **Rule** tabs allow you to quickly set the operators that qualify the configuration, prior to running the test, and assists you in further scanning the configuration to locate specific information from that file.

Tests are then linked to Standards. Tests must be linked to a Standard to run. When the criteria for a Standard is met by a configuration, the Test validates against the content of the configuration.

Chained Compliance is established by completing the following tasks:

- Creating a Test
- Defining a Rule
- Defining a Remedy
- Creating another step (if needed)

The **Chained Compliance** feature has three tabs:

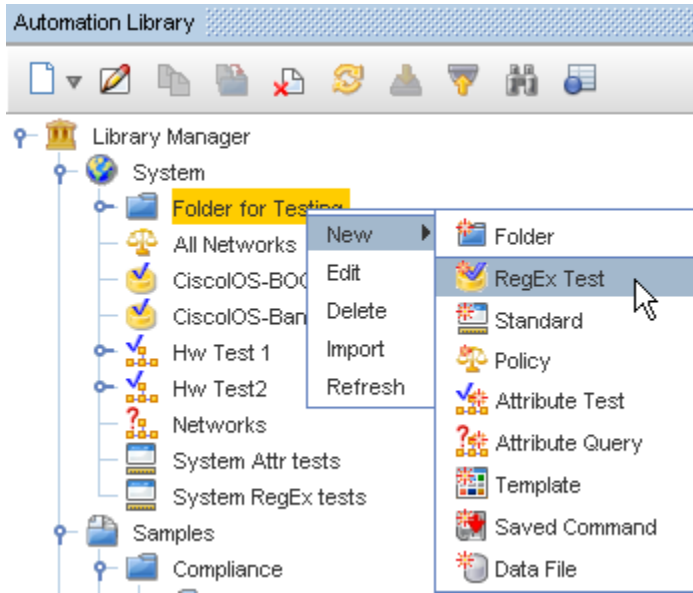
- **General** - containing basic step information, including the step name and description
- **Scope** - Allows you to select the **input source**, and then click down to a specific context within that source. You can narrow the selections using "Begins with" or "Ends with" regular expressions and filters. Each regular expression can extract variables for use later. You can control the behavior when an empty scope is found, by either selecting to "Abort" the test, or to generate a "Remedy".
- **Rule** - Allows you to insert a rule if the scope is empty. The Rule contains the ability to select another context.

**Before you begin creating a test:**

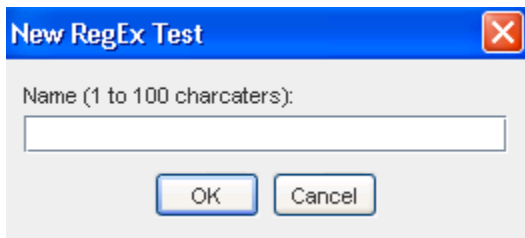
- You may want to review your list of existing tests to see if you want to run one of those Compliance tests, or you may want to edit an existing Compliance test to create a new test.
  - Note that the selections for Preconditions and Check Patterns have been converted to information contained within **Steps** in each test. See [Introducing Chained Steps](#) for more details.
  - You may also want to review the listing of [Sample Categories - Available Samples](#) in the Automation Library. You may decide to use one of these samples for your compliance testing. If so, make sure you [Copying Samples](#) before you attempt to use or customize the contents of the sample test and make it your own.
- 1 To begin creating a new RegEx Compliance test, select the **Automation Library** (from **Tools** in the menu bar).



- 2 When the Library Manager opens, right-click on **System** (or a folder name), then select **New** -> **RegEx Test**.



3 From the New RegEx Test window, enter a **name** for the new test, then click **Ok**.



The **Automation Library Editor** opens, with the tabs needed to create your own test displayed.

Automation Library Editor - New RegEX Test - Customer 1

General Steps Filter

Name: New RegEX Test - Customer 1

Severity: INFORMATION

Specifications

Created Info

User Name:

Date:

Modified Info

User Name:

Date:

Description

Keywords

Add

Remove

Steps: At least one step must be defined

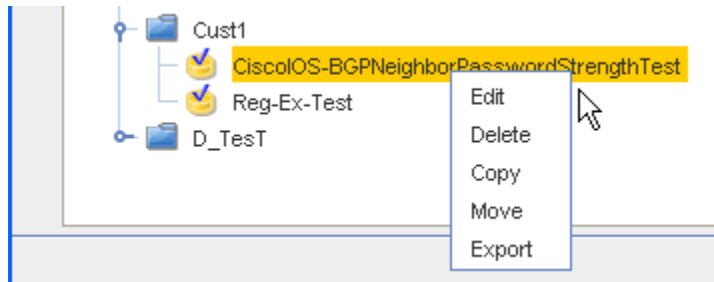
Save

General tab,

- 1 You must select the **Severity** of this test (if not using the default) by clicking the drop-down arrow, then making a selection from the options.
- 2 You can add **Keywords**. First in the keywords field, enter any keyword you want the test to search for, then click **Add**. Notice that the keyword is now added.
- 3 Click **Save** when you have made additions to the tab.
- 4 Continue on to the [Introducing Chained Steps](#) to add information and make selections for this new test. Remember, at least one step must be defined for this test.

### Right-Click Options on a RegEx Test

Once you have established your RegEx test, there are several actions you can take using the right-click options.



#### You can select:

- **Edit** - to open the Automation Library Test Editor, and make any needed changes or edits
- **Delete** - to remove this test from the container
- **Copy** - to copy this test to use at another location, or to use as a template to create another test
- **Move** - this test to another location within your network
- **Export** - this test to a location outside your network

#### Parameters

##### Working with Parameters

Parameters are generalized attributes that can be applied to the RegEx (regular expressions) to be used in either the Scope tab or the Rule tab within the Automation Library Editor. Most tests within the Samples folder contain parameters you can easily substitute for values whenever you want to run the test.

When you have reviewed the various categories in **Samples**, and selected a test to execute against certain devices within your network to determine compliance, you must view and work within the Automation Library Editor.

---

**Note** To view the parameters (if applicable) for this test, continue with the [Parameters tab - Automation Library Editor for Tests](#) tab of the Automation Library Editor. If there are Parameters associated with this test, they are displayed in this tab. If not, the Parameters tab does not display. The descriptive information contained within the Parameters tab is read-only.

---

In order to use or customize a test, you must first [Copying Samples](#) of the test from the Library Manager section, and then place the copy of the test within the Automation Library, or anywhere within your Network.

---

**Note** Parameters are not needed for Standards or Policies.

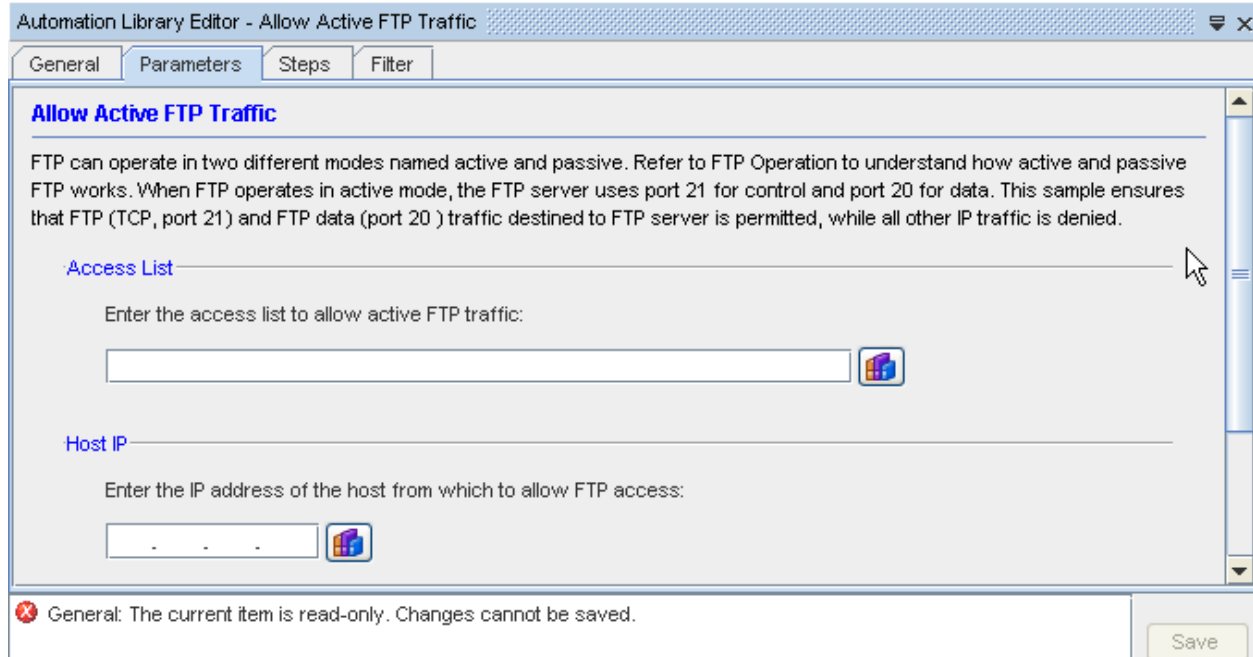
---

#### Parameters tab - Automation Library Editor for Tests

##### At the Parameters tab

Depending on the test you are using to customize for your own testing needs, there are various fields where parameter information is included.

**Note** If there are no parameters associated with this test, the Parameters tab does not display within the Automation Library Editor.



**Note** Along with the name of the test, you will see a description of the actual test. The text contained within the description cannot be edited.

This example of Parameters is Allow Active FTP Traffic sample test.

- 1 For this test, you must fill in the appropriate values for the parameters. Hard code (manually) enter the name of the **Extended ACLextend** into the field.
- 2 At the Access List, enter the appropriate **ACL**.
- 3 Enter the **Host IP Address** in the next field.
- 4 You have now completed selecting the Parameters for your test. Click **Save** to save the information contained in this tab.

**Note** If there are other fields within the Parameters window, each field must be populated with data before your Parameter selection is complete.

**Note:** If you are editing a sample test or are building your own Compliance test, proceed to the next tab, [Introducing Chained Steps](#).

### Chained Compliance Steps

### Introducing Chained Steps

The purpose of a (textually based) Compliance Test is to check that certain statements are contained within a Device's configuration files to verify that the device is **compliant** with the rules and policies defined by the organization that manages the device.

If the device is **non-compliant**, the Compliance Test may optionally generate a remediation, which can be applied to the Device. The goal of the remediation is to change the Device's configuration so that after the remediation is applied, the Device becomes compliant.

---

**Note** Previously, Preconditions and Check Patterns tabs were used in the Automation Library Editor when creating or customizing a RegEx Compliance test. Now, the **Chained Compliance** feature offers General, Scope, and Rule tabs contained within the **Steps** tab.

---

These new tabs take the place of the previous tabs. Using the **Scope** and **Rule** tabs allow you to quickly set the operators that qualify the configuration, prior to running the test, and assist you in further scanning the configuration to locate specific information from that file.

A Steps Compliance test consists of one or more Steps that are executed in order, from the first step to the last. Each Step, individually, has all the abilities of a RegEx test, including:

- The ability to define a scope and disqualify the test if the scope is not met, or as an alternative, generate a remedy if the scope is empty
- The ability to extract stanzas from the steps input for use in the Rule, or in subsequent steps
- The ability to execute a Rule against the configuration

Each step in a test is logically divided into components, each of which is **optional**. However, you must define at least one step, and have content within either the Scope or Rule tab.

These are:

- **Scope Definition:** which defines the textual scope to be used for the rule processing, and optionally passed to subsequent steps. Scope definition can be sub-divided into stanza extraction, stanza filtering, and the handling of an empty scope (as either a disqualified test or the generation of a remedy).
- **Rule Processing:** which includes executing a Regular Expression (RegEx) Pattern against the stanzas generated by the steps Scope Definition (or against other selectable inputs); and Remedy Generation, which is executed if the rule processing for a step determines that the device is not compliant.

Several enhancements have been provided that give Step Compliance much more flexibility and power. They include:

- The ability for a step to use the configuration text as input, or to take input from the stanzas generated in a previous step
- The ability to iterate over the input stanzas, sub-dividing them into sub-stanzas
- The ability to define a named variable that holds the values that matched a regular expression grouping for each sub-stanza



For additional information on the Compliance Steps, see [The Chained Compliance Steps Design Overview](#).

Continue on with the [The General tab in Steps](#).

### Chained Compliance Best Practices

The following are items to consider when using the Chained Compliance Steps to create RegEx Compliance tests.

- If a "Beginning With" has been defined, you must also define an "Ending With".
- You must have a Scope definition or a Rule definition, or both.
- If a test contains Steps, there must be at least one Step with a Rule defined within the Step.
- A Rule cannot have the same "Input source" as the Step.
- You cannot forward reference a Step. For example, if you have Step 1 and Step 2, and Step 3 (in that order) Step 1 cannot access variables from Step 2 or Step 3.
- You should not move a Step out of order (doing so may break the dependencies).
- Steps referred to must exist.

### The General tab in Steps

When working within the Policy Editor, once a Test has been selected, the tabs for working with a test display in the right panel of the Policy Editor.

The **General tab** contains the Name and the Description.

You can now continue on with the Steps (Chain Compliance procedure), and go to the [The Scope tab in Steps](#) first, or to the [The Rule tab in Steps](#). Scope defines the context, and Rule is used to test the contents of the Scope.

For additional information on the Compliance Steps, see [The Chained Compliance Steps Design Overview](#).

### The Scope tab in Steps

---

**Note** Entering content into this tab is optional. However, if you do not enter content with the Scope tab, you must enter content into the Rule tab.

---

You can define a **Scope** for this Compliance test. This new scope feature replaces the former Preconditions tab in the Automation Library editor. Scope allows you to set the input for the step.

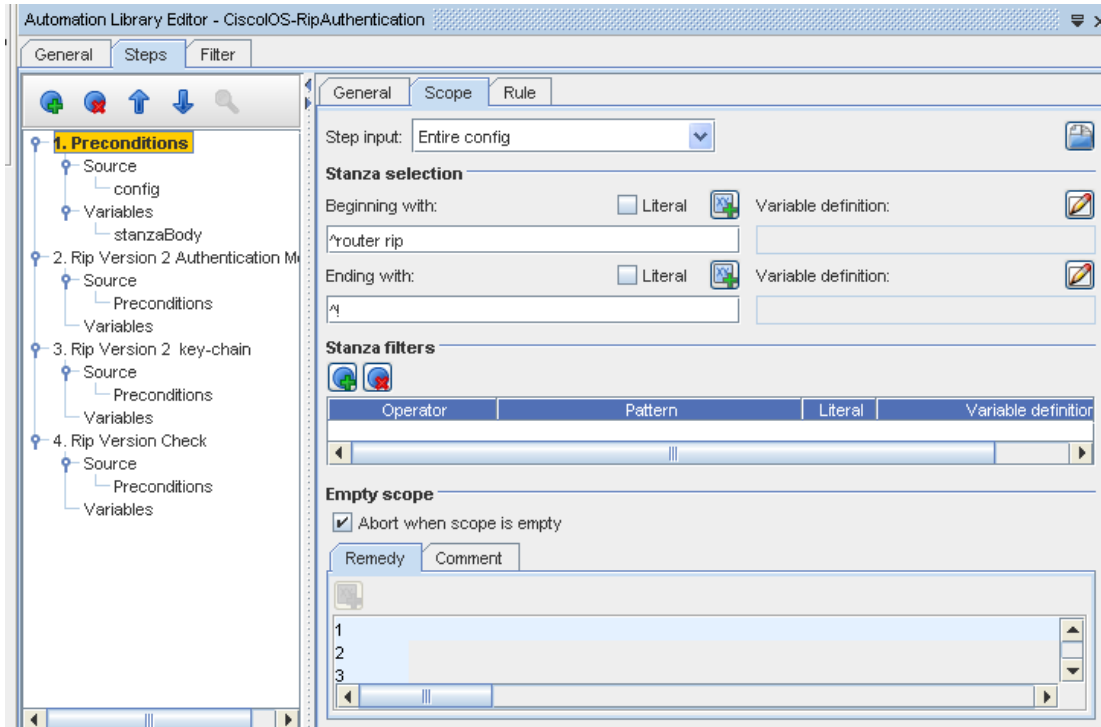
- 1 The first action you take within this tab is to click the **Add Step**  icon. This then puts **Step 1** into the navigation tree, and also lists **Step 1** as the Name of this step in the General tab.

With this tab you can specify **configuration commands** that must be present before the test is run. You will also enter the **actual expression** that is searched for in the configuration, and the remedy for an empty scope.

- This **Scope** tab allows you to select the **Step input source** .

- You can define variables from these items, or set a pre-defined scope (for example, Cisco IOS Interfaces).
- The **Step input** is the main or first source your test searches for in the configuration files.

**Note** For the first step, the default Input source is Entire Config. This cannot be changed, and is already selected.



**Note** Each time you add another step, the step is numbered. For example, you may have 1. Preconditions, 2. Rip Version 2 Authentication Module, etc.

Notice that when you make a change in the Name field in the General tab, the change is then reflected in the Navigation tree where the steps are listed.

- 2 You can continue to create steps and further define your search within the device configuration by going to the **Scope** tab or **Rule** tab.
- 3 Next, you can select to narrow your context by using "Beginning with" and "Ending with" **regular expressions and filters** in the Stanza selection section. Each regular expression can extract variables for later use. You can select to have a **Literal** string (which you enter manually), or you can select a **Variable definition** using the icon to view the available options. The **Literal** check box indicates the text is **not** treated as a RegEx.

Now, when the test is run, the "**Beginning With**" content is the first content that the test searches for within the configuration.

The **Ending with**: ^! represents where the search ends within the content of the configuration.

- 4 Once you have determined your RegEx expression, and created a group, you must then give that group a variable definition. Click the **Edit Variable Definition** icon to define a group.
- 5 At the **Stanza filters** section, you can add a row for filters. Select one of the following from the **Operator** drop-down: Contains Any, Not Contains, or Contains All.
- 6 At the Empty scopesection, you can select to **Abort** the test if the **scope** is not found (when Scope is empty) . You can also decide to add a Remedy Configlet by entering the remedy contents into the Remedy section. This instructs the test to use this specific Remedy if the scope context defined is not found during the test.
- 7 If needed, you can **add comments** that define your remedy in the **Comments** section.
- 8 If warranted, continue by going to the [The Rule tab in Steps](#).
- 9 For additional information on the Compliance Steps, see [The Chained Compliance Steps Design Overview](#).

### The Rule tab in Steps

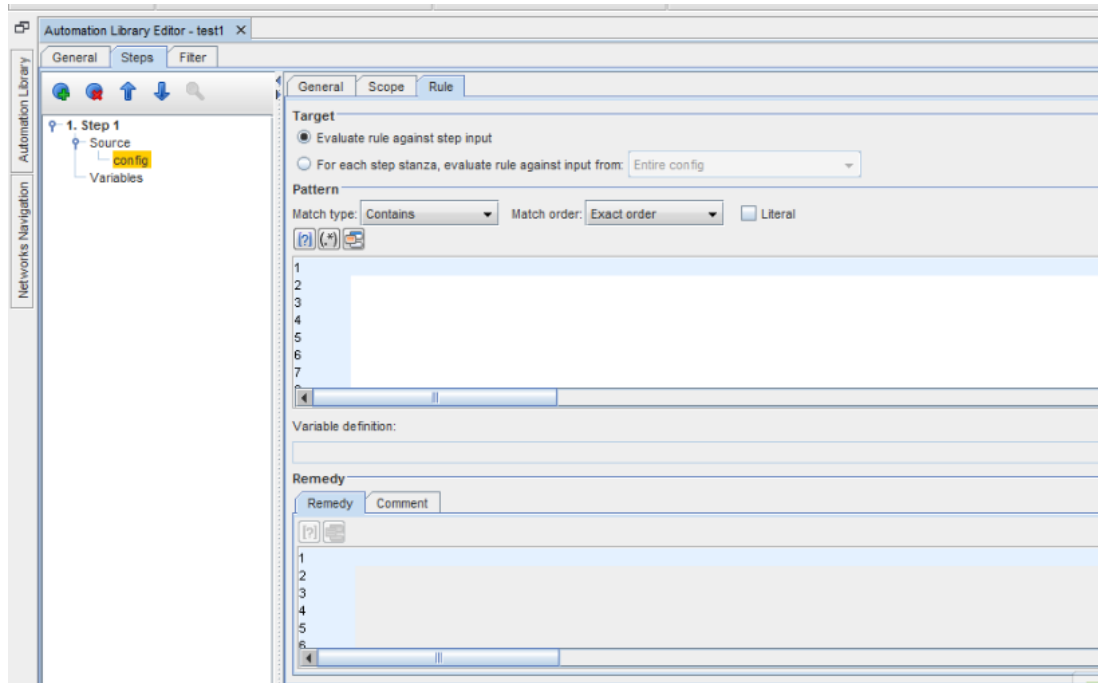
---

**Note** Entering content into this tab is optional, however, if you do not enter content with the Rule tab, you must enter content in the Scope tab.

---

You can use predefined configlets as templates in the RegEx Rule and Remedy section. The content of a template that has to be included in the RegEx tests should be static without any variables or reference to other templates, else an error message appears. The content of a template that has to be included in the remedy section should be static text.

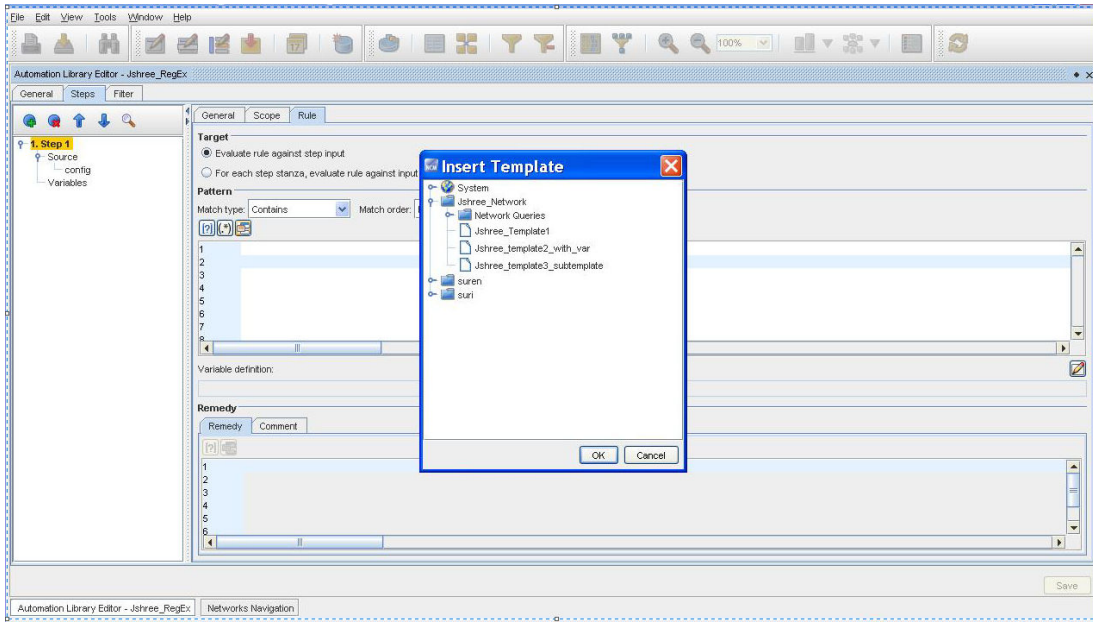
Information contained within this tab is used to **test** the section defined in the **Scope**.



- 1 At this first Targetsection, select to **Evaluate the rule against step input** from the scope content (by clicking the radio button) , or select **For each step stanza, evaluate rule against input from** (by clicking the radio button and then making a selection from the options in the drop-down arrow).
- 2 At the Pattern section, make your choices by clicking the drop-down arrow and seeing the options offered in the **Match Order** and **Match Type** sections. You can also select to insert variables using the icon. If you manually enter information, you can then check **Literal**.
- 3 At the Variable Definition section, you can edit the existing field, if applicable, or assign **variable names** to any groups captured in the regular expression.
- 4 At the Remedysection, enter a **Remedy**, and then use the icon to insert a variable for a portion of the Remedy.
- 5 Once completed with the Rule tab, click **Save**.
- 6 Return to the Automation Library editor by selecting the [Filter tab - Automation Library Editor for Tests](#) tab in the right panel of the Automation Library.

Using the **Select Template** icon: A Select Template icon is added in both Rule and Remedy section of the RegEx.

- 1 Click the **Select Template** icon. The Insert Template window appears with all the predefined templates.
- 2 Select the required template and click **OK**.
- 3 Only one template in a line is supported. You can include multiple templates in line by line matching criteria.



For additional information on the Compliance Steps, see [The Chained Compliance Steps Design Overview](#).

### Create Another Step

Once you have created the first step, you can create additional steps by clicking the **Add Step** icon while in the Scope tab or the Rule tab. Each step can:

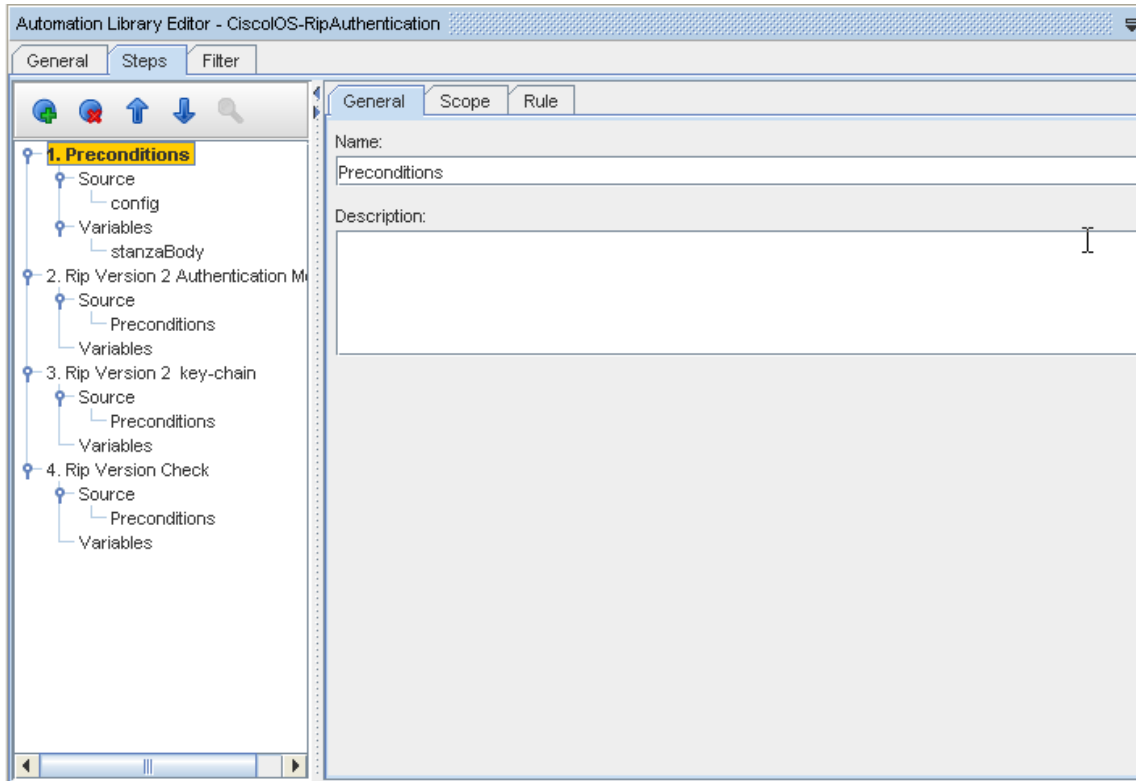
- Test within the stanzas from the previous step , or from any one of the previous steps
- Test within the entire configuration

You can repeat creating steps as many times as you need.

---

**Note** Each time you add another step, the step is numbered. For example, you may have 1. Preconditions 2. Rip Version 2 Authentication Module, and 3. Rip Version 2 key-chain, etc.

---

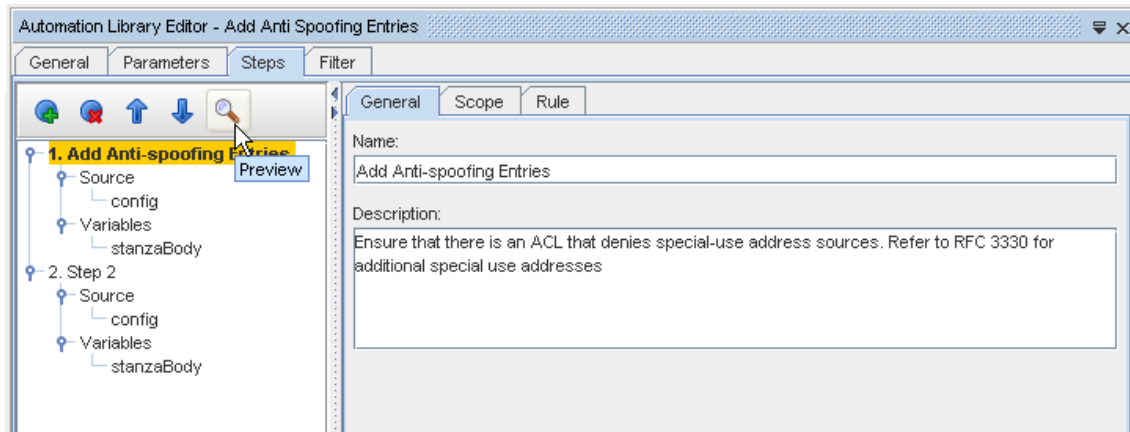


For additional information on the Compliance Steps, see [The Chained Compliance Steps Design Overview](#).

### Previewing a Test

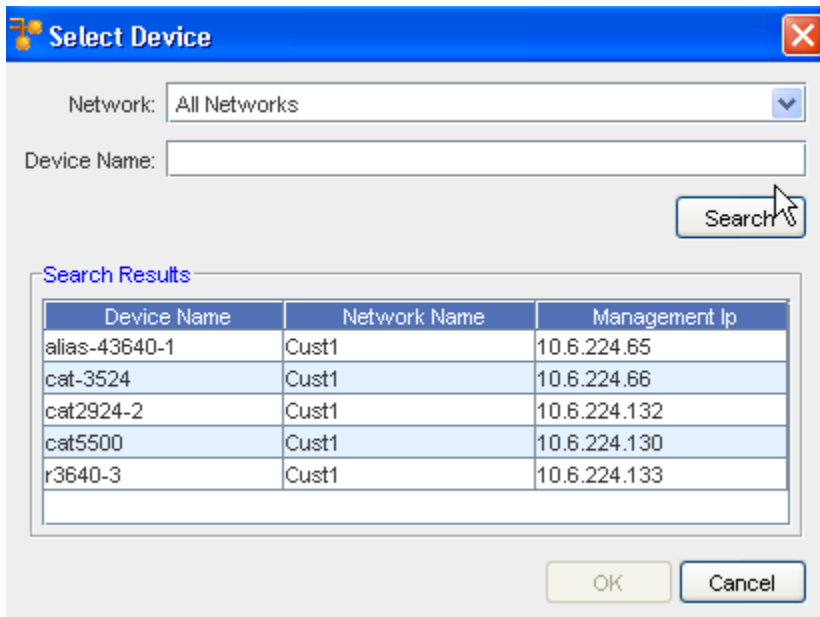
When creating Steps within Network Configuration Manager Chained Compliance, you can also **Preview a test**, displaying test information. This can be done even if you have not completed all the Steps for the test, or if you have not yet Saved the test. This feature allows you to get instance test results, based on several selections, while creating your test.

See the following example of **Previewing a test** .



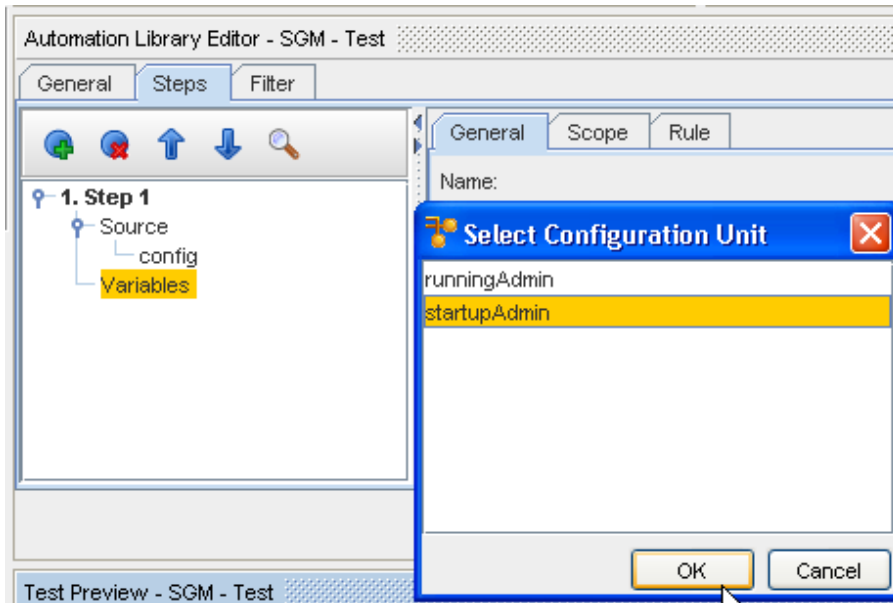
**Note** You can preview a test at anytime, as long as the test is a valid test , without errors.

- 1 To begin the Preview process, select a **valid test** from the Steps navigation tree in the Library Editor, then click the **Preview** icon on the tool bar.
- 2 Next, at the Select Device window, you can select from the **Network** drop-down options to select one specific **Network**, or **All Networks**.
- 3 At the Device Name field, you can either enter in the **name of one Device** (or the partial name of a device),then click **Search**. To view a listing of all available devices, click Search.
- 4 Select **one device** from the listing.

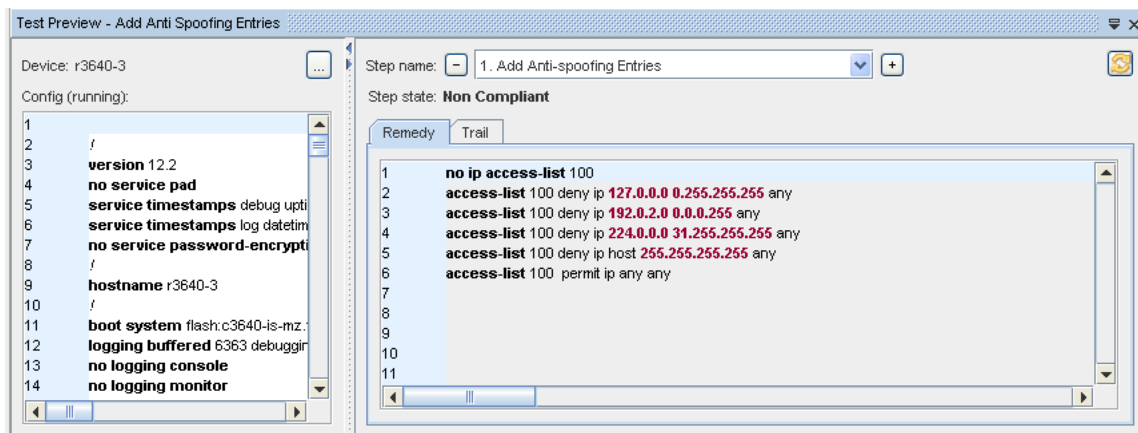


- After selecting the device, click **Ok**.

**Note** When you select a device for preview, the application determines what the primary RegEx auditable units are. If more than one exists, you are then prompted to select one. If only a single primary RegEx auditable unit exists, that one is loaded automatically. If the device you selected has no primary configs available, an error message displays, and you will must select another device from the Select Device window.



- When you have selected a device, the Select Configuration Unit window opens, where you must make a selection before you can view the Preview of the test. Select a configuration unit from the list, then click **Ok**. The Test Preview results display.

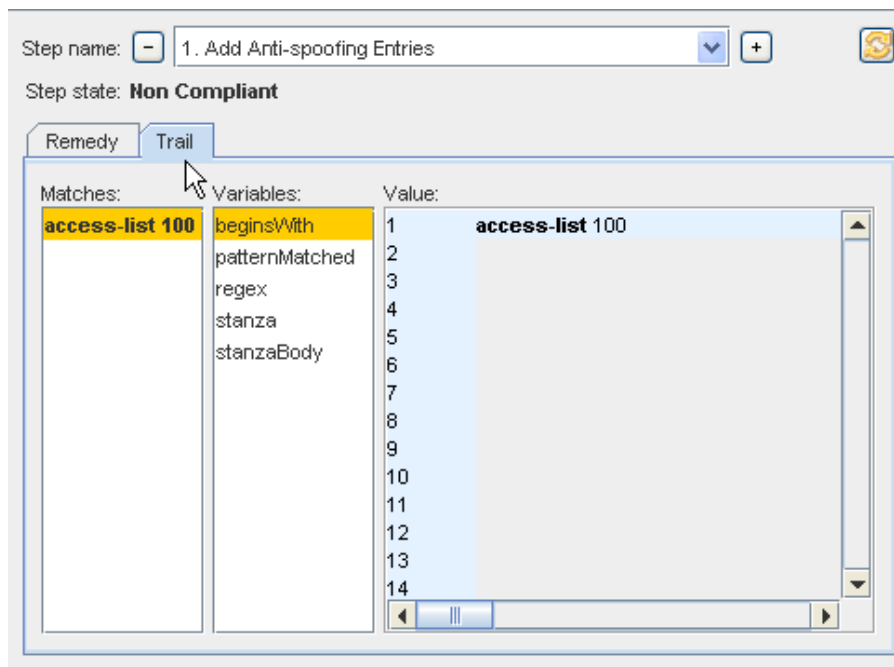


- In the left pane, the **default configuration** for the selected device is displayed for the device that you selected. This is the default configuration on the device. Note that the configuration may not always be running.



- The right pane contains the Step results of the step displayed in the Step name section. To see the results for another step, you can click the Step name drop-down arrow and select a Step, or you can use the plus sign (+) to change to the next step name, or the minus sign (-) to go back to the previous step name. Test results are immediately shown, based on the content of the Step information.
- Note that the **Step state** is displayed under the Step name. In this instance, the Device is shown to be **Non-Compliant** for this test. There are several types associated with the Step state.
  - **Compliant** - the device is in compliance with the current step
  - **Non-Compliant** - the device is not in compliance with the current step
  - **Not Audited** - there is no content in the Rule tab
  - **Did Not Qualify** - attempted to run the Step, but the Scope was empty, for example, nothing in the input for the step matched the scope or the filters

7 Click the **Remedy** or the **Trail** tab to view additional information.



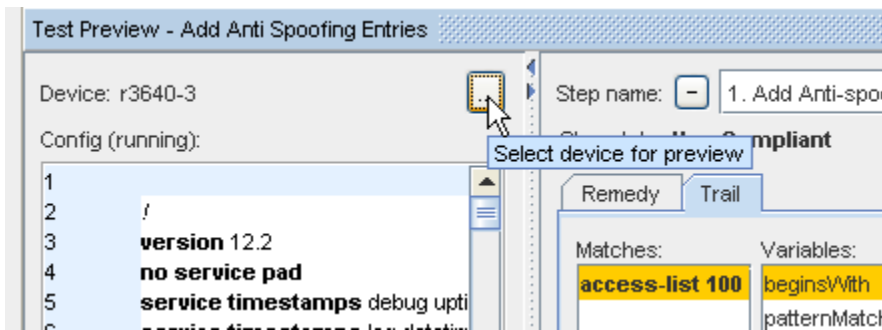
If you have a **Remedy** included in that step (from the Rule tab content), this information is displayed in the Remedy tab. The Remedy that shows in that tab is only the Remedy for that specific Step.

The Trail tab contains the **Matches** information shows the **first match**, and the **Variables** are shown in the second pane. The **Value** section is the actual content of the variable. You can click within the list of **Variables** to see the **Value** displayed for that Match.

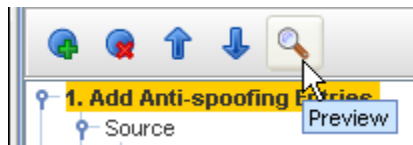
**Notes:**

- You can use the plus sign ( +) and the minus sign (-) to go between Steps to preview the test results for each step
  - You can alter the information within the Configuration content, and then click the **Refresh** icon to refresh the view, and see new test results
  - You can also edit the existing information contained within the test (in the General, Scope and Rule tabs) in the Test Editor, and then click the **Preview** button again to view completely new test results based on your test changes.
  - You can go back and forth between the Test Editor and the Test Preview as many times as needed to view test results based on any number of changes; selecting a new device using the Select device for preview button; making changes to the General, Scope and Rule tabs content; changing the content of the configuration displayed in the Preview.
  - You can work in the Test Editor, while still viewing the results of another test in the Preview
- Previewing and running more tests,

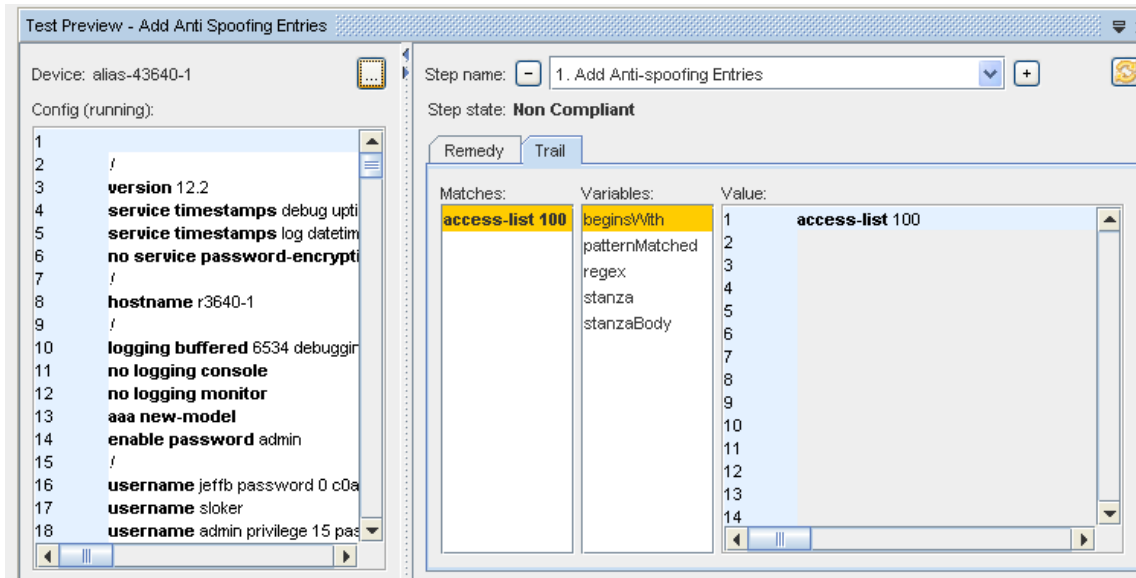
- 1 First, to change the device you are testing against, click the **Select device for preview** icon (in the right pane) to view the Select Device window.



- 2 With the Device Select window open, select **another device** to run this test against, and click **Ok**.
- 3 Click the **Preview** test icon again, to preview the test results for that device.



The preview results are once again displayed, based on the device selected, and the options and selections previously entered in the Compliance steps.



Again, remember that you can make changes to the configuration content, click Refresh, and run the test again. When changes are made to the config, you will see the results of the test in the Remedy and Trail tabs. The results displayed in the **Matches:** section shows as regular text when Compliant, and shows in **bold** when Non-Compliant.

#### Editing Tests,

- 1 You can edit the test you are previewing by going back into the Step Editor and making changes to the content in any or all of the Steps.
- 2 Once changes are made, click the Preview button, and make Network and Device selections to view new test results, based on your changes. This is not needed if the configuration is already loaded.
- 3 You can also go back to the Step editor, and select a different test from the navigation tree (for example Step 2) and then click the Preview button to see the test results and additional test information based on the Step you selected.

**Note** The Test Preview only displays and refreshes the results of the last test previewed when the Preview button was used. The name of the test currently being previewed is displayed on the Test Preview window's title bar.

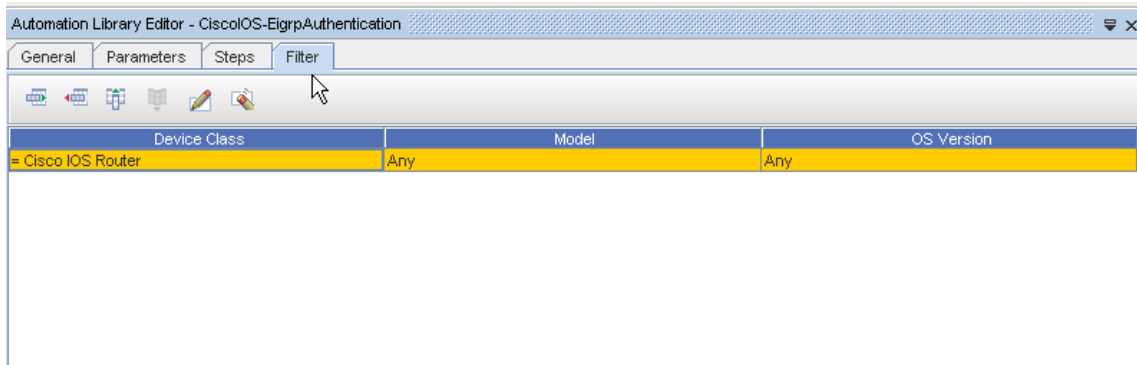


## Filter

### Working with Filters

When creating a new Compliance Test or using a sample Compliance Test, you can add Filters or edit existing filters, depending on the test you want to run within your network.

Filters further restrict the devices that pass through the standards.

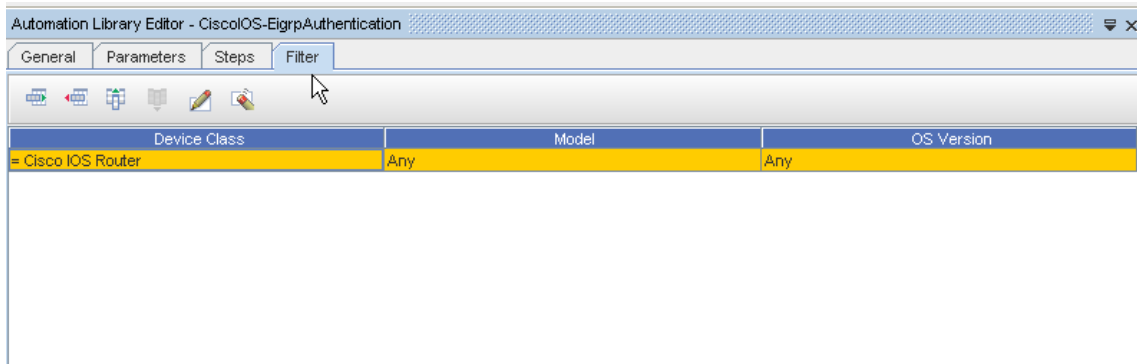


See:

[Filter tab - Automation Library Editor for Tests](#)

**Filter tab - Automation Library Editor for Tests**

When working with either a sample Compliance Test or creating a new Compliance Test, you may want to add filters or edit existing filters.

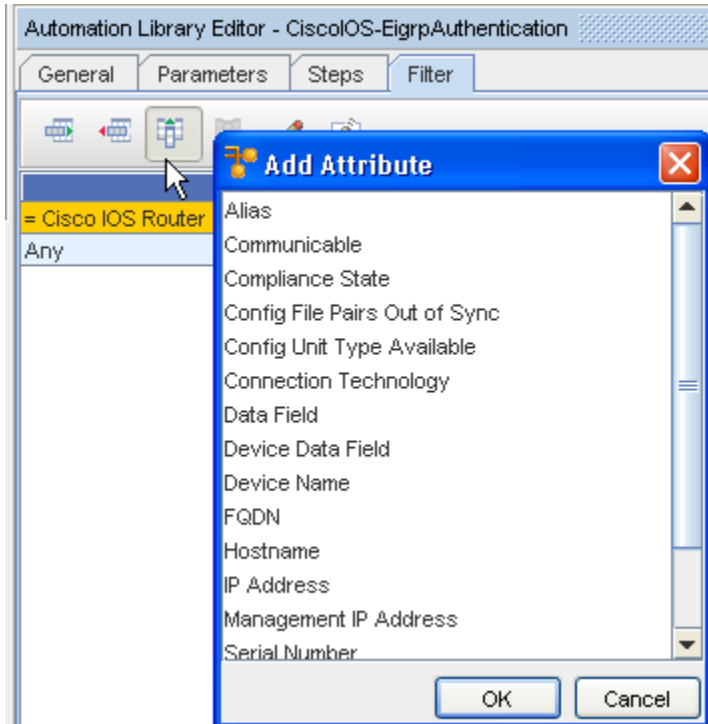


- 1 Click the **Filter tab** to view and work with the filters for a RegEx Compliance Test.
- 2 Filters are groups based on Device Class, on Model, and more.
- 3 Filters further restrict the devices that pass through the standards.

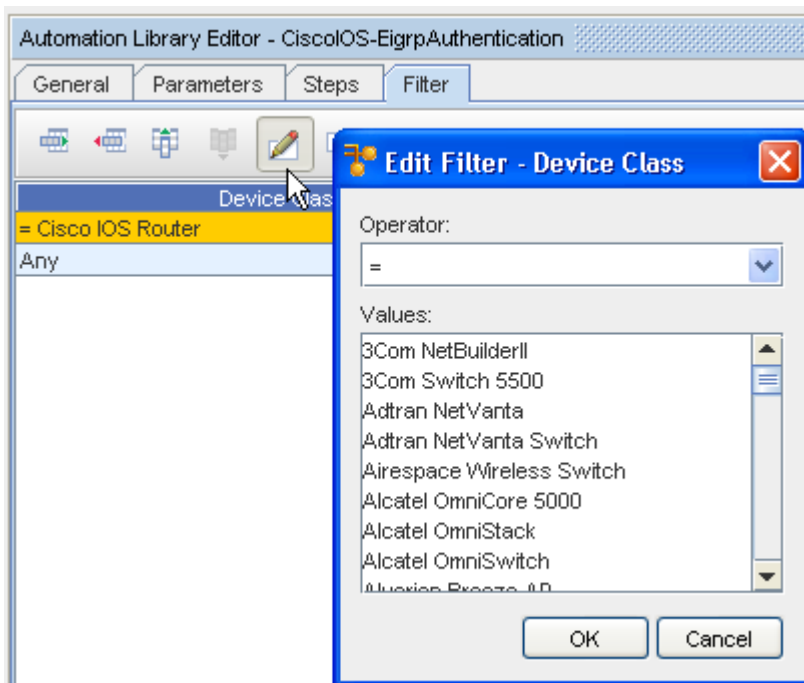


Use the following icons to:

- 4 Note that Device Class, Model, and OS Version are default options for filters. To add additional filters, or change filters, click the **Add a Filter Attribute** icon. When you have made an Attribute selection, click **Ok**.



- 5 You can select the **Edit Filter** icon to edit existing filters within the test. First, highlight the Attribute name (Filter name, in this case, Device Class) then click the **Edit Filter** icon.



- 6 After selecting from the **Operator** drop-down options, and then selecting from the **Values** section, click **Ok**.
- 7 Once you have added or edited the filters for the test, click **Save**.

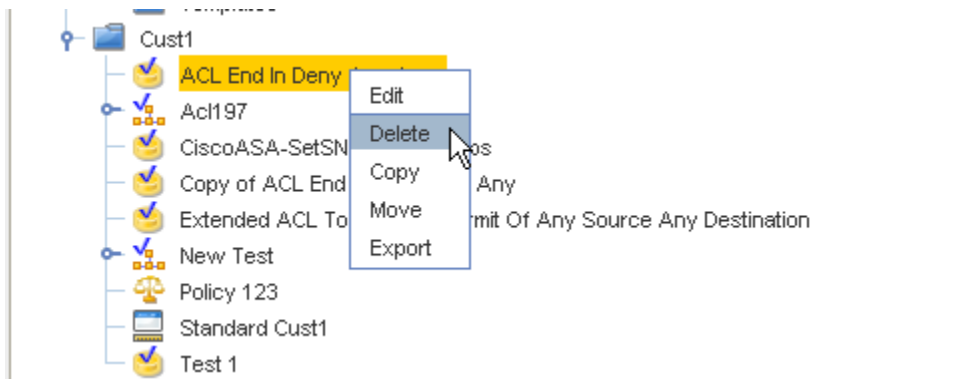
Icon	Action
	Add additional filter conditions
	Remove existing filter conditions
	Add a filter attribute
	Remove an existing filter attribute
	Edit the Filter
	Clear all data

The new test with your changes is now saved. You can run this test by **double-clicking on the test**.

### Deleting Tests

When a test is no longer needed, it can be deleted using the right-click options.

- 1 First, **select the test** you want to delete from the list of tests.
- 2 Next, right-click on the test, then from the options, select **Delete**.
- 3 At the confirmation message, click **Ok**. The test is now deleted from the list of tests.

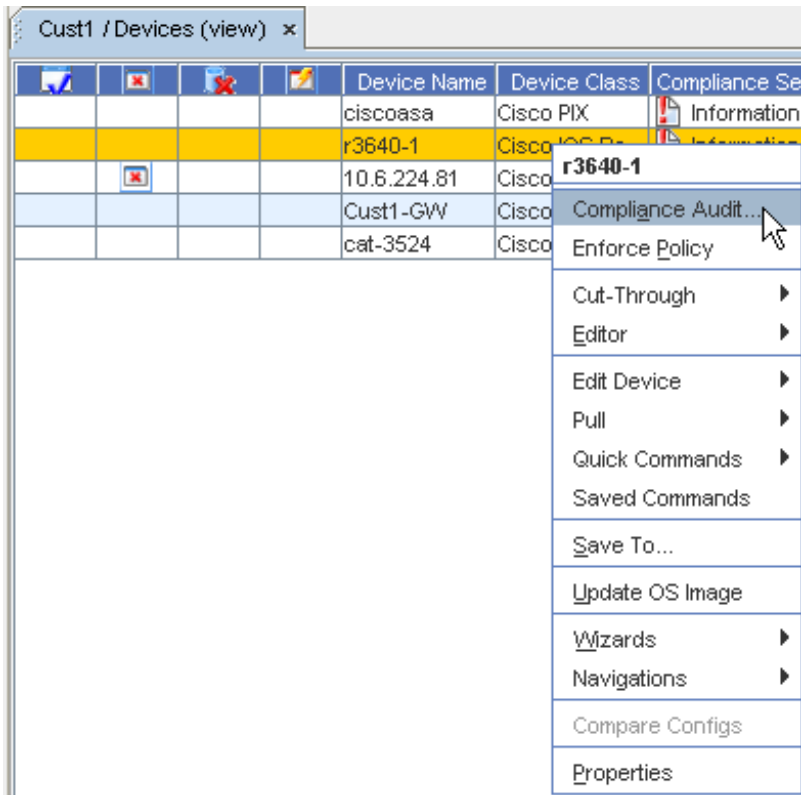


**Important** Be aware that when Deleting Tests, **any Standard** that is linked will be **affected**.



### Running Compliance Tests

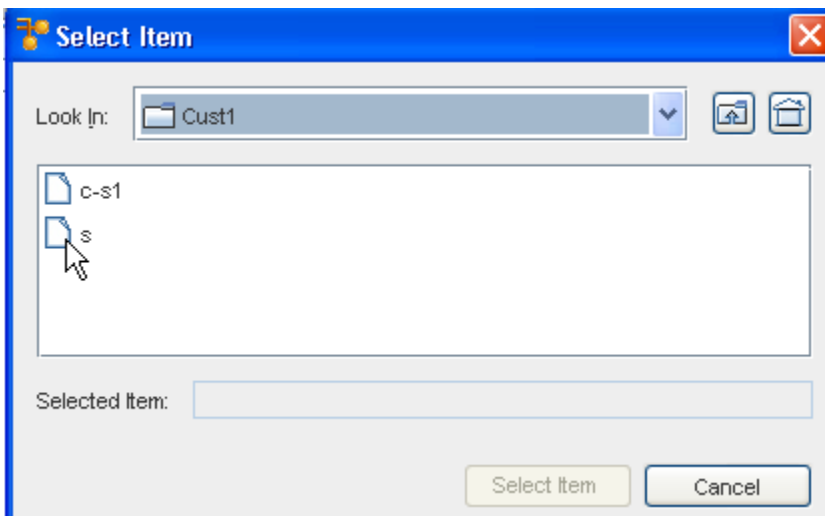
To Run a compliance test,

- 1 From the **Devices View**, select the device or devices you want to run the compliance test against.
- 2 **Right-click on the device, then select Compliance Audit.**

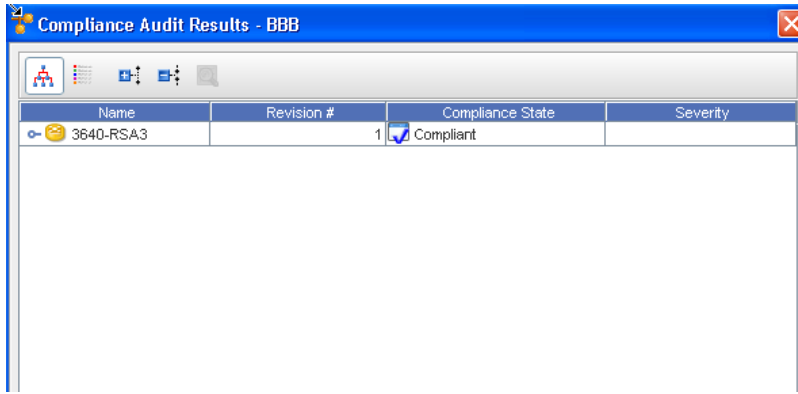


- From the Select Item window, click the drop-down arrow if needed.

**Note** You can use the two icons   (Up one Level and Home) to expand or contract the listing contents).



- Make your selection from the list, then click the **Select Item** button.
- At the Compliance Audit Results window, your results are displayed.



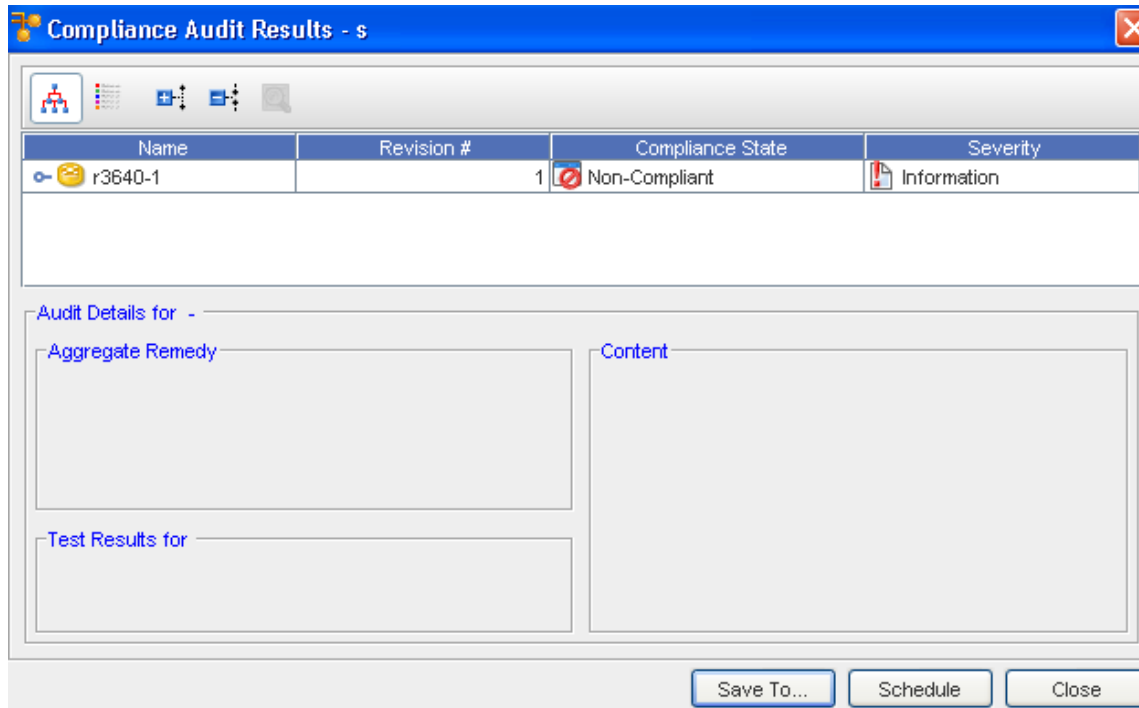
Notice that the compliance test results show that this specific device is Compliant. If your Compliance Test is Non-Compliant, from this window, you can select to **Save** the results, or you can [Scheduling a Run Time](#).

6 Click **Close** when you have reviewed the audit results.





### Compliance Audit Results



When viewing the Compliance Audit Results, you can use the **Results** icon in the tool bar to display the information.





Icon	Description
	Displays the devices in the Name column in a tree format
	Displays the devices in the Name column in a list format
	Expands the tree or list
	Collapses the tree or list

Notice that the compliance test results show that this specific device is Compliant. If your Compliance Test is Non-Compliant, from this window, you can select to **Save** the results, or you can [Scheduling a Run Time](#).

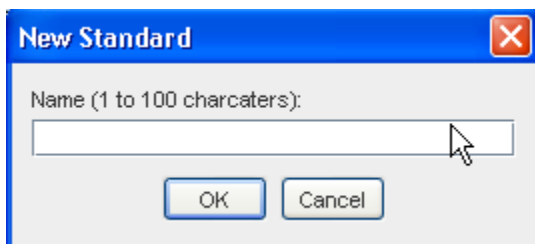
## Working with a Standard

### Creating a New Standard

A Standard allows you to set up **filters and tests** that are run against specific device classes. Filters for standards are optional, but you can have as many tests as needed.

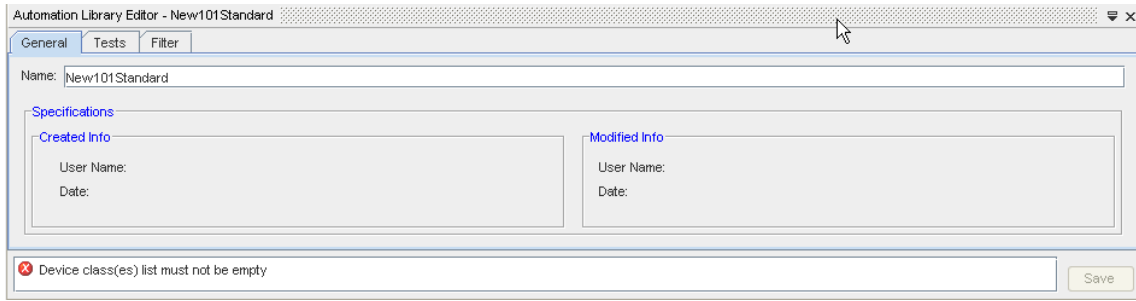
**Note** With Multi-Config, Compliance Policies now incorporate Standards and Tests targeted on specific configuration files.

- 1 To create a new Standard, you must first select the **Automation Library** .
- 2 When the Library Manager opens, right-click on **System** (or a folder name), then select **New** -> **Standard** .
- 3 From the New Standard window, enter a **name** for the new Standard, then click **Ok**.



The Automation Library editor for the newly named Standard displays.

At the General tab,

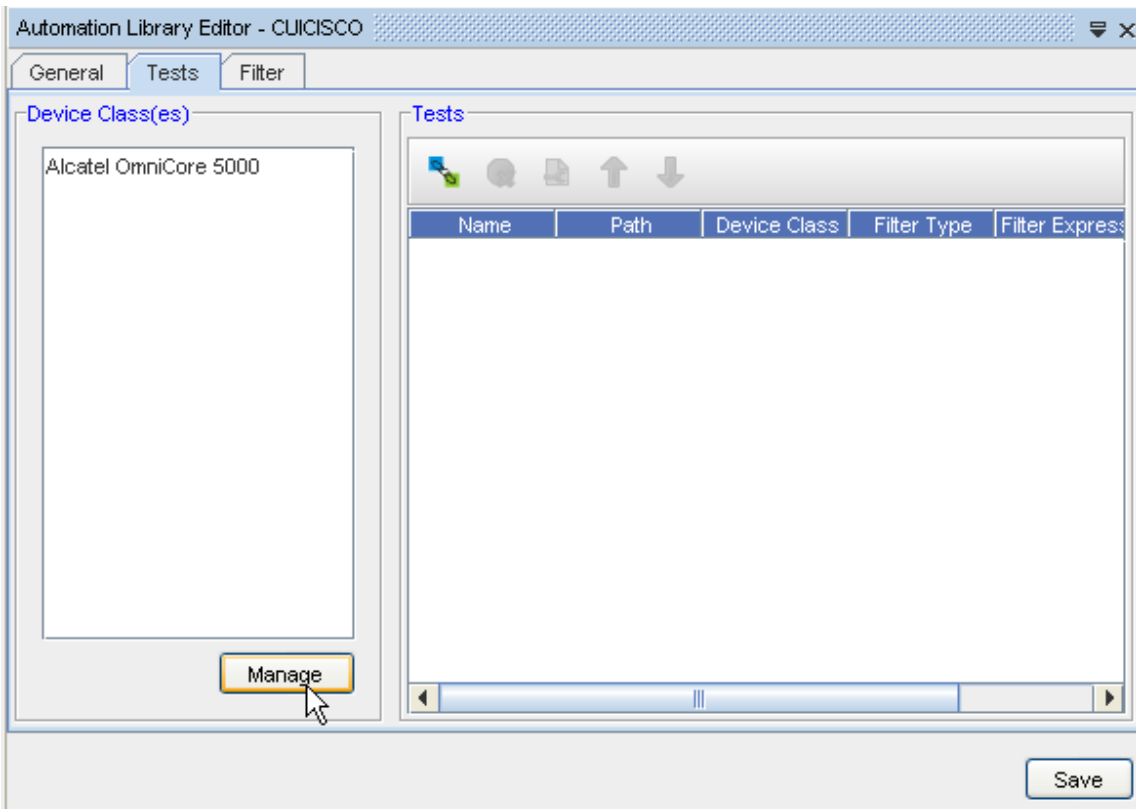


1 Beginning with the **General** tab, make sure the name is correct. If not, make changes, then click **Save**.

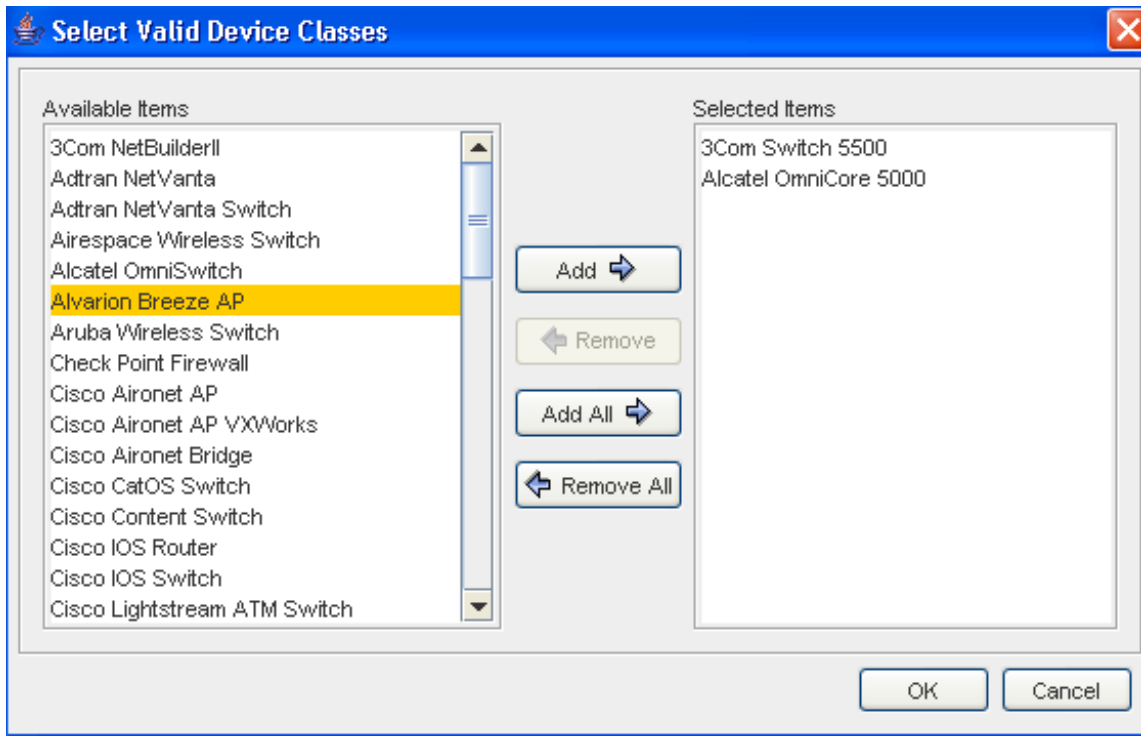
2 Click the **Tests** tab.

At the Tests tab,

1 At the **Tests** tab, click **Manage** to select the Device Classes from the list.



2 Move the selected Device Classes from the Available items column into the **Selected Items** column, by first highlighting the item or items in the Available Items column, then clicking the **Add** or **Add All** button.








- 3 Click **Ok** after moving the devices classes into the Selected Items column.
- 4 To Link a Standard to a test, click the **Add** button, and then select a test. Once the test is selected, click **Ok**. See that test you selected is now linked into the Standard.

Test tool bar

When in the Test section of the Tests tab, the tool bar can be used.









Icon	Usage
	Used to add a test.
	Used to remove an existing test.
	Displays the Add Audit Units window, allowing you to add any available Audit Units and Device Classes if applicable.
	Moves any test you have to the top-most position.
	Moves any test down on the list of tests.

At the Filter tab,

- 1 At the **Filter tab**, select to add filters by first clicking the **Add Condition** bar, then selecting the filter criteria from the **Attribute** and **Operator** drop-down arrow options.
- 2 Add and **Expression**, then click **Save**.

Filter tool bar

When in the Test section of the Tests tab, the tool bar can be used.

Icon	Usage
	Used to add a filter condition.
	Used to remove an existing filter condition.
	Displays the Add Attribute window, where you can add an attribute to the list of filters.
	When an attribute Name column is clicked, you can then use this icon to remove the clicked attribute name from that listing of attributes (or columns).
	Moves any test you have to the top-most position.
	Clears any attribute from the list.

- 3 You can now **Close** the Automation Library Editor, and see your Standard is now in the folder you used to create your Standard in.

**Note** Once a Standard has been created and then added to the Library Manager, you can then right-click on that Standard, and select Edit (to change any previously selected options), or you can select Delete to delete it from the list.

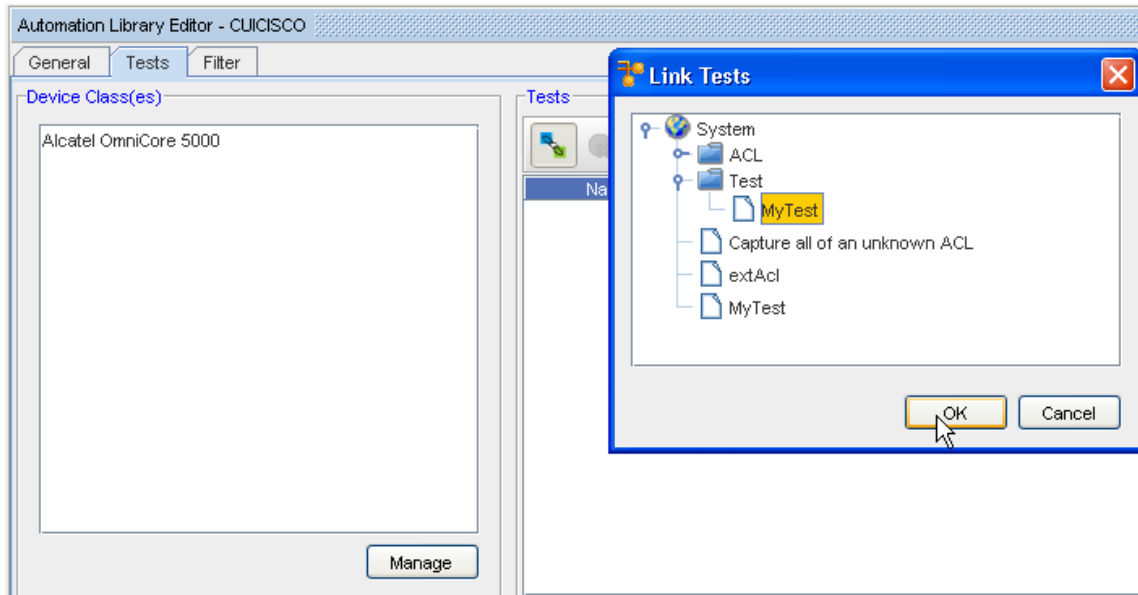
For a Test to be linked to a Standard, the Test must be defined **before** it is shown as available for linking to a Standard.

### Removing Standards

Standards can be deleted (removed) when they are no longer needed to validate config files.

### Adding a Test to a Standard

- 1 You can add an **Attributed Test** to a standard in the same way that you add a RegEx-based test to a standard.
- 2 [Creating a New Standard](#) in the Automation library, and use the **Tests** tab to first add the appropriate Device classes to be tested using the Manager button.
- 3 Now, using the **Add** icon, add **Tests** to the standard.



- 4 At the Add Tests window, select the **test** (or tests) you want to add to the Standard. Click **Ok** when you have selected the tests to add.
- 5 Once added, click **Save** to save this Standard.

---

**Note** Attributed tests, as well as RegEx tests can be selected for the same standard.

---

One significant difference is when selecting an attributed test, is that the Attributed Test automatically picks the appropriate Configuration Unit to be audited.

The algorithm to do this is based on examining the various terms in the Attributed Compliance Test rules, and choosing the Configuration Unit that contains the most number of terms from the rules.

---

**Note** For RegEx tests, you must pick the appropriate textual configuration unit, if there is more than one.

---

## Working with a Policy

### Creating a New Policy

A policy is a set of **user-define guidelines** for any device configuration changes. These guidelines can only be defined by a user with Manage Compliance privileges.

A Policy must be selected, and then applied to a resource. Whenever a new or changed device configuration is pulled or pushed into the system, the configuration is run against the Policy for a compliance check .

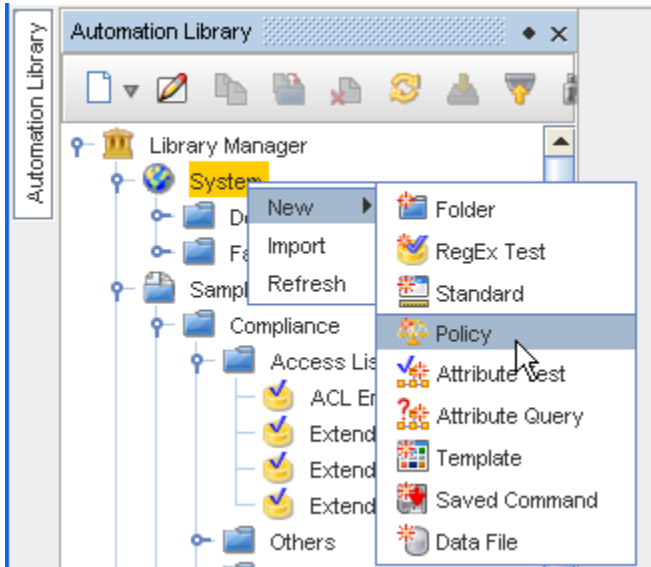
---

**Note** With Multi-Config, Compliance Policies now incorporate Standards and Tests targeted on specific configuration files.

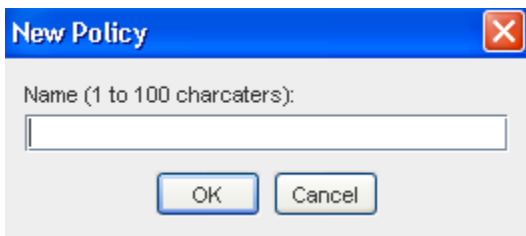
---

- 1 Open **Tools->Automation Library** .

- Expand the **Library Manager**.



- Right-click on **System** (or a folder name), then select **New**, then **Policy**.

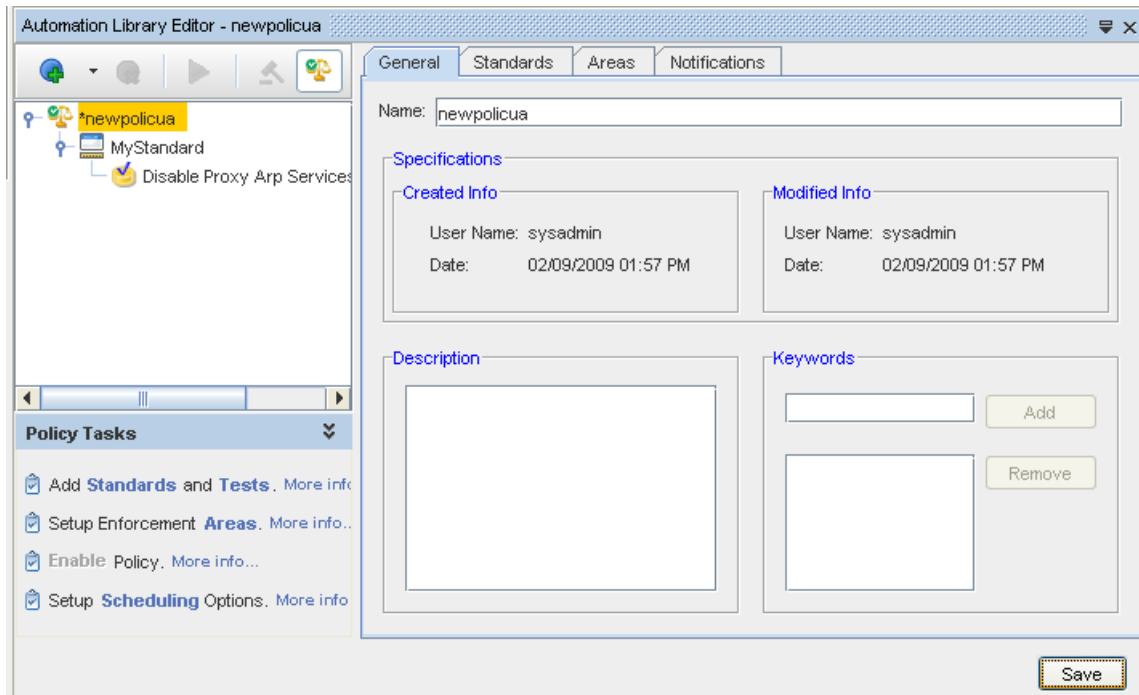


- Enter a Policy **Name**, then click **Ok**.
- With the Automation Library Policy Editor displayed, begin creating the Policy using the **tabs** in the Editor (General, Standards, Areas, and Notifications).

---

**Note** You can use the Policy Tasks to take you through the list of activities you must complete to create a policy. For more information on using the Policy Tasks, go to [New Policy View](#), and [Policy Tasks - Quick Complete - Quick Complete](#).

---



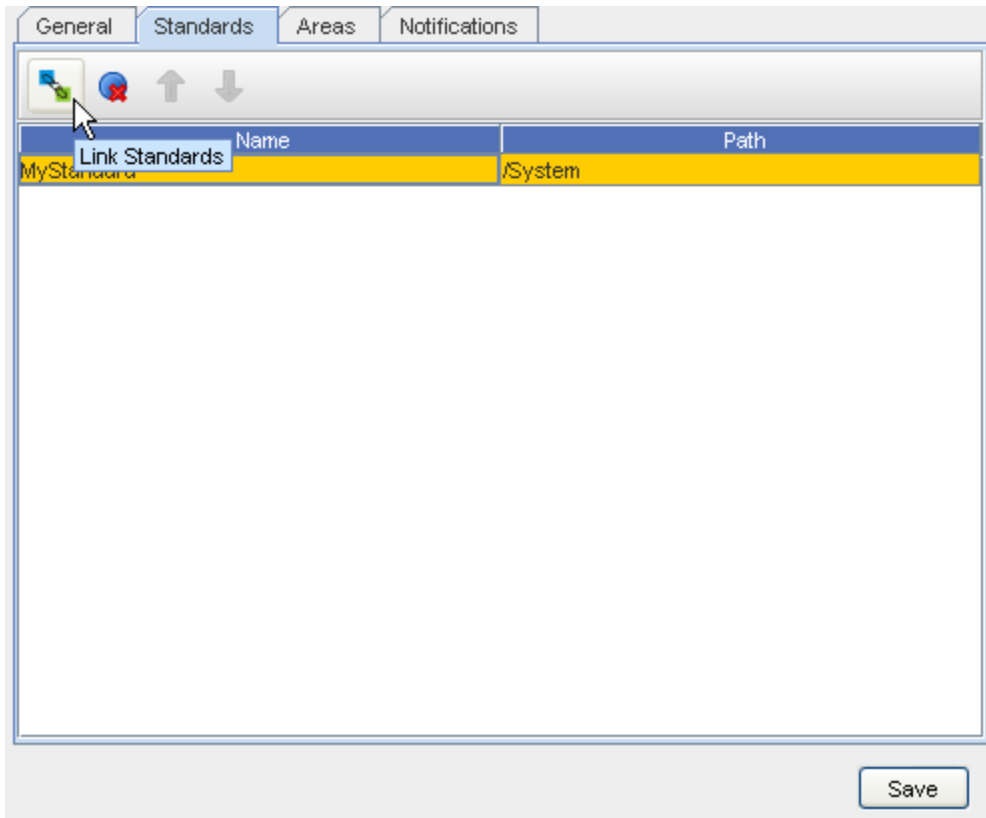
At the General tab,

- 1 Here you can enter a **Description** to make this policy distinctive.
- 2 You can also enter keywords by entering a keyword, then clicking the **Add** button in the **Keywords** section. Continue on to the Standards tab.

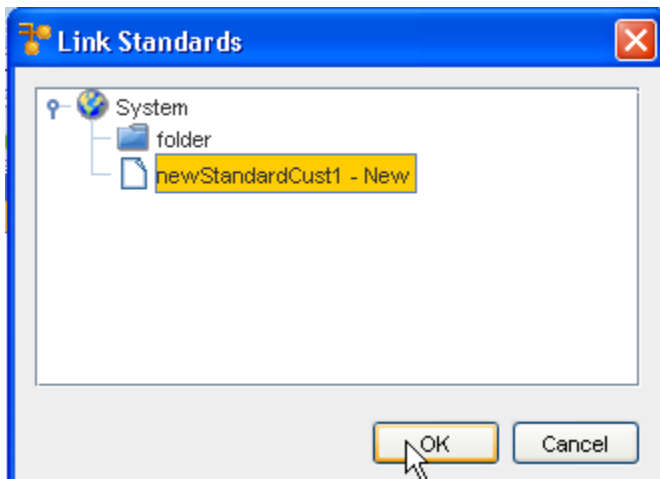
The screenshot displays a web-based configuration interface for a Network Configuration Manager. At the top, there are four tabs: 'General', 'Standards', 'Areas', and 'Notifications'. The 'Standards' tab is currently selected. Below the tabs, a text input field contains the name 'newpolicua'. Underneath, there is a 'Specifications' section containing two sub-sections: 'Created Info' and 'Modified Info'. Both sub-sections show 'User Name: sysadmin' and 'Date: 02/09/2009 01:57 PM'. Below these are two more sections: 'Description', which is an empty text area, and 'Keywords', which includes a text input field, an 'Add' button, and a 'Remove' button. At the bottom right of the interface is a 'Save' button.

At the Standards tab,



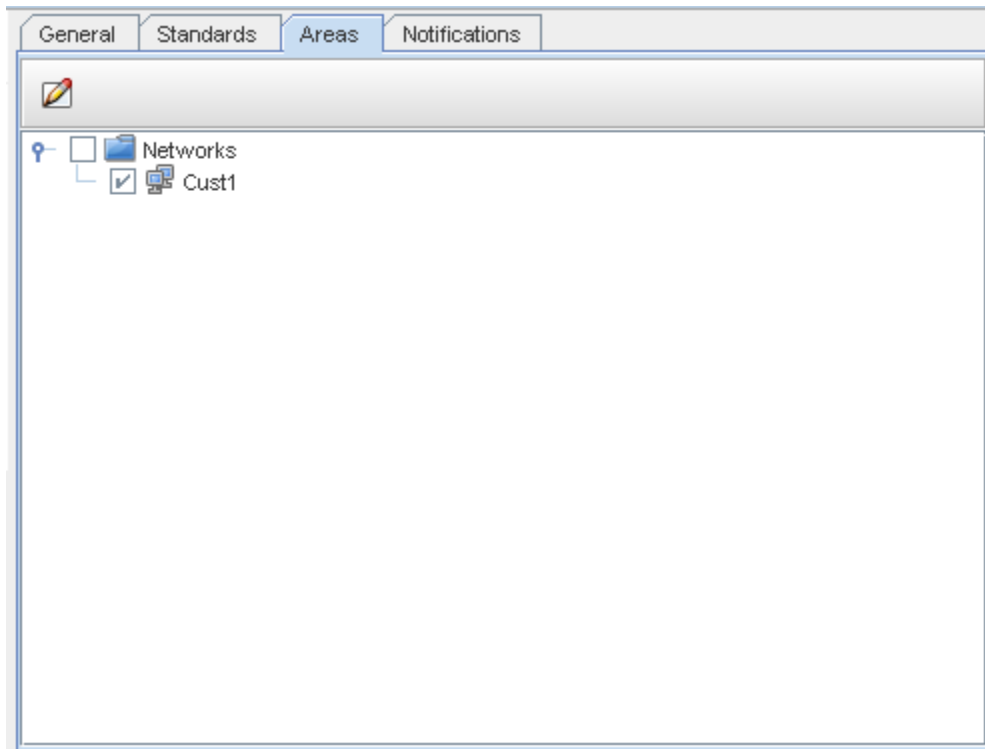


- 1 Go to the **Standards** tab, and enter the information needed for the Policy. Click **Link Standard** to link a **Standard** from the selections (under System) that display in the Link Standards window.



- 2 Click **Ok**.

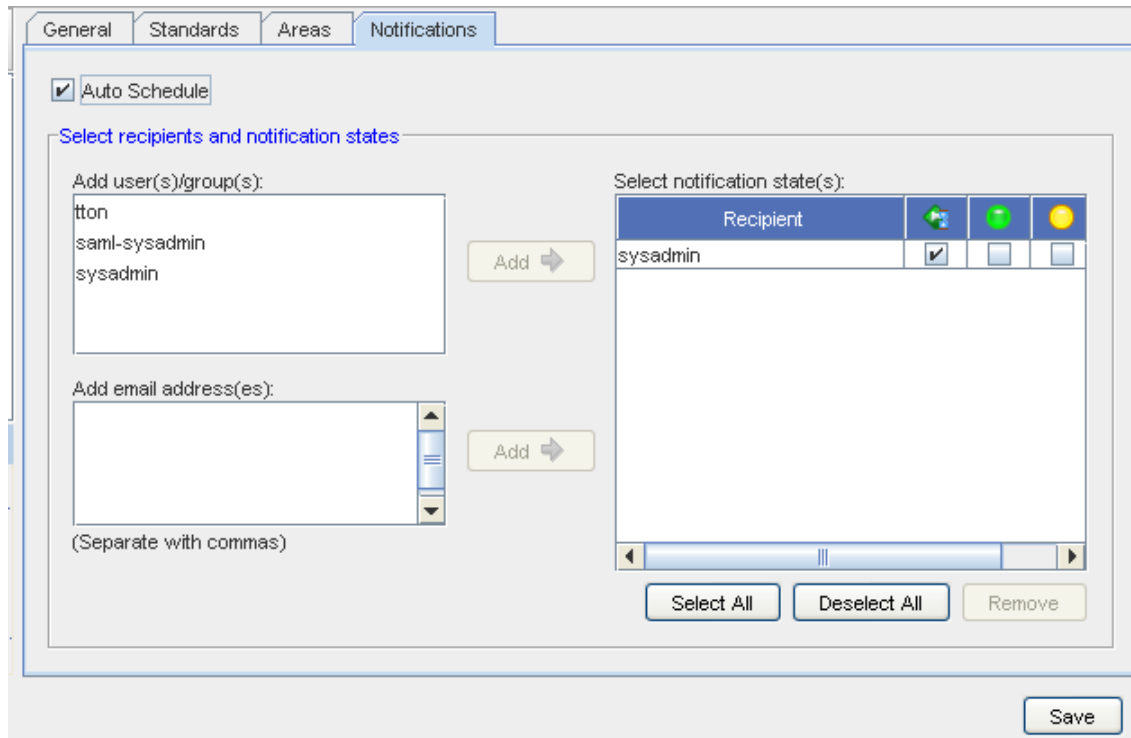
At the Areas tab,



- 1 At the **Areas** tab, select the **Edit** icon in the toolbar to launch a popup field, where you can set or modify areas this policy affects, or make your selection from what is displayed in the panel.
- 2 Click **Save**.

At the Notifications tab,

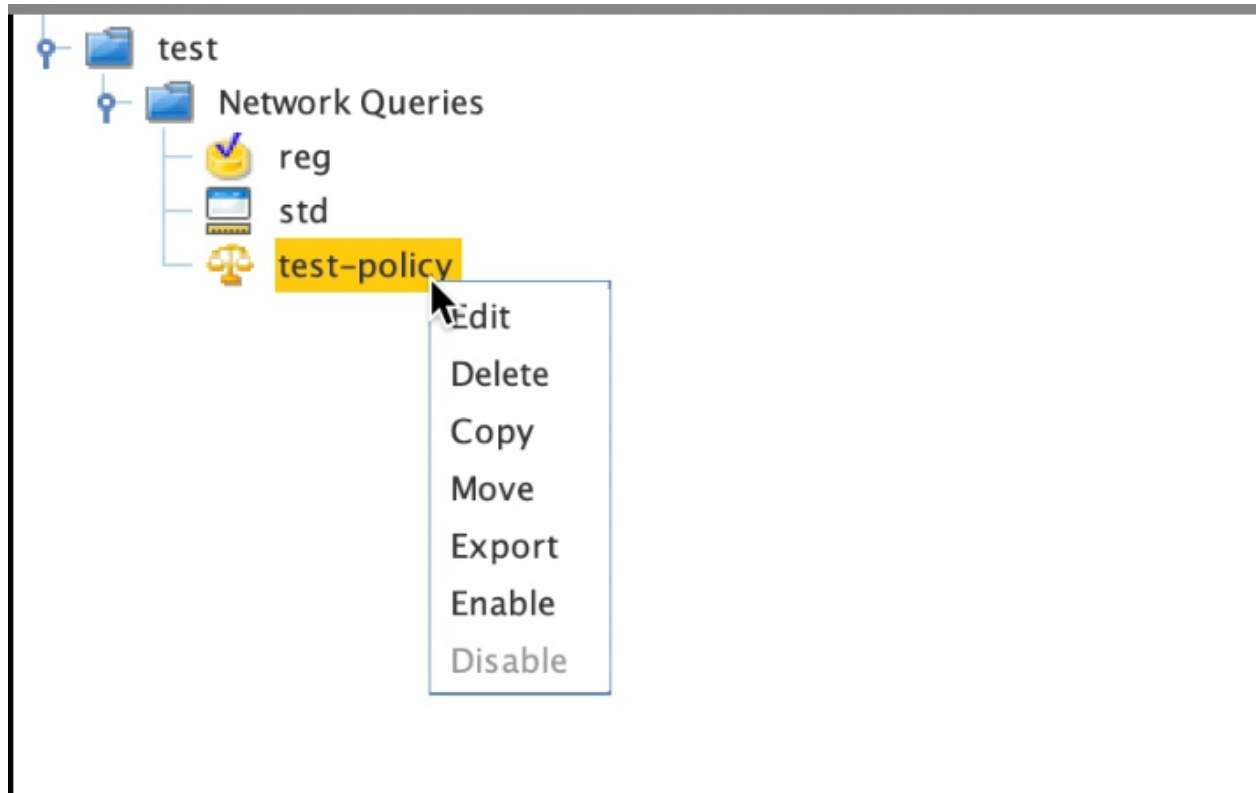
From this tab you can **Automatically Schedule the jobs to push remedies** generated by Compliance tests to any non-Compliant devices.



- 1 In the top portion of the tab, click within the **Auto Schedule** check box. Select **Auto-Schedule** for remedy jobs to be scheduled by the application.
- 2 In the **Select recipients and notification states** section of the window, you can add the users to the Select Notification states by first highlighting the user name, then clicking the **Add** button.
- 3 At the **Add email address(es)** section, you can enter in as many **email address** as you need to ensure the notification of the job is sent to those who need to have this information. Once you add an email address, click the **Add** button. This moves the email names you have entered into the Recipient section.
- 4 At the **Select notification state(s)** section, place a check mark into each appropriate notification check box. You can also Use the Select All or Deselect All buttons for notification. You can also double-click a row to select all the check boxes within that row.
- 5 Once your list of recipients and their notification states are selected, click **Ok**.

### Right-Click Options on Policy

Once you have established your Policy , there are several actions you can take using the right-click options.



You can select:

- **Edit** - to open the Automation Library Policy , and make any needed changes or edits
- **Delete** - to remove this policy from the container
- **Copy** - to copy this policy to use at another location, or to use as a template to create another policy
- **Move** - this policy to another location within your network
- **Export** - this policy to a location outside your network
- **Enable** - to enable the policy

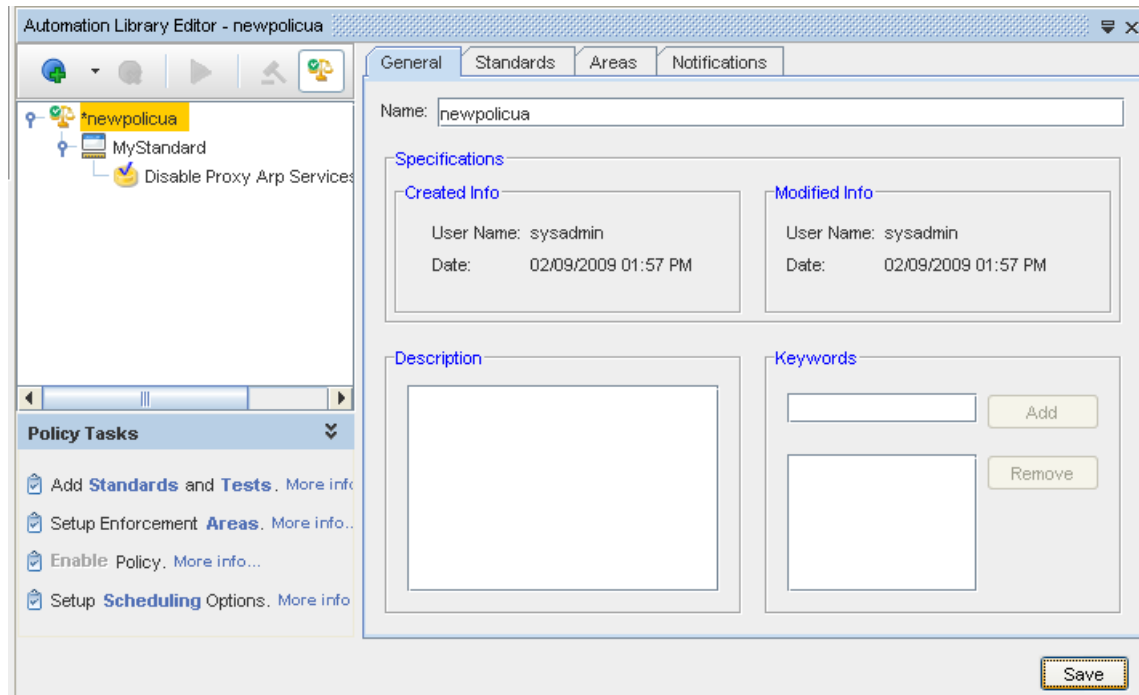
### New Policy Tasks - Quick Complete

### New Policy View, and Policy Tasks - Quick Complete

New Policy View, and Policy Tasks - Quick Complete

With this release, an enhanced way to view and work with the policy and all of its components has been added to the editor. The view consists mainly of a navigation tree showing the Policy as the root, and all the Standards and their linked tests and queries.

Clicking an item within the navigation tree (left panel) changes the tabs displayed in the right panel to allow viewing and editing of the item selected from the tree.



A toolbar above the navigation tree provides additional icons allowing you to work quickly with the policy components.



The toolbar in Policy Tasks provides the following capabilities:

- Adding a Standard to the Policy (see [Adding Standards and Tests - Using Policy Tasks Using Policy Tasks](#)).
- Adding a test ( [Creating a New Attributed Test](#) or [Creating a New RegEx Compliance Test](#)) to the Policy (see [Adding Standards and Tests - Using Policy Tasks Using Policy Tasks](#)).
- Adding an Attributed Query
- Removing items from the Policy
- Running an Attributed Test or Query
- Enforcing a Policy
- Enabling a Policy

In addition, a Policy Tasks panel is displayed below the tree that provides a quick status of the policy's overall completion status. The panel shows three tasks **required** for the policy to become effective, and **one optional** task (scheduling).

Each task provides links that launch into the dialogs or tabs needed to complete that specific task.

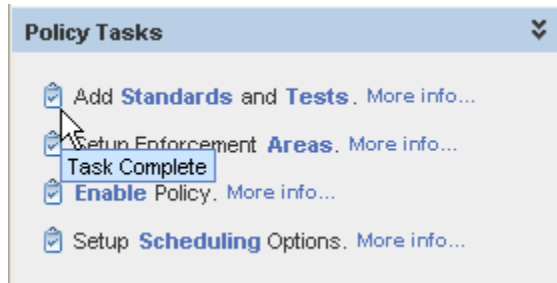
---

**Note** Note that these links are a quick access to the actions that can be completed using the tool bar options in the Library Editor.

---



When each task is completed, a check mark displays to indicate that task is now complete.



Note that the policy can be saved, even when one or more of the tasks is incomplete.

### **Adding Standards and Tests - Using Policy Tasks**

When using the Policy Tasks check list, notice that when you select to Add a Standard, the Add Standard window opens. Also, behind this window, the Policy Editor has automatically moved into the Standard tab.

The first option is Add Standards and tests. This task is marked complete when at least one standard, with one enabled test is added to the policy .

The More Info...link that offers you some important information. Use this link to refresh your memory on creating Standards and Tests.

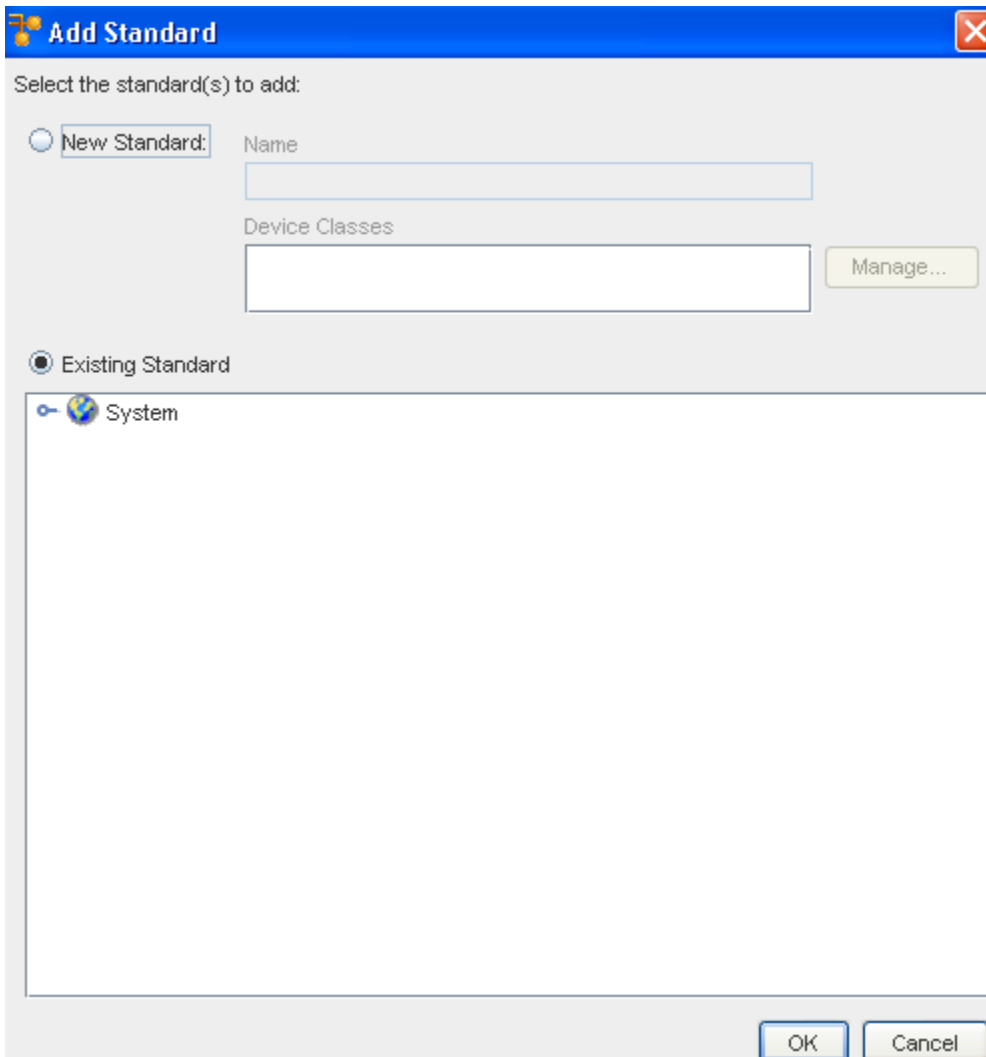
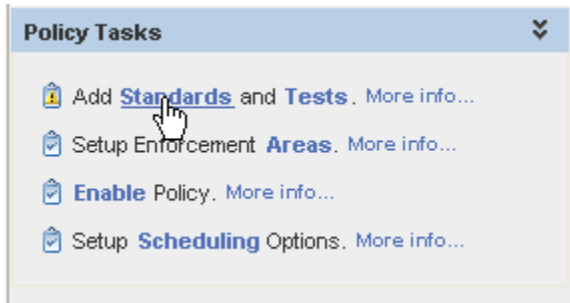
---

**Note** You can also click More info... for additional information on this task.

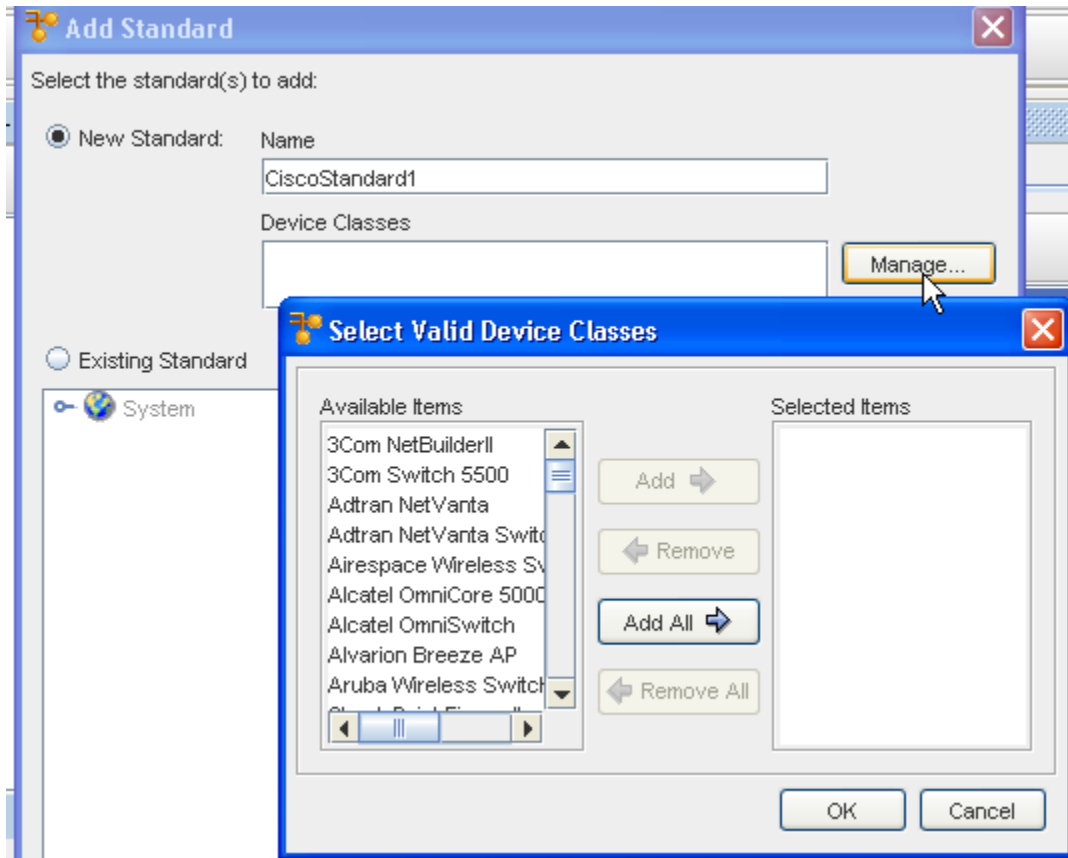
---

Standards

### **Add Link Standards - Selecting New Standard**



- 1 You can select a New Standard, by clicking in the New Standard radio button. Enter a Standard Name , then select Manage to view, and then select a valid Device Class .



- 2 Once you have moved your Available Device Classes items into the Selected Items pane, click OK.
- 3 At the Add Standard window, click Ok. A new Standard is created, and is displayed in the Policy tree. The Standard is created in the same folder where the Policy resides.

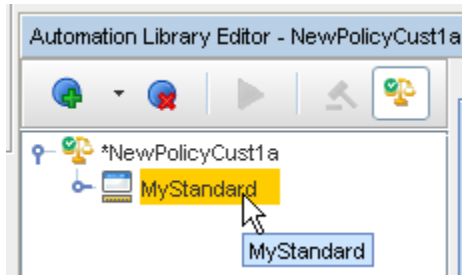
#### Add Standards - Selecting Existing Standard

- 1 If you have selected the Existing Standard radio button, you can navigate through the system to select an existing Standard to add.
- 2 Once you have made your selection, click Ok.

You can add either a new or existing Standard, or both. There is no limit on the number of Standards you can add to a Policy.

The standards you have selected are now listed under the Policy name in the navigation tree. If you have added an existing Standard that is already linked to Tests, the Tests are listed under the Standard's name in the tree.



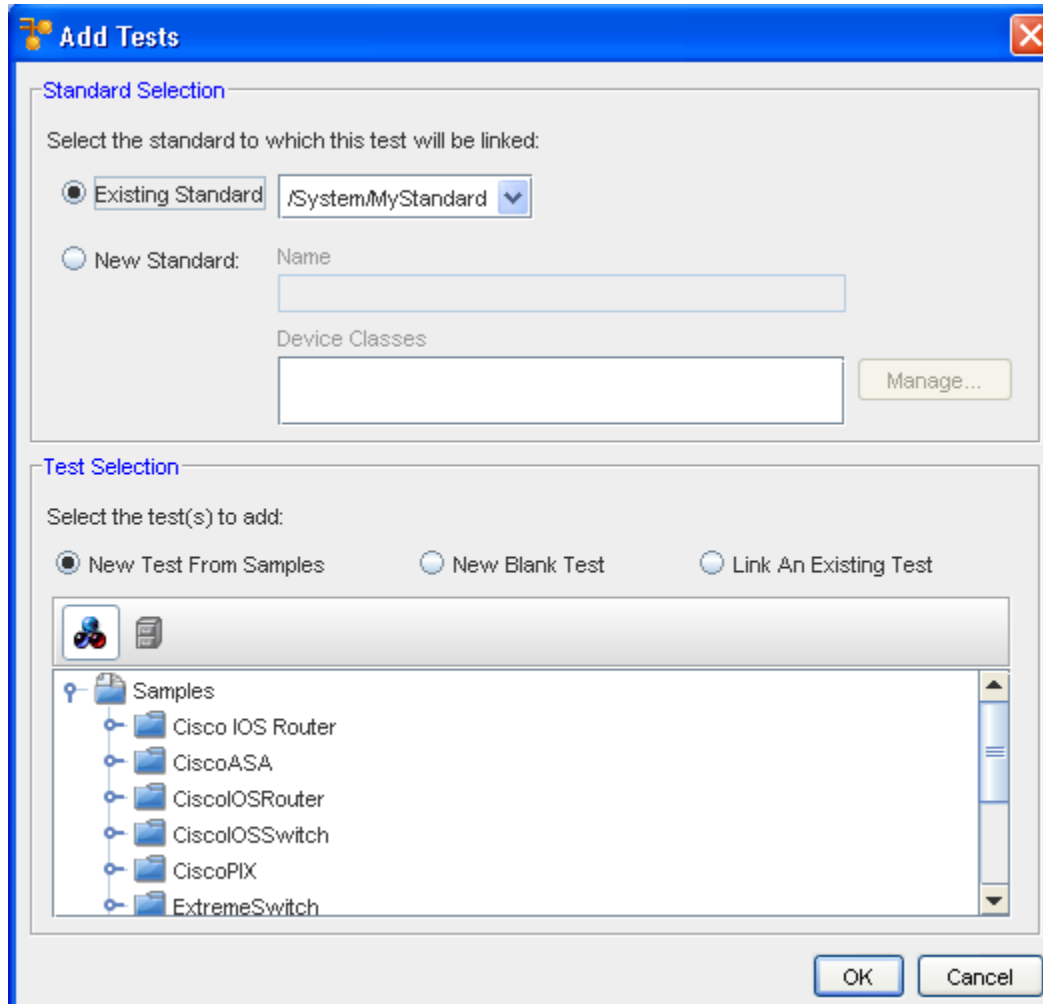


## Adding Tests - Using Policy Tasks

### Add Tests - Standard Selection

A Test can only be added to the policy by linking it to a standard.

This dialog allows you to select the standard under which the test is added, or to create a new standard. If a standard was selected in the Policy tree, this standard is displayed as the default selection.

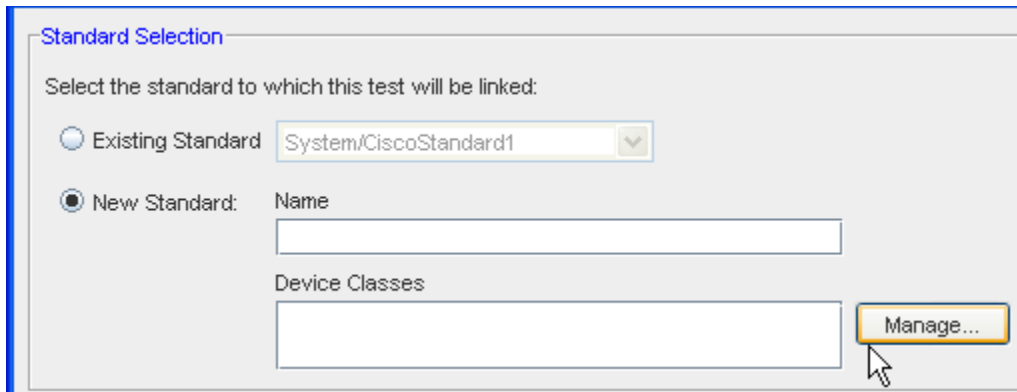


- 1 To select an Existing Standard , click in the Existing Standard radio button, then select a Standard (from the drop-down arrow options) to link to the test. The drop-down arrow shows all the Standards that are linked to the Policy.

**Note** Note that this option is not available when the Policy is not linked to any Standards.



- 2 If selecting a New Standard, click within the New Standard radio button.

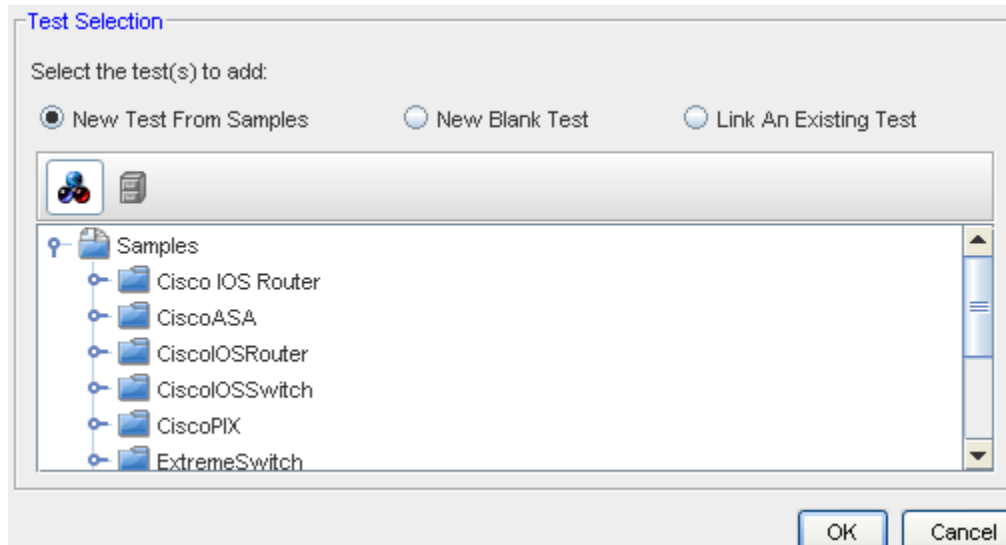


- 3 Enter a Standard Name, then click Manage to select one or more valid Device Classes.
- 4 Click Ok when you have made your Device Classes selections.

### Test Selection

At the Test Selection section, you have several options to choose from in selecting the test (or tests) to add to the Policy.

- **New Test From Samples** : create one or more tests using VMware provided Samples as a template. This option creates new copies of the selected sample tests, and links them to the selected standard.
- **New Blank Test** : creates a new test, starting with an empty form. The new test is created and linked to the selected standard.
- **Link an Existing Test** : if the tests you want to add to the policy already exists in the Automation Library, this option allows you to add the tests to the policy.



### Add Tests - New Test From Samples

- 1 If you select the New Test From Samples radio button, a listing of the Sample tests is presented. Go through the list, then expand the list to view the tests.

2 Make your selection from this list, then click Ok.

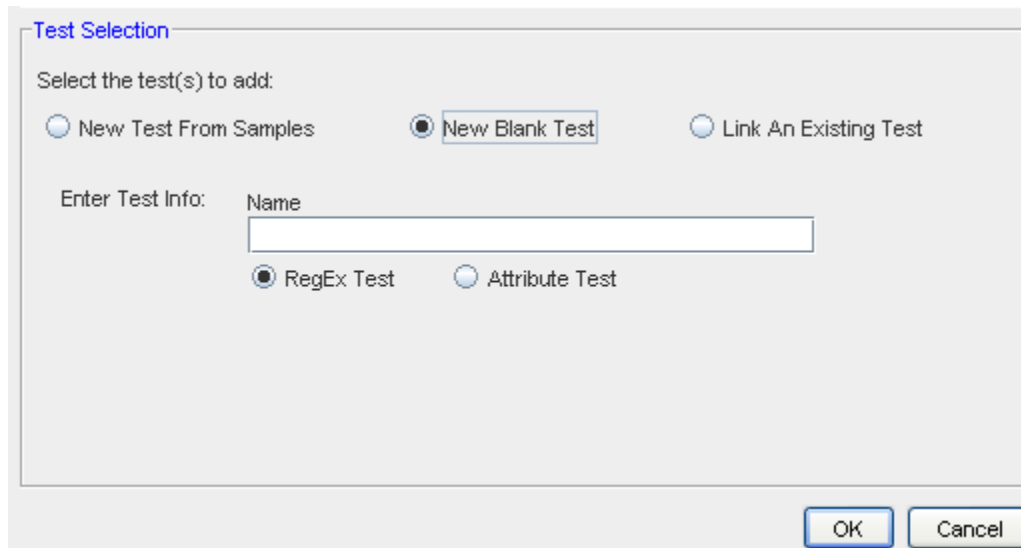
When using this option, you can browse Samples by Device Classes (using the icon shown below), or browse Samples by Categories (using the icon to the right - shown below).



When you have completed both Adding a Standard and a Test, the check mark is added to this task, and you can move on to the next Policy task.

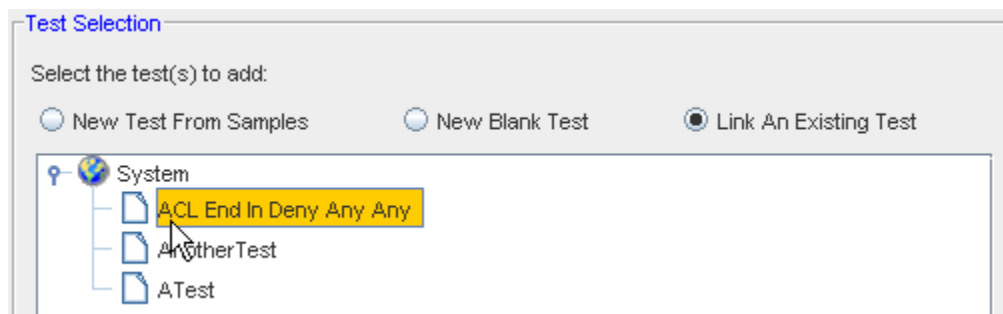
### Add Tests - New Blank Test

- 1 When New Blank Test is selected (as shown below), you can enter the Name of the test, and select the appropriate radio button for either a RegEx test or an Attribute Test.
- 2 After entering the test name and selecting the type of test, click Ok.



When you have completed both Adding a Standard and a Test, the check mark is added to this task, and you can move on to the next Policy task.

### Add Tests - link and Existing Test



If you select to Link An Existing Test, all existing tests are displayed. From here, you must select at least one test for linking into the Policy. Once selected, click Ok.

When you have completed both Adding a Standard and adding a Test, the check mark is added to this task, and you can move on to the next Policy task.

### Standard Test Device Class Mismatch

RegEx tests have filters that can specify to which Device Class the test applies. When a test is added, either from the samples for from existing items, a check is performed to ensure that the Test and the Standard Device Class match.

---

**Note** You are still allowed to add the test to the Standard, even if there is a mismatch.

---

### Linked Tests Auditable Units

When a test is linked to a Standard, you are allowed to select the configuration files to which the test applies. By default, the application selects the Primary text-based configuration unit for each device class specified in the Standard for a Regular Expression test.

For an Attribute test, the application uses an algorithm to determine the default configuration unit, based on the tables included in the test. It is possible that a default configuration unit cannot be determined. In this case, the application alerts you that a default configuration was not assigned for one or more device packages.

### Setup Enforcement Areas

#### Editing Standards and Tests within the Policy Editor

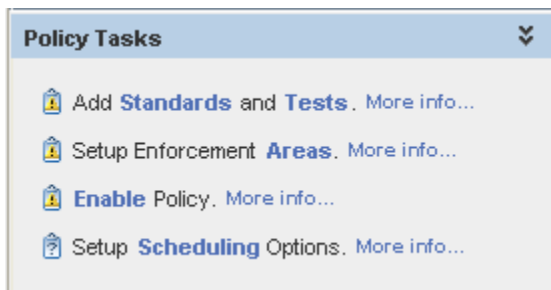
#### Enable Policy

#### Setup Scheduling Options

#### Setup Enforcement Areas

When using the Policy Tasks check list, notice that when you select to **Setup Enforcement Areas**, the Select Enforcement Areas window opens. Also, behind this window, the Policy Editor has automatically moved into the **Areas** tab.

- 1 From the Policy Task check list, select The Setup Enforcement **Areas** link.

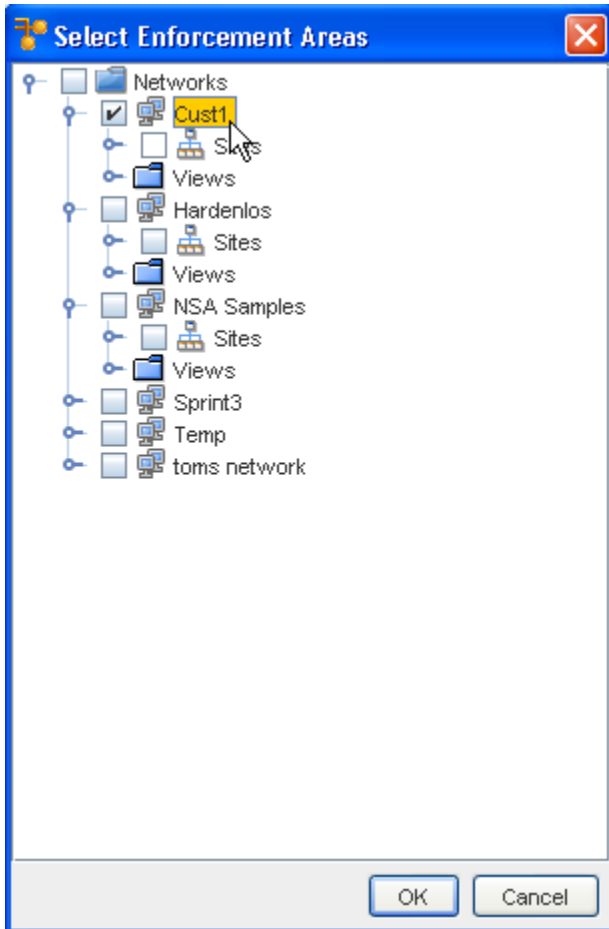


The Select Enforcement Areas window opens. From this window you can expand on the selections, to further see what areas are available.

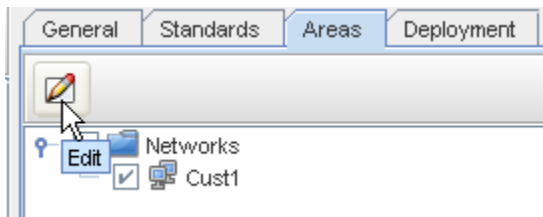
---

**Note** You can also click **More info...** for additional information on this task.

---



- 2 Make a selection from the **Enforcement Areas** by clicking within the check boxes, then click **Ok**.
- 3 If you review your selection and want to edit the actual areas, click the **Edit** icon to once again go to the Areas tab, and make a selection change, or add additional selections.
- 4 Click **Ok** when you have made changes to your original selection.

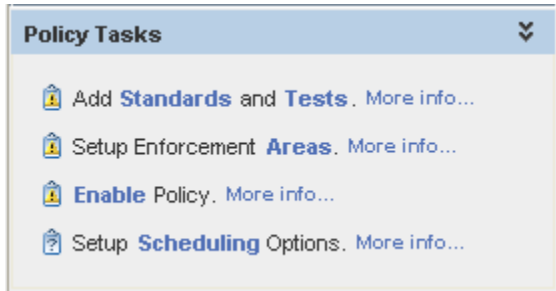



Notice that once you have made your Enforcement Areas selections, a Policy Tasks check mark has been added to the listing of Policy Tasks. You can now go on to the **Enable Policy** task.

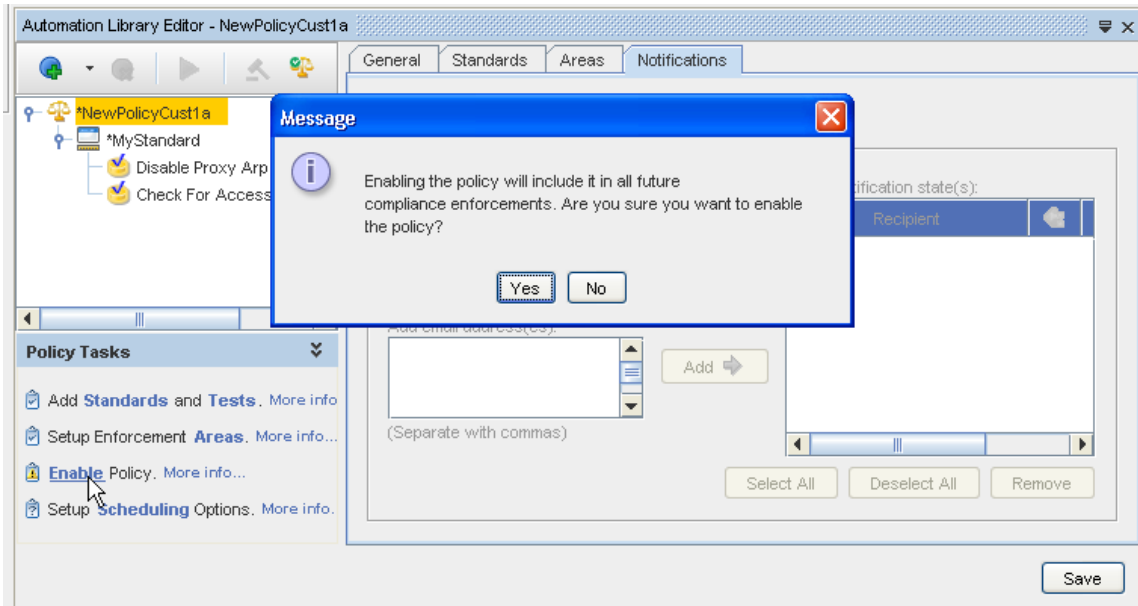
[Adding Standards and Tests - Using Policy Tasks](#)  
**Enable Policy**

When using the Policy Tasks check list, a confirmation Message appears asking if you are sure you want to enable this policy.

**Note** You can also click **More info...** for additional information on this task.

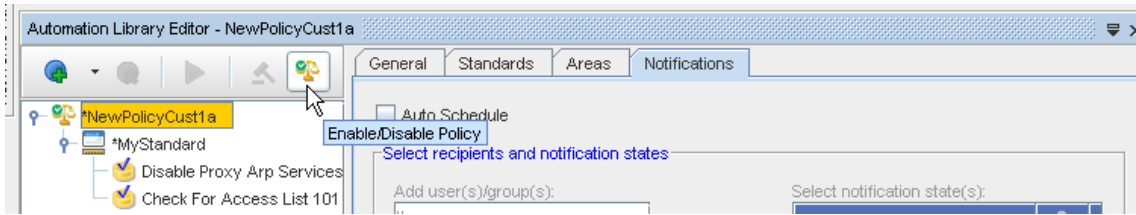


- 1 when using the Policy Tasks check list, notice that when you select to  **Enable Policy** a Message appears asking if you are sure you want to enable this policy.



Once you have a Policy that is present in the navigation tree, you can select to Enable or Disable that specific Policy. Notice that each time you select a Policy, then click the **Enable/Disable Policy** icon, a confirmation Message appears. Notice also that a Policy must be saved before it can be Enabled. If the Policy is not saved, the Enable Policy icon is not selectable from the tool bar.

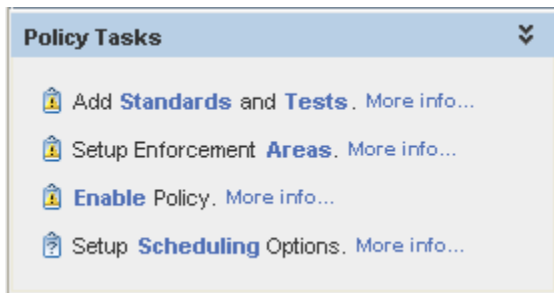
- 2 Read the message, and then select to **Yes** Enable/Disable the Policy, or **No**, do not Enable/Disable the Policy.



## Adding Standards and Tests - Using Policy Tasks

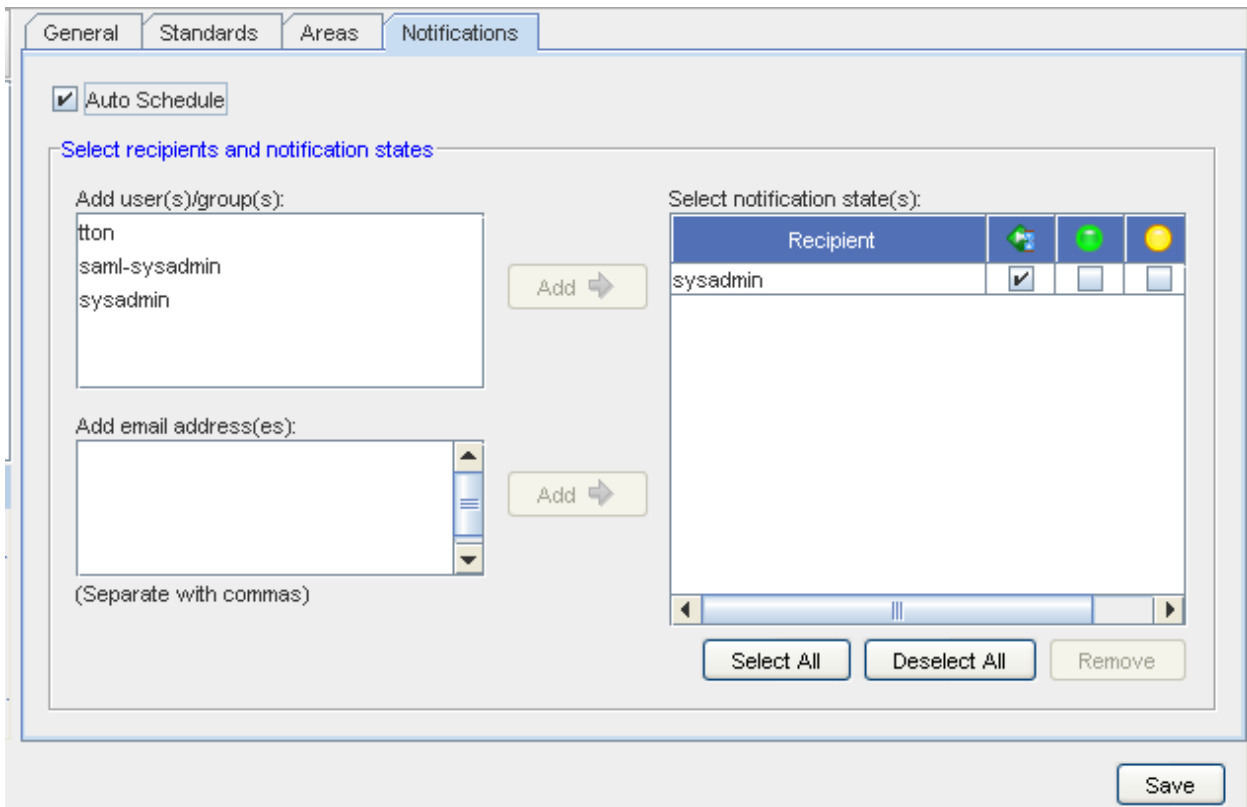
### Setup Scheduling Options

When using the Policy Tasks check list, notice that when you select to **Setup Scheduling Options**, the Policy Editor has automatically moved into the **Notifications** tab.



**Note** You can also click **More info...** for additional information on this task.

From this tab you can **Automatically Schedule the Policy** to run for compliance verification.



- 1 In the top portion of the tab, select the check box to **Auto Schedule**.



- 2 In the **Select recipients and notification states** section of the window, you can add the users to the Select Notification states by first highlighting the user name, then clicking the **Add** button.
- 3 At the **Add email address(es)** section, you can enter as many **email address** as you need to ensure the notification of the job is sent to those who need to have this information. Once you add an email address, click the **Add** button. This moves the email names you have entered into the Recipient section.
- 4 At the **Select Notification State(s)** section, place a check mark into each appropriate notification check box. You can also Use the Select All or Deselect All buttons for notification.
- 5 Once your list of recipients and their notification state are selected, click **Ok**.

When you use the Policy Task check list (going from one task to another) upon completion of that task, a check mark displays to the left of that task indicating that task is now complete. You have now completed the Auto Schedule portion of the Policy Tasks.

### Adding Standards and Tests - Using Policy Tasks

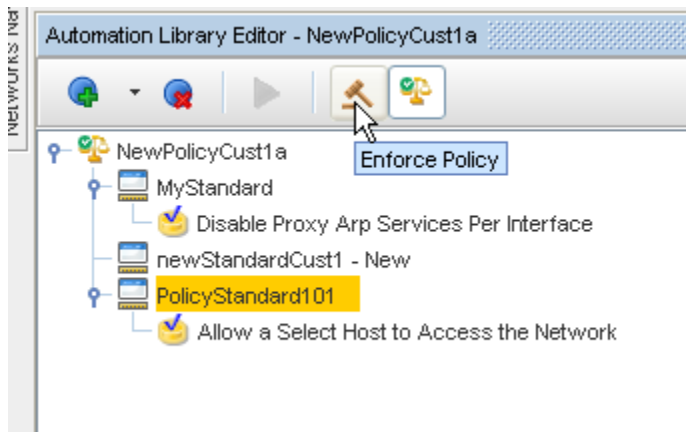
#### Enforce Policy Task

- 1 Once you have your completed Policy, you can then enforce the Policy by selecting the Policy, then selecting the **Enforce Policy** icon. You can also enforce the Policy after making changes. Note that the Policy must be Enabled for this action to have any effect.

---

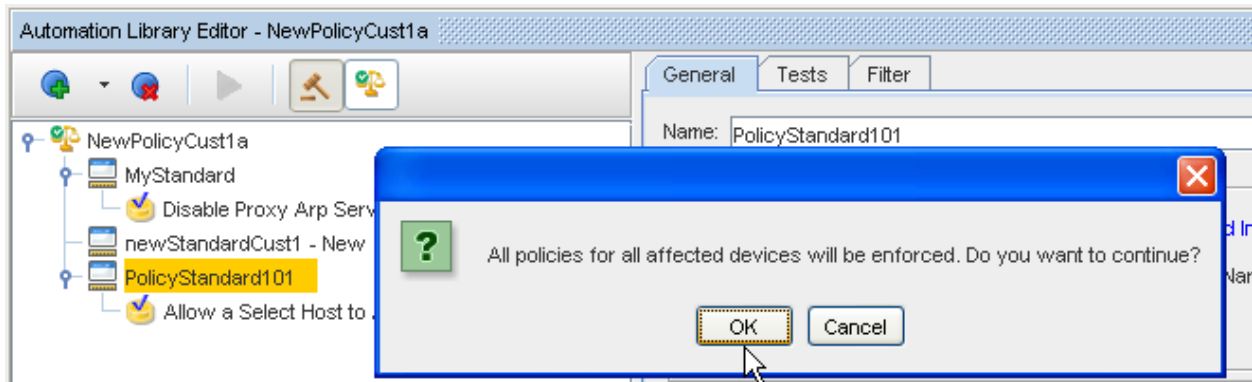
**Note** If the Policy is not Enabled, the Enforce Policy icon is not selectable.

---



- 2 After selecting to Enforce the Policy, a message appears (as follows). Select **OK** to continue to Enforce the Policy, or **Cancel** to stop the action.

If you select **Ok**, a process begins to enforce Compliance on all the devices included within the Policy's enforcement area. When the process is complete, all views that show the compliance state are refreshed to display new compliance states.



Now, all policies for all the affected devices are enforced.

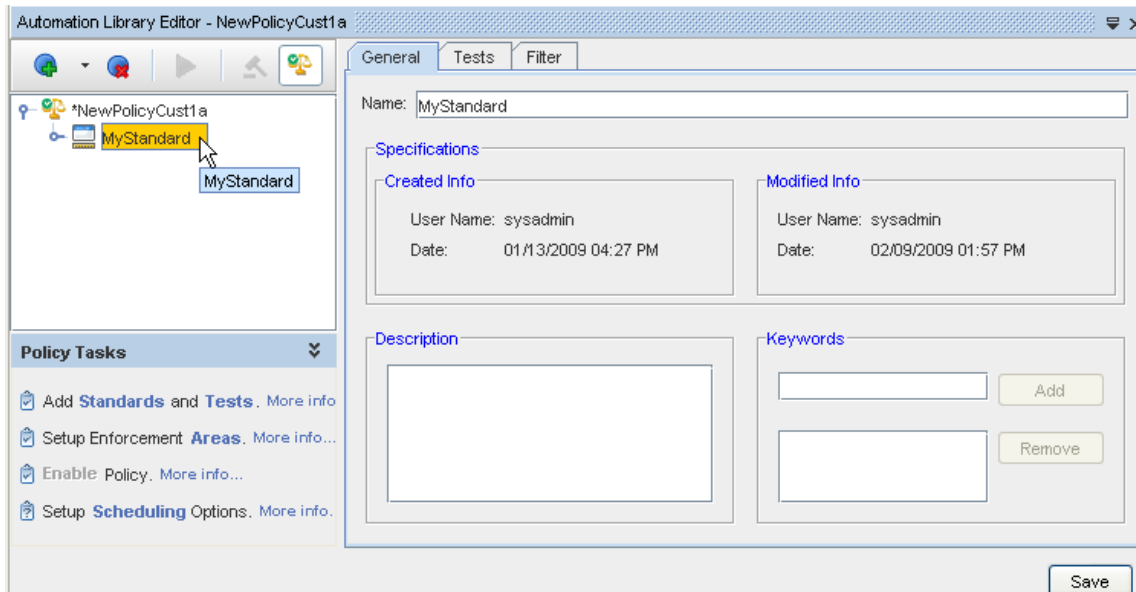
### Adding Standards and Tests - Using Policy Tasks

#### Editing Standards and Tests within the Policy Editor

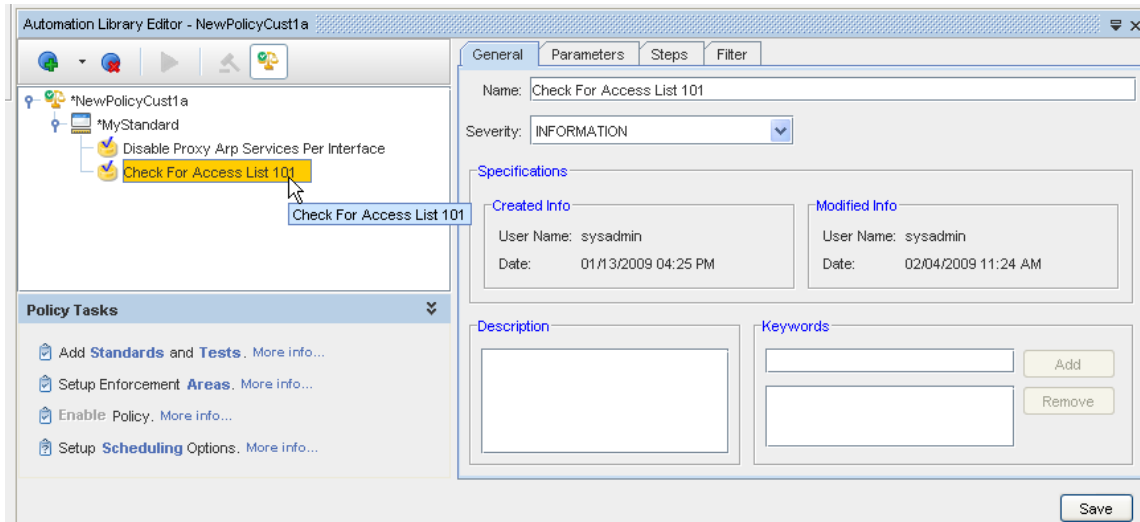
After creating a new Policy, or locating and selecting an existing Policy from the Automation Library, you can **edit** that Policy, the Standard, and the Test from **within the navigation tree** in the Policy Editor.

For example, when you have created a new Policy, then have the Policy open for editing, you can go through the policy tasks. The first task would be to add a Standard, then to add a Test.

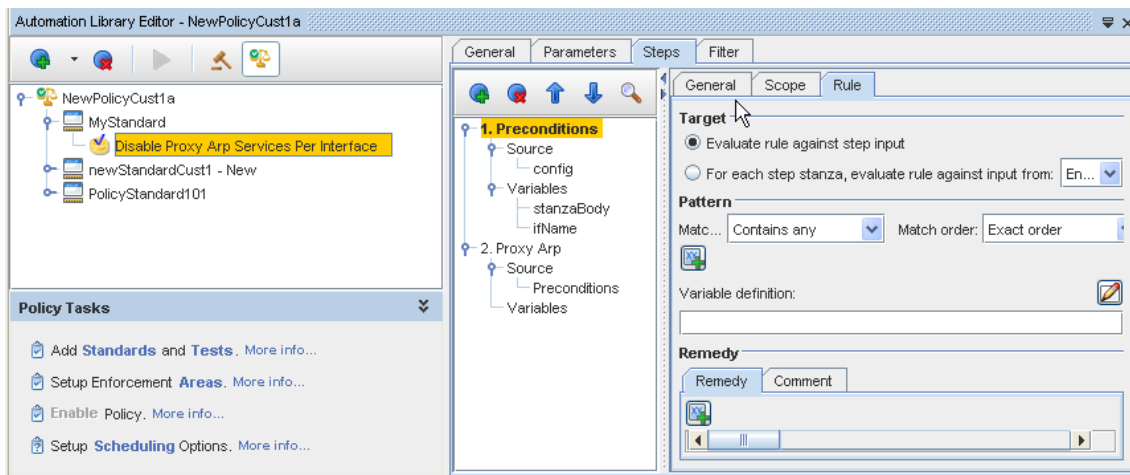
Once you have added a **Standard** and **Test** to the Policy, you can go to the Test and the Standard (located in the Navigation tree of the Policy), and then Edit the contents of the Standard and Test - all while you are still in the Policy Editor.



- 1 By just clicking the **Standard name** in the Policy navigation tree (as shown above), the Standard Editor opens. At the Standard Editor you can edit the existing Standard information contained in any or all of the tabs (General, Tests, and Filter), and then **Save** those Standard changes.



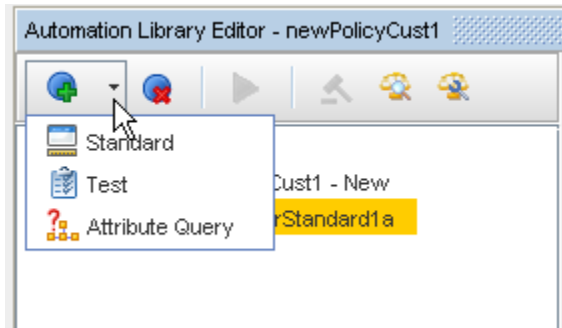
- 2 You can also click the **Test name**, in the Policy navigation tree, and open the Test Editor. From the Test Editor, you can make any needed changes in any of the tabs, then **Save** your changes.



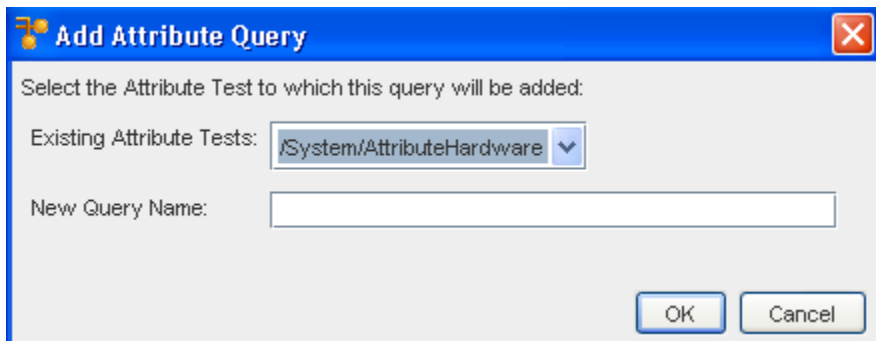
You can also work within the test to **add** a new test, **remove** an existing test, **enforce a policy**, or **change the order** of the tests as they appear in this section.

#### Add another Standard, Test, or Attribute Query

- 1 When you click the **Add** icon, and then select to add **another Standard**, the Standard Editor opens, where you can enter the appropriate information into the Standard Editor tabs. Be sure to **Save** this Standard when you are through adding content.
- 2 If you decide to add another **Test**, the Test Editor opens, allowing you to create the test here within the Policy. Go through each tab to enter the information for this new test.



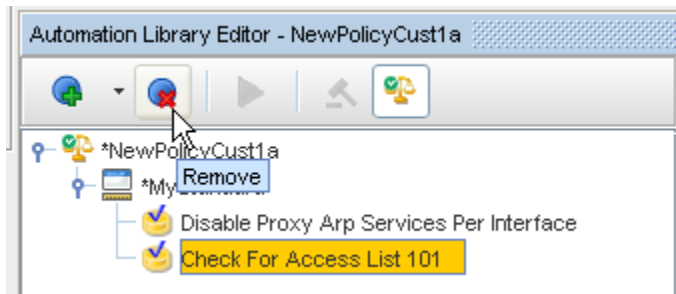
- 3 You can also add an **Attribute Query**. Once that option is selected, the Add Attribute Query window opens. Make a selection for the test you want to edit, then enter in a new **Query Name** . Click **Ok**.



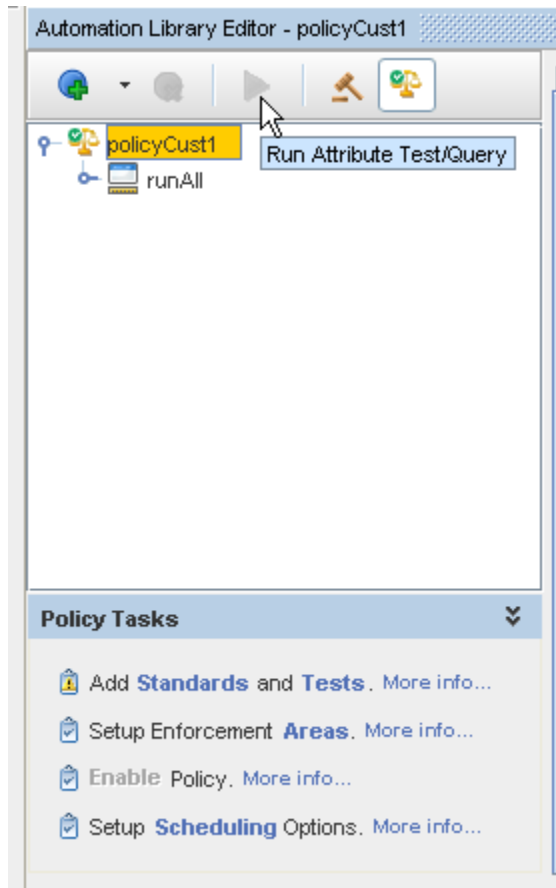
### Remove items in the tree

You can use the **Remove** icon to remove any item you have in the navigation tree.

- 1 Highlight the Standard, Test, or Query you want to remove from the list.
- 2 Click **Remove**.



### Run Attribute Test/Query



With this feature, you can run a Query or a Test and then preview the results. This utility is also made available in the Policy Editor. The Run Attributed Test/Query button (located in the tool bar) is enabled when an Attribute test or query is selected. When selected, this action runs the item selected (test or query) and displays the results in a separate view. Note that like the case of the attribute test and query editors, the results correspond to the latest, unsaved modifications.

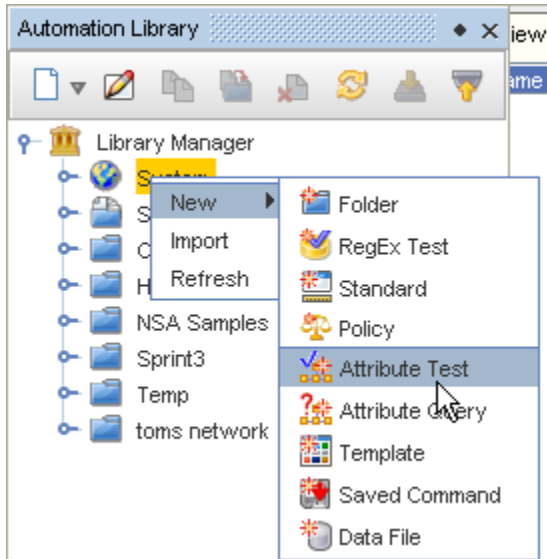
[Adding Standards and Tests - Using Policy Tasks](#)

## Working with an Attributed Test

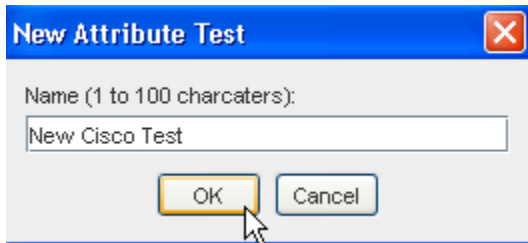
### Creating a New Attributed Test

Building or creating a new test allows you to customize your own compliance .

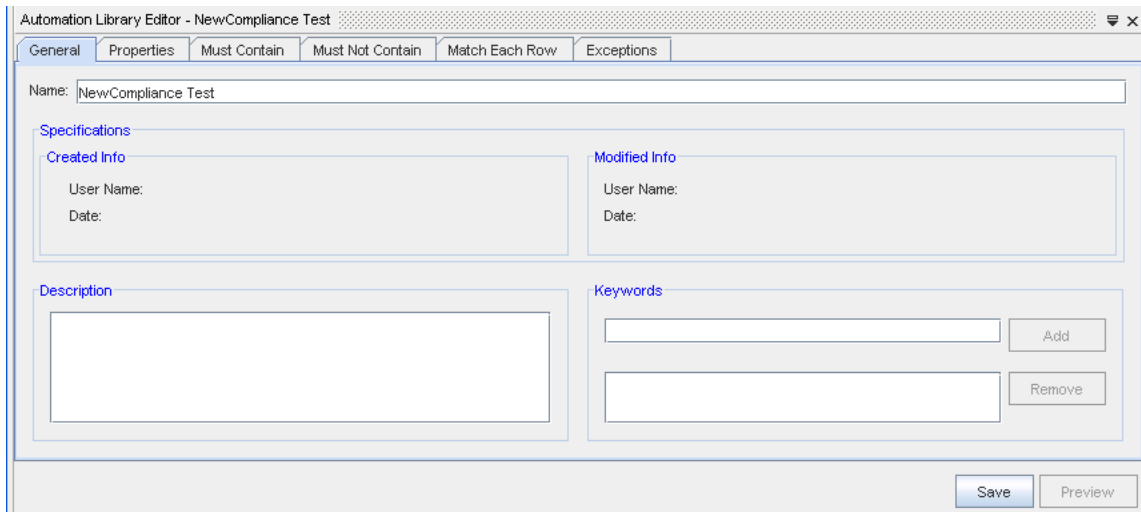
- 1 To create a new Attribute Test, you must first select the **Automation Library**.
- 2 When the Library Manager opens, right-click on **System** (or a folder name), then select **New** -> **Attributed Test**.



3 From the New Attribute Test window, enter a **name** for the new test, then click **Ok**.



The Automation Library Editor for the new attributed test opens.



- The **Name** field is the name of the test; if updated here, it is saved with the updated name (if the Save button is clicked).
- The **Description** field serves as a description of what the test is testing, as well as any special design notes about how the test functions. It is available to the Audit Trail when the compliance test is executed.

- The **Keywords** field allows you to save one or more keywords that can be used to locate the test.

The properties tab contains general properties of the test.

The screenshot shows a software window titled "Automation Library Editor - NewCompliance Test". It has several tabs: "General", "Properties" (which is active), "Must Contain", "Must Not Contain", "Match Each Row", and "Exceptions". Under the "Properties" tab, there is a "Severity" dropdown menu currently set to "INFORMATION". Below that is a large text area for "Failure Description". At the bottom, there are three checkboxes: "Must Contain Exact Match", "Must Contain Ordered Match", and "Must Contain Replicate On" (which has a dropdown arrow). At the very bottom right of the window are "Save" and "Preview" buttons.

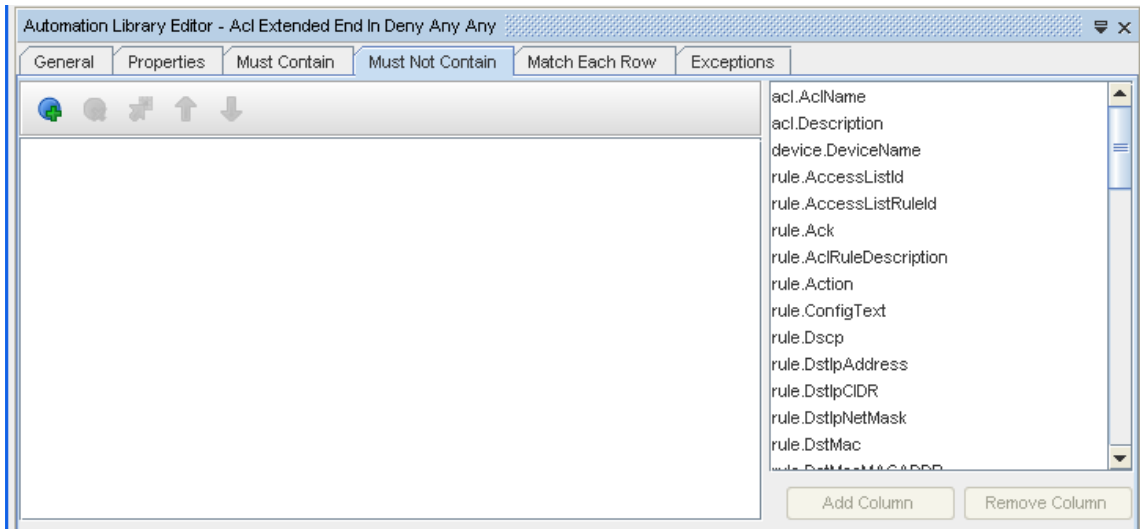
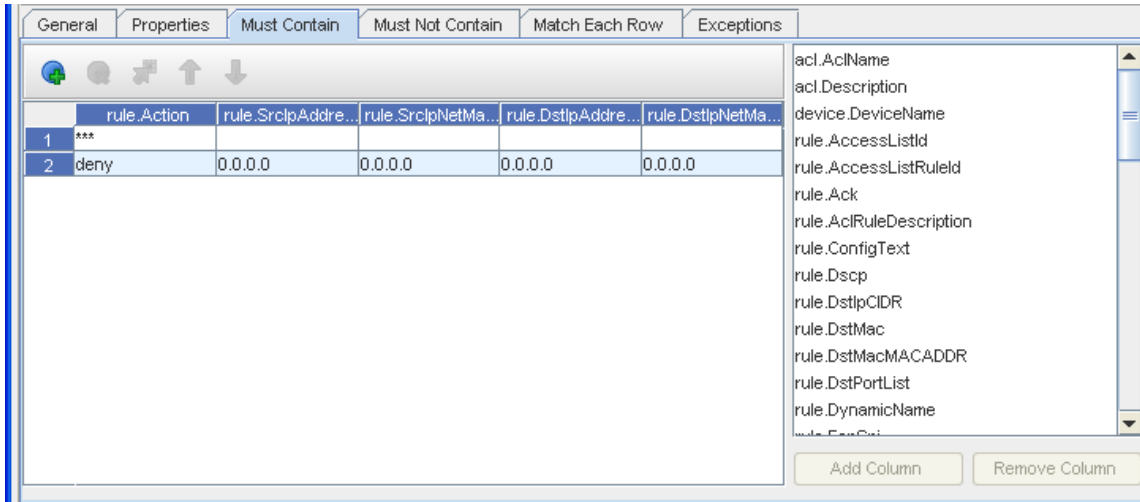
- The **Severity** drop-down fields indicate the severity of a test failure; this is rolled up into compliance and auditing reports.
  - The **Failure Description** field serves as a description of what it means when the test fails. This field should describe the nature of the failure, and what corrective action needs to be taken. The Failure Description is rolled up to compliance and auditing reports.
  - The **Must Contain Exact Match** check box applies only to the Must Contain Rules; if checked, the rules must match exactly the rows in the Primary Result Set. No additional rows are allowed in the Primary Result Set that do not appear in the Must Contain rules. If not checked, additional rows by the Must Contain rules are allowed.
  - The **Must Contain Ordered Match** check box applies only to the Must Contain Rules; if checked, the rules are matched against the Primary Result Set, in order; that is the rules and rows in the result set must appear in the **same order**.
  - The **Must Contain Replicate On** field drop-down options contain the aliases from the primary Query. If an alias is selected, the Must Contain rule set is applied repeatedly, each time the object referred to by the alias changes (as determined by a change in the primary key of the table the alias refers to).
- 4 From the drop-down arrow, select a **Severity**.
  - 5 Enter a **Failure Description** if needed.
  - 6 Select the appropriate **Must Contain** check box, then click within the appropriate **check box**.
  - 7 If appropriate, click the **Must Contain Replicate On** drop-down arrow, and make a selection from the options.

---

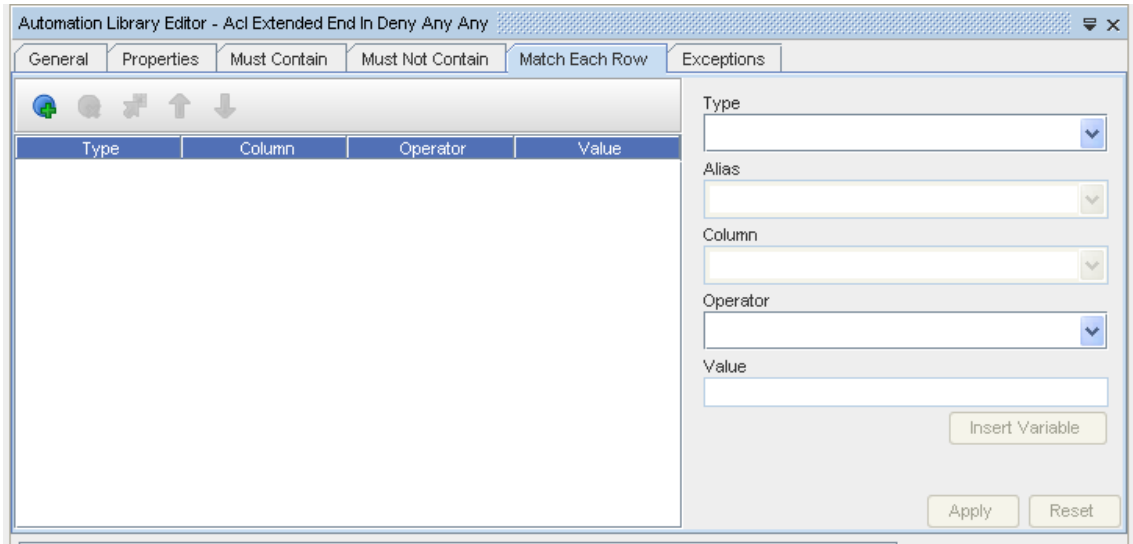
**Note** You must **Save** the empty test before you are allowed to add any queries to it.

---

Now, use the Must Contain, Must Not Contain, or the Match Each Row tab to insert your parameters. See the following examples.











8 Click **Apply** or **Save**. Your test is now customized and can be linked.

At the General tab,

At the Properties tab,

### Icons

Icon	Description
	Used to Remove a row in the listing.
	Used to Insert an additional line.
	Used to Move the selected item in the list up or down within the list.
	Used to Add a row in the left section of the window.

### Must Contain

### Must Not Contain

### Match Each Row

**Note** Note the **Exceptions tab** is used to detail any exceptions to the rules you have previously entered.

### Linking Tests to Standards

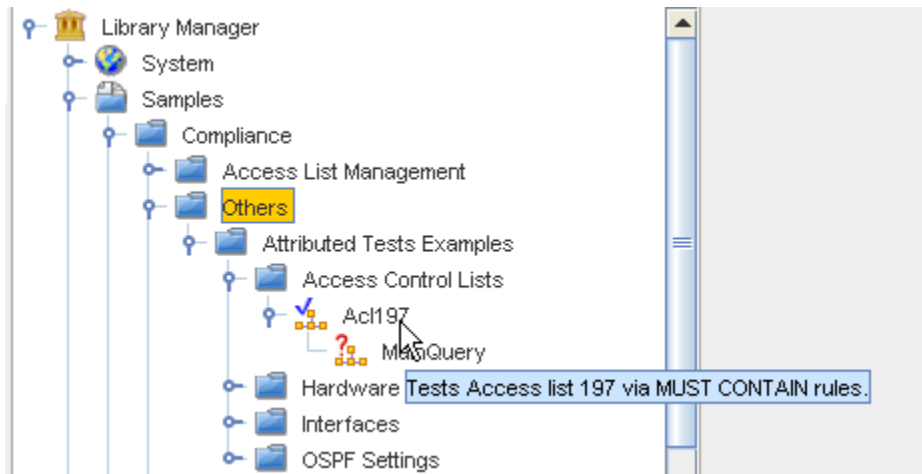
For a Test to be linked to a Standard, the Test must be defined **before** it is shown as available for linking to a Standard.

### Customizing an Existing Attributed Test

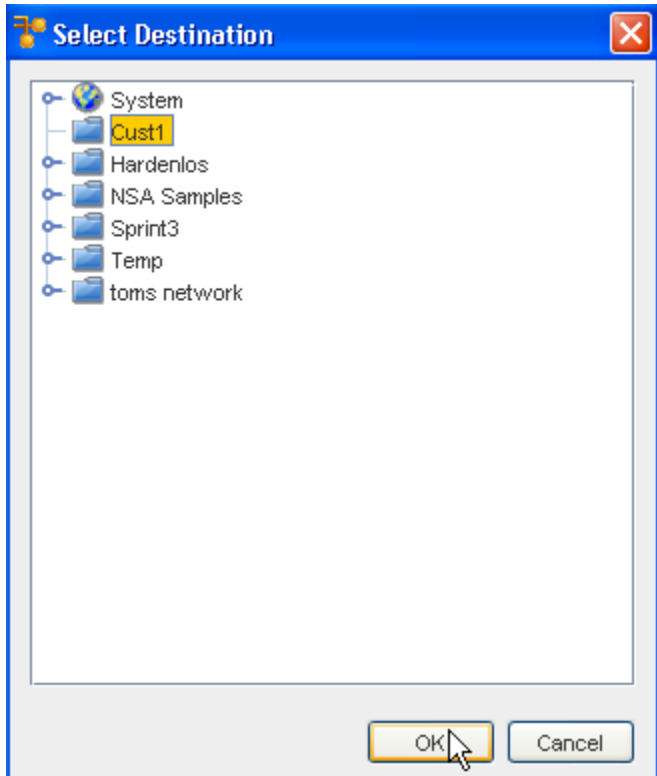
To edit (customize) an existing Attributed test, you must first locate the test you want to edit.

To view the Library Manager navigation tree, select **Automation Library** from **Tools** on the menu bar.

- 1 Click the **Library Manager**, and expand the view to show the **System**, and the listing of Networks within your application.
- 2 Click **Samples**, **Compliance**, then click **Others**.
- 3 Click the **Attributed Tests Examples** category.
- 4 Once the category is opened, select an **Attributed Test** from the list of examples.
- 5 Right-click the example, and select **Copy** from the options.

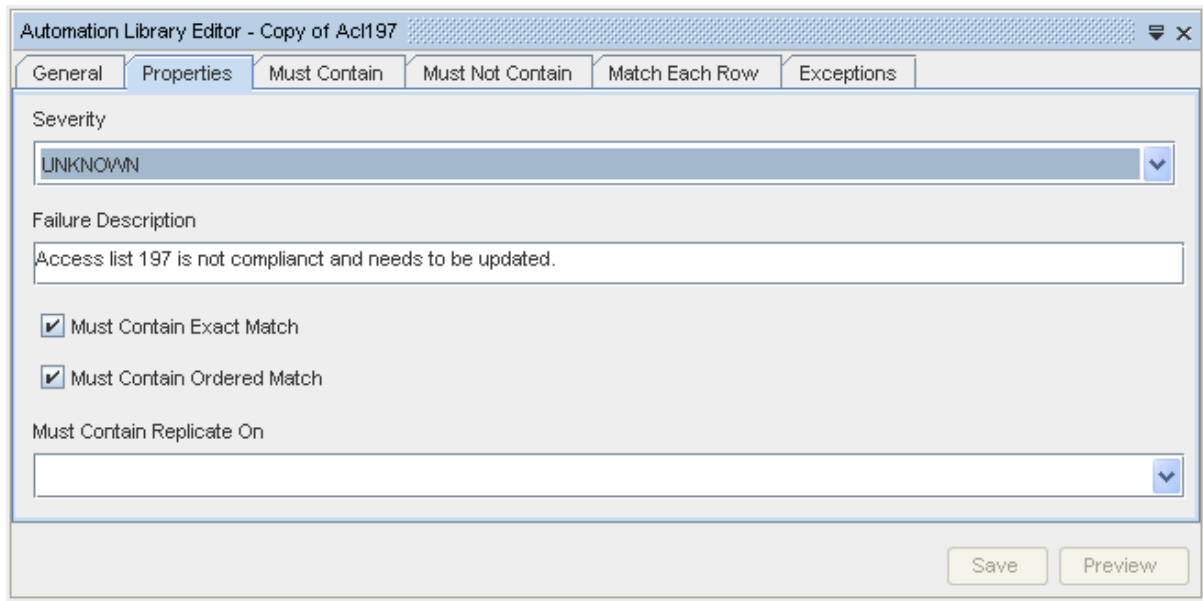


- 6 Select a location to copy to the test to, then click **OK**.



The test you selected is now displayed in the destination you selected.

- 7 Right-click the test name, then select **Edit** from the options.
- 8 The Editor is now open, where you can go through each of the tabs, and either add to, change, or delete the existing information.



See [Creating a New Attributed Test](#) for additional information.

- 9 Once you have made all your edits to this existing test - to make it customized - click **Save** to save all your changes, then close the editor.
- 10 To Run the test, double-click on the test name. The test results are displayed.

## Working with Queries

### Introducing Queries

Network Configuration Manager offers a set of pre-defined queries accessible from the Automation Library navigation tree. **Queries are like reports** displayed in a spreadsheet-like fashion.

Each Query that is pre-define by Network Configuration Manager **contains device information** . These pre-defined queries can be quickly and easily displayed to view device information based on various criteria selections.

Once you have reviewed the established, pre-defined queries, you may want to use a query for a template in creating your own customized query, to view specific device information.

What you should first know is the information (or Metadata) that resides in each query. There are several ways to review the information that is contained within each query. Go to **Sample Queries** section to review the contents of each query. You can also go to the [Metadata Information](#) section in Network Configuration Manager to review the available information. See [Metadata](#) for more information.

This Query feature does not replace the textual, configuration-based, model of Devices with Network Configuration Manager. Rather, this feature is an extension to the existing feature. This new Queries feature provides an easy way to look-up and combine information in a Device class-independent manner.

---

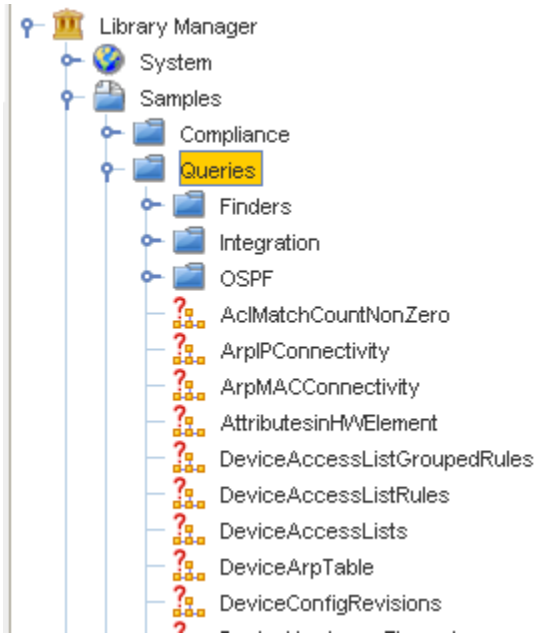
**Note** Not all Devices are supported. The most frequently used device attributes on the **most common devices** are supported. Even within a supported Device, certain facilities may not be provided. For example, a switch may not implement OSPF Protocol settings.

---

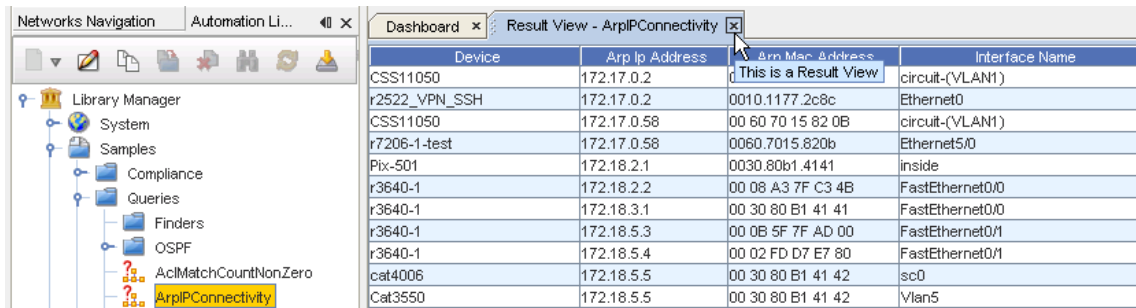
- 1 To view the Library Manager navigation tree, select **Automation Library** from **Tools** on the menu bar.
- 2 Click the **Library Manager** and expand the view to show the **System** and **Samples** , and the listing of Networks within your application.
- 3 Click **Samples**, then **Queries**.

Note that there are three different types of queries.

- **Finders** does just that - finds objects of a particular type, searched for by a particular criteria
- **Integration** - reveals results on the Interfaces, Credentials, and Device Lists
- **OSPF** - shows results for the routing protocols



4 From here, select a **Query**, and double-click on the **Query** to view the Query Results.



### Some things you should know about viewing information in Queries

- Right-clicking in a **column heading** displays the Select Display Column where you can add or delete column headings from the query.
- Right-clicking on an **item in a column** displays a list of links to go to for additional query information.

### Query Concepts

Even though Network Configuration Manager offers a great number of pre-defined queries, the real power of the Attributed Model (AM) is in the ability of users to formulate their own **customized queries**.

Queries are defined by completing various tabs within the **Query Form** . Query Forms are now used to create Policies, Standards, and Tests.

To create or build your own **query**, some database concepts must first be understood.

**Tables** are used to hold Objects and to express **relationships between Objects** . A table is essentially a row-column view of arbitrary data, like the Result Set or Result Views.

Tables contain **key values** that allow you to find a particular record. There are two types of keys:

- Absolute
- Relative

**Absolute keys** - identify a **single row** (record) within a table; therefore an absolute key has a unique value for each row within the table.

**Relative keys** - identify a **unique value**, but only in the context of an Object containing the objects in the table. For example, InterfaceName is a relative key, because in the context of a single Device, there can be only one Interface with a given name.

The AM uses **four** types of Absolute Keys:

- **OIDs** - (stands for Object IDentifier). OIDs are generated by Network Configuration Manager, and are used in almost all of the existing tables. These are 32-byte binary values. OID keys are almost always named "XXXOid" where XXX is the name of the Object class.
- **IDs** (or Long identifiers) - Long Identifiers were introduced as part of the AM. The Long identifiers are a Long integer, generated by the database itself when the record containing the key is first written to the database. Long ID keys are usually named "XXXId" where XXX is the name of the Object class.
- **Device IDX keys** - These are integer keys, provided by Device Services, that uniquely identify a device. Device IDX values are used in logs generated by Device Services. This key is named "Deviceldx".
- **RDN** – which is an acronym for Relatively Distinguished Name. This is a relative key, used within Device Services to distinguish one attribute from another in the AM. RDN keys are not used by the Application Server. RDNs can be viewed to aid debugging.

You do not normally have to be concerned with keys, other than to recognize them. Most queries make keys initially not visible. It is possible, however, to construct queries based on a specific key.

Keys are often used to relate entries in one table to another. For example, AclExtendedRule contains a relative key, the RuleNumber, and a reference to the absolute key of the AccessList that contains it (which is AccessListId). The AccessList entries in turn, contain Deviceld keys, which identify the Device they belong to.

Queries can be built without referring specifically to the keys needed to relate tables. Instead, the Query references the Navigation by name, which specifies how two (or often more) tables are related.

These are the same Navigations as shown in [Introducing the Data Model](#).

Navigations often express relationships, for example the Device query contains AccessList, which contains AclExtendedRule. Going in reverse order, AclExtendedRule is contained in AccessList, which is contained in Device.

There is also an implicit references relationship, such as InterfaceAccessList references AccessList.

Tables consist of columns, which contain the attributes associated with the Objects represented by the Table. Columns contain typed data, such as Strings, Integers, Longs, IpAddresses, or binary data.

The Query Forms allow selection of the columns to display in the result set, or the ability to match values in one or more columns, to select one or more rows from the table.

### Running Pre-Defined Sample Queries

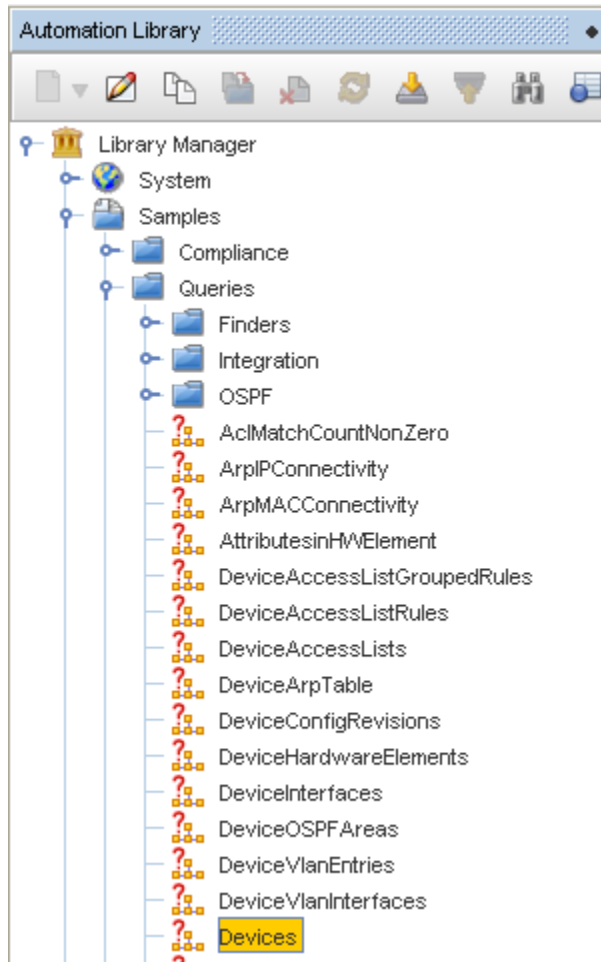
Shown in the following graphic is the Automation Library navigation tree, with a specific Sample Query (Device By Name) selected, and a sample **Query Result** on the right.

The Query Results are shown in a tab labeled **Result View** (and includes the Query name). Think of a result view as similar to a spreadsheet page.

- The first row is a set of column headers that are constructed from the DisplayNames of each attribute returned in the Query.
- The remaining rows in the result view show data returned by the Query. Each row may have data from one or more objects in the model.

As shown, the Queries folder contains a sub-folder named **Finders**, which is expanded to show a great many Queries that are shipped as examples with Network Configuration Manager.

Each of the **Finder** queries finds objects of a particular type, searched for by a particular criteria.



For example, the highlighted Query is **Device**, which allows you to search for Devices based on their Device attribute.

Device Name	Management Ip	Device Idx	Type	Vendor	Model	Status	Out Of Sync	Device
10.6.224.81	10.6.224.81	1004	Router	CISCO		Operational	false	Cisco IOS I
3640-RSA2	192.168.10.3	1007	Router	CISCO	3640	Operational	false	Cisco IOS I
3640-RSA3	192.168.10.4	1006	Router	CISCO	3640	Operational	false	Cisco IOS I
3640-RSA4	192.168.10.5	1008	Router	CISCO	3640	Operational	false	Cisco IOS I
Cust1-GW	10.6.224.193	1003	Router	CISCO	7206	Operational	false	Cisco IOS I
cat-3524	10.6.224.66	1002	Switch	CISCO	WS-C3524-XL-EN	Operational	false	Cisco IOS :
ciscoasa	10.6.224.71	1005	Firewall	CISCO	ASA5510	Operational	false	Cisco PIX
r3640-1	10.6.224.194	1001	Router	CISCO	3640	Operational	false	Cisco IOS I

You can run a Query (shown in the Automation Library tree) by double-clicking the Query name. Some Queries run immediately and display their results, which are shown in a Result View. Other Queries may prompt for one or more input parameters that limit their results.

The **Finder** Queries all prompt for an **input parameter** which can generally be identified from their name (such as Device By Name, will prompt for the Device Name).



When a Finder prompts for a name or other string, it can generally be supplied as a **partial regular expression**. For example, to find all the Devices that contain the characters **dev**, enter that string for the parameter, and press Enter.

Alternately, to see **all the Devices**, press **ENTER** at the prompt, without supplying any input.

In more formal terms, a selection is applied to the Query based on the entered text. If text represents the text that is entered, a selection is performed according to the regular expression **\*text.\***, which will match the input regular expression with arbitrary characters in preceding it, or succeeding it.

Some Finder Queries prompt for an IP address instead (these are typically named "- by Subnet Containing IP".)

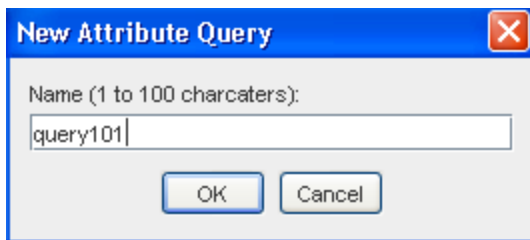
---

**Note** Note that all the samples contained in the Automation Library Samples folder are **read-only**, and cannot be modified. They are applied **globally to all Devices** in the system (regardless of which Networks they belong to).

---

### Creating a New Attribute Query

- 1 To create a new Query, you must first select the **Automation Library** .
- 2 When the Library Manager opens, right-click on **System** (or a folder name), then select **New -> Attribute Query**.
- 3 From the New Attribute Query window, enter a **name** for the new test, then click **Ok**. The Automation Library Editor opens.



The Tables tab is now opened and active.

Tables Tab,

The error message (located at the bottom left) warns that you must have at least **one** table specified.

---

**Note** Tables are objects or object classes; the Alias is the **variable name** for the object class.

---

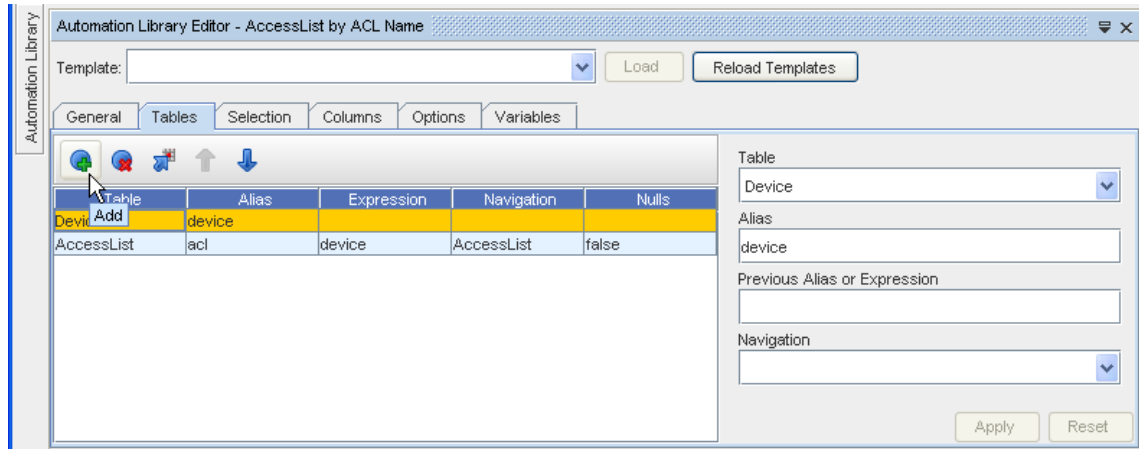

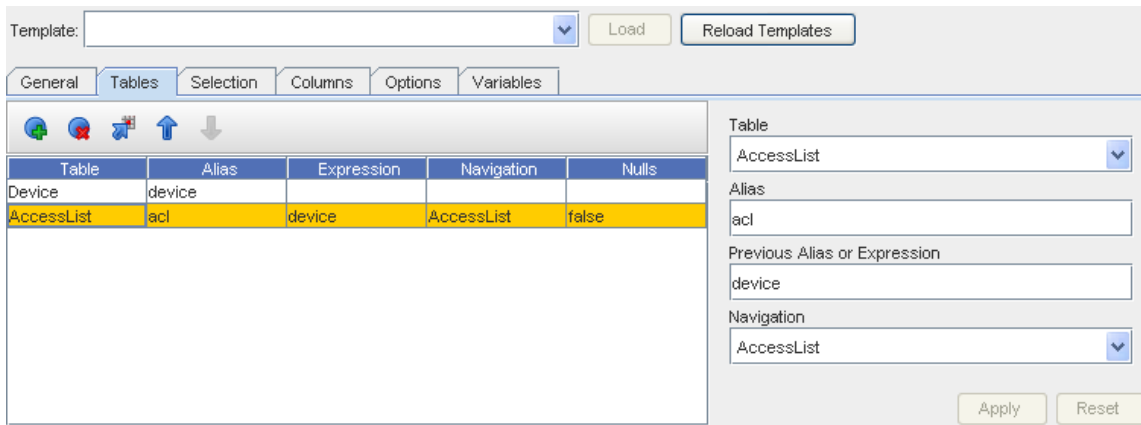


Table tool bar

Following are the icons available on the Tables tab

- 1 Click **Add**  to add a table. At the Table section, click the drop-down arrow to view the listing of tables.
- 2 Make a selection from the list of tables to be specified in the **Query**.



- 3 Notice that when you select a table (in this case **ArpEntry**), the Alias is already created, and populates the Alias field. However, you can assign your own alias.

Table  
 AccessList

Alias  
 acl

Previous Alias or Expression  
 device

Navigation  
 AccessList

**Note** The Allow Nulls check box includes rows in the result set, even if there are no entries in the current table that correspond to entries in the previous table it was joined to. You cannot execute the query until one or more columns are specified to be in the result set. The red error message at the bottom of the editor is informing you of this.

- 4 Click **Apply**, and go on to the next tab.

Selection tab,

Items selected from this tab represent the information to be retrieved. If the Query is executed without adding a selection clause, it displays the Access List Extended Rules for every Device in the system.


Template: [ ] Load Reload Templates

General Tables Selection Columns Options Variables



Type	Column	Operator	Value
	acl.AclName	CONTAINS	\${name}



Type [ ]  
 Alias [ ]  
 Column [ ]  
 Operator [ ]

Apply Reset

- 1 Click **Add** , then go through the drop-down options for **Type**, **Alias**, **Column**, **Operator** and **Value**, and make your selections.
- 2 Click **Apply** when you have made all your selections.

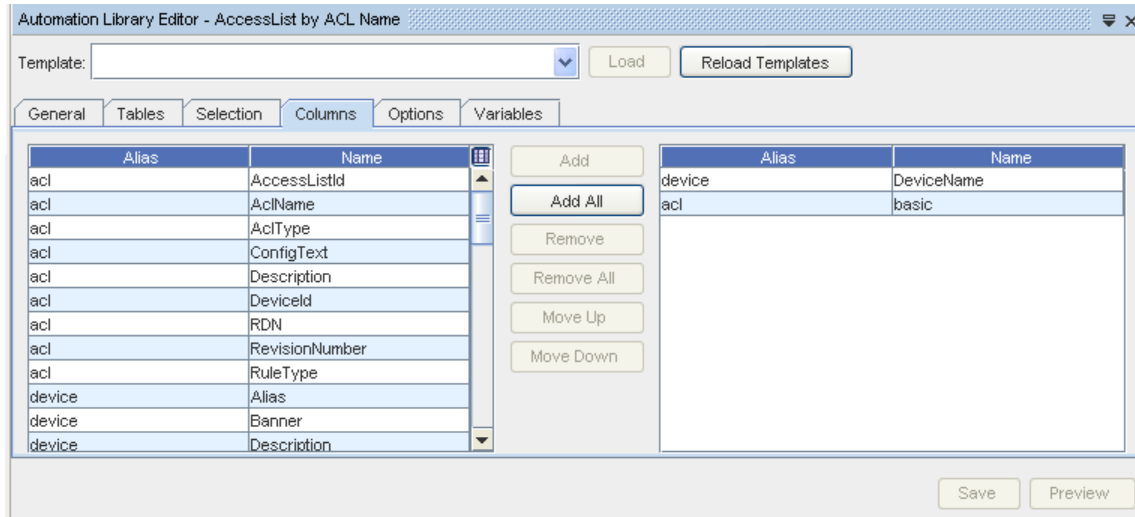
Selection tool bar

Icon	Description
	Used to Add a row in the left section of the window
	Used to Remove a row in the listing

Icon	Description
	Used to Insert an additional line
	Used to Move the selected item in the list up or down within the list

Column tab,

Use the columns tab to specify which columns should appear in your Result View.



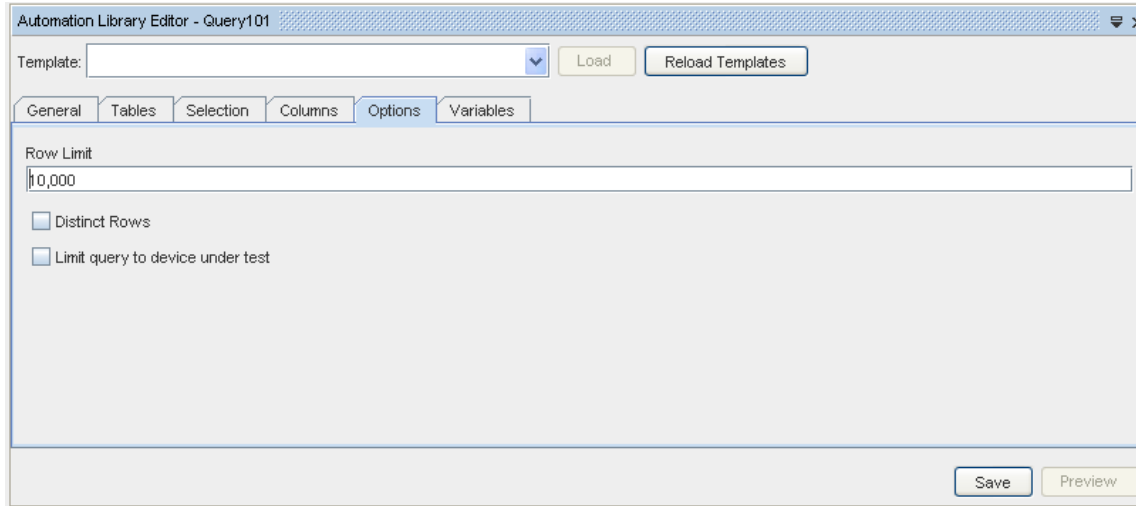
- 1 At the **Columns** tab, you have a selection of columns that can be added to the Query. These columns represent what is returned in the query results, in other words, all the properties within a device. A quick way to include all the device properties is to select **basic** from the columns listing. Once selected, click **Add** or **Add All** to add your selections.
- 2 Click **Save**, and then click **Preview** to preview your Query Results. Select the Preview button to look at the results of the query, which is displayed as a new Result View.

Options tab,

The options tab has some miscellaneous fields that control behavior of the query execution.

The **Row Limit** field sets an upper bound on the number of result set rows that the Network Configuration Manager server will return. The default value when a new query is created is 10,000, which means the server will return a maximum of 10,000 rows of data in a Query Result.

This limit is imposed to limit the maximum amount time and/or memory the Query can take. In exceptional cases, you may need to lower the Row Limit (if the Query can take large amounts of time), or increase the Row Limit (if you need to see more than 10,000 rows in the Result Set.) If a Query generates more than Row Limit rows, only the first Row Limit rows will be returned and a warning message appears indicating Row Limit was hit.







1 This section contains **Row Limit** information. Generally, the default is acceptable. If not, you can make other changes.

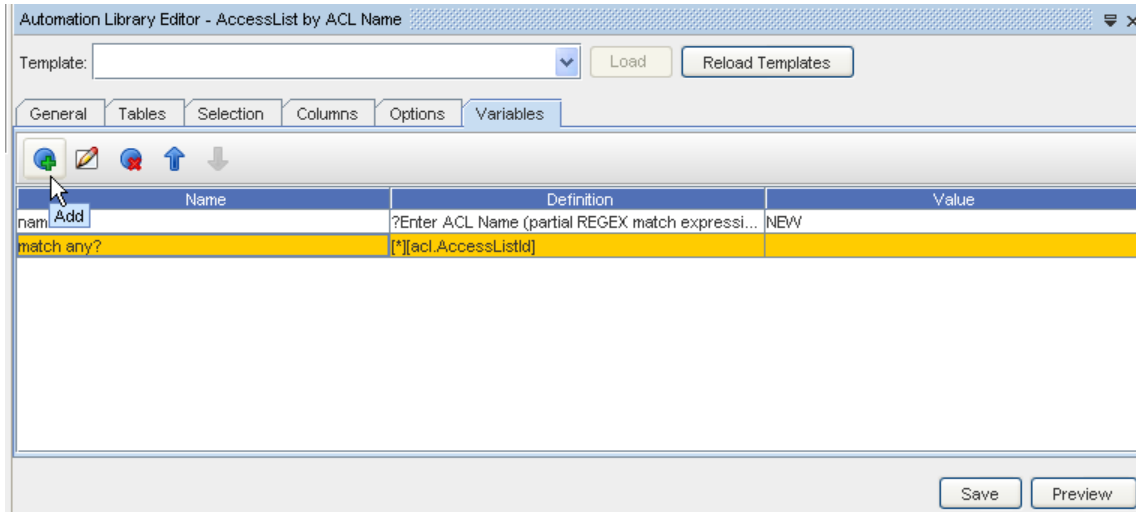
2 Click **Save** to keep the default, or to keep your changes.

Variables tab,

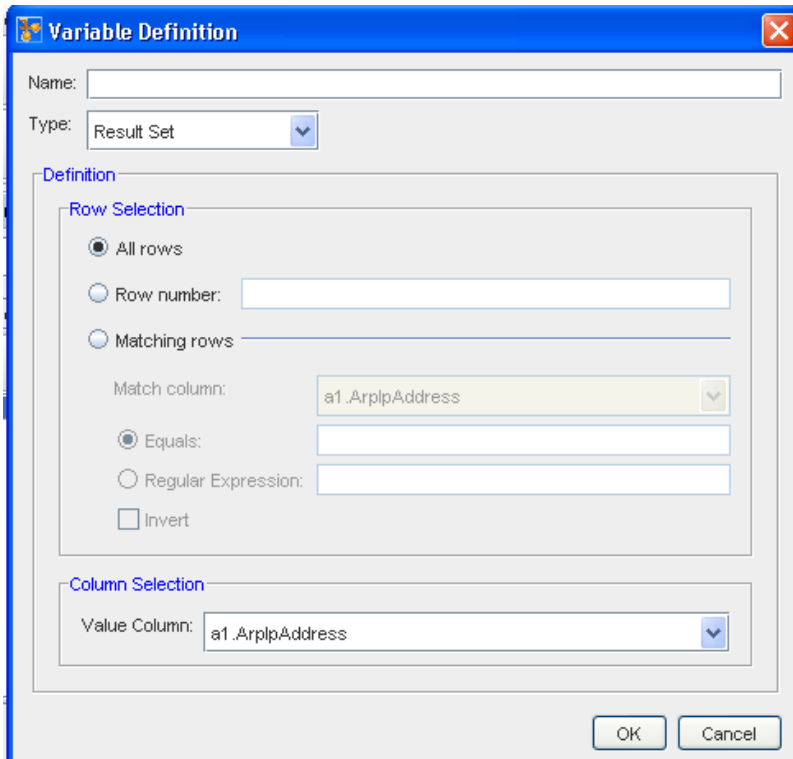
The Variables tab allows you to define Variables that are required as input to the query, or computed from the query's result set after it has executed. These Variables can be used in Attributed Compliance Test rules, or as part of a query's selection criteria. Any values supplied as input with the query are initialized before the query is executed. The remaining values are calculated just after the Query is processed, and the Result Set is generated.

Variables tool bar

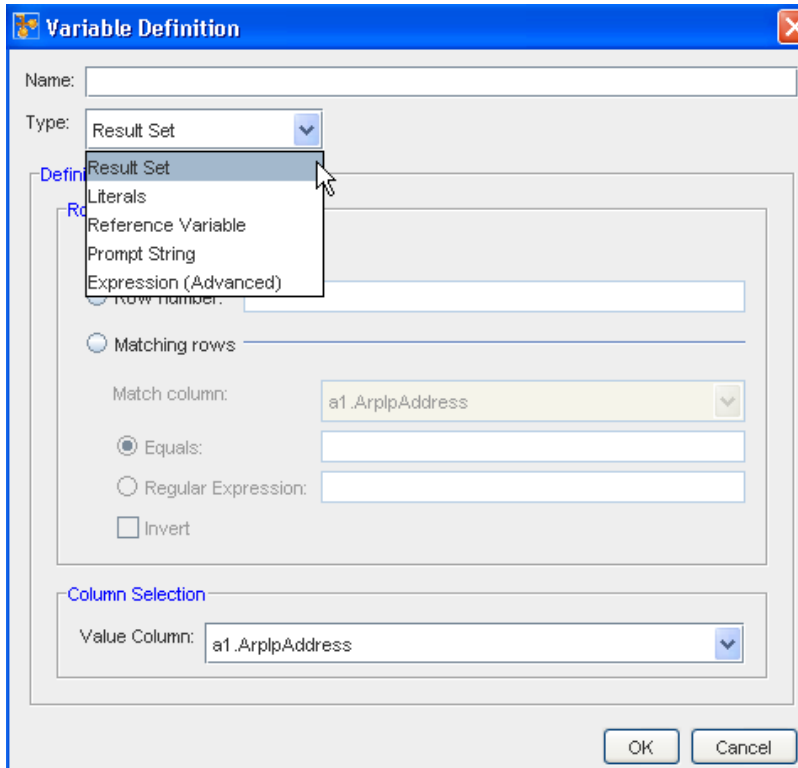
Icon	Description
	Used to Add a row in the left section of the window
	Used to Edit existing information
	Used to Remove a row in the listing
	Used to Move the selected item in the list up or down within the list




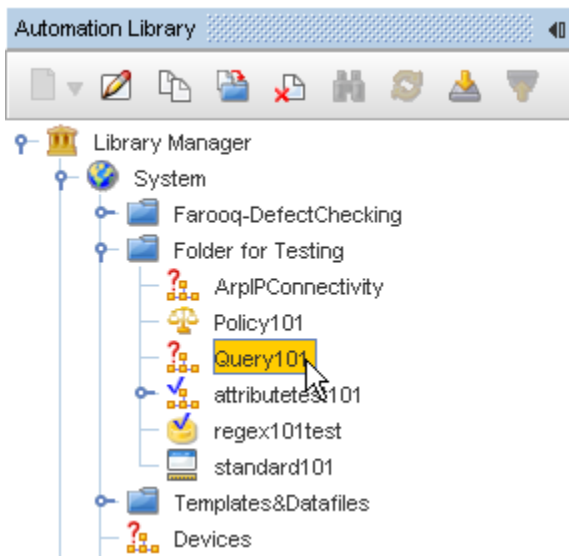
- 1 Click **Add**  to display the Variable Definition window.



- 2 Enter a **Name** for the definition.
- 3 From the drop-down arrow, make a **Type** selection.



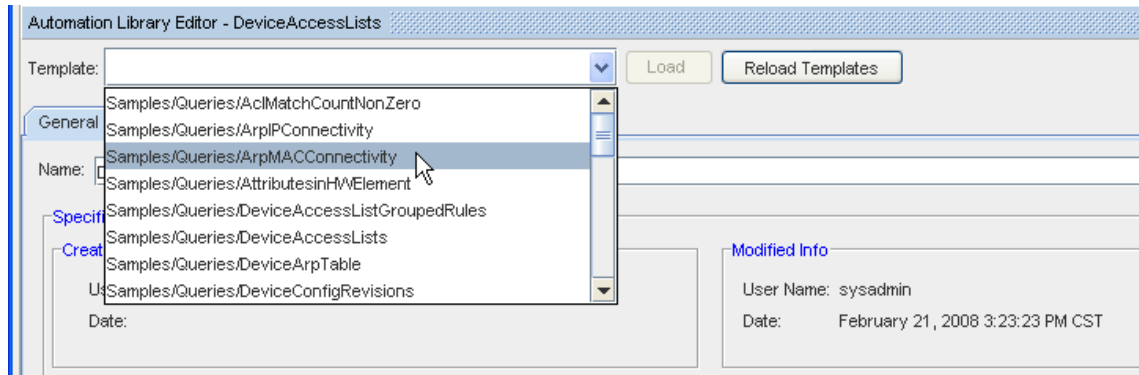
- 4 Based on your **Type** selection, this window changes to accommodate the selection. Complete making your selections on this window, including the **Column Selection**, if appropriate.
- 5 Click **Ok** when you have made all your Variable Definition selections.
- 6 Click **Preview** to see the Results of the selections in this tab.
- 7 Now, click **Save** to save all your selections for this Query, and then **Close**  the Automation Library Query editor. Your Query is now in the folder in System.



**Customizing a Query - based on an Existing Query**

To build your own customized Query, **based on an existing Query** , the Template mechanism in the **General** tab provides a convenient way to do this.

- 1 Click the **Template** pull-down menu in the General Tab. A list of available Query templates display.
- 2 Select the desired template, and then select the **Load** button.



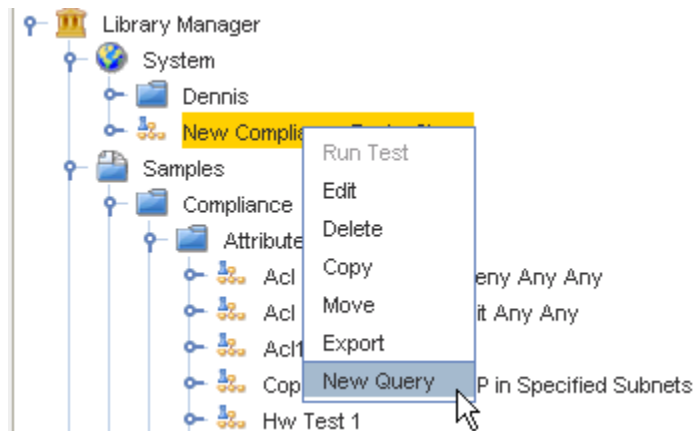
Doing these two steps erases any existing Query definition in the Editor, and replaces it with a copy of the templates Editor (except for the new Query name you must enter). See [Creating a New Attribute Query](#).

### Creating a Primary Query

**Important** You must save the empty Compliance Test before you are allowed to add any queries.

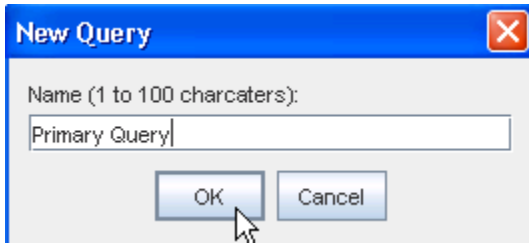
The Primary Query must be created **before** any additional Queries are created.

To create the Primary Query,

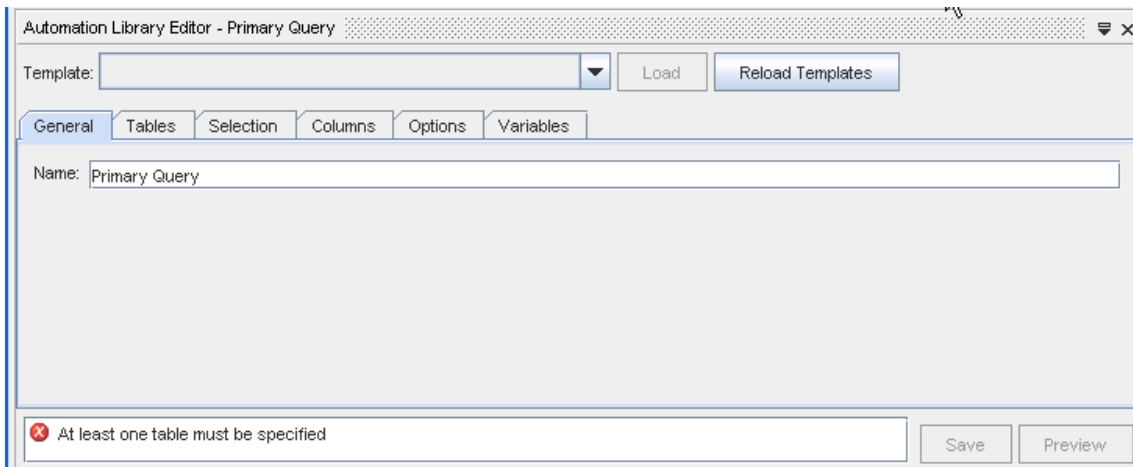
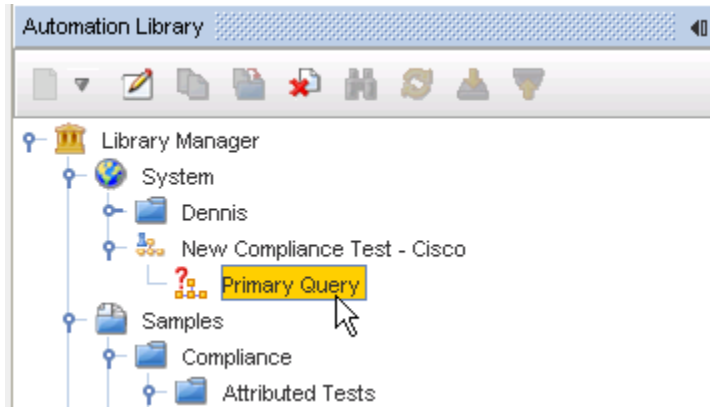


- 1 From the test, right-click then select **New Query** from the list of options.
- 2 At the New Query window, enter a **name for the query**. In this example, Primary Query is used for the name. Click **Ok** after entering the name.





The new Primary Query test is now in the Library Manager listing, and the Editor form opens.



### Rules when creating a new query:

**Note** There are certain rules that the Primary Query must obey in its construction.

- The first table must be "Device". Compliance tests are run against a single Device, which is the first table entry. A selection clause is automatically be added to select the Device being tested by one of it's primary keys.
- The columns selected must include all the columns that are referenced in the compliance test rules.
- You may want to supply appropriate Selection criteria. For example, if you intend to test a specific Access List's rules, you must add a selection criteria that selects only the desired Access List.

- It is possible to use a **Primary Query** that joins attributes between multiple Devices, provided the Device being tested is listed as the first table in the join list.
- The Primary Query must not have a selection clause for the Device to be tested; instead such a selection is implicitly added when Network Configuration Manager executes the test as a result of revision processing, or a user requested auditing.
- The compliance engine adds additional columns to the Query (e.g. keys of the objects in the result set) to facilitate the identification and generating of remedies. You should recognize that remedy actions are only generated against the Device being tested.

To continue creating a Primary Query, go to [Creating a New Attribute Query](#) and follow the steps outlined in that procedure.

### Viewing Query Results

Once a query is selected, the results of the query are displayed. The information is rendered in a spreadsheet-like view called a Result View. The rows within the table represent Objects, and the columns represent Attributes of those Objects. Each cell represents a particular attribute value for a particular object.

Each time a different query is selected, the query name displays as a tab (in a Results View), allowing you to move from one view of selected information to another view if needed. This way, you display and work with several groupings of data at one time. These tabs remain open until you select to close them by clicking the small x in the upper right corner.

In this example, the **Network**, **Attributes in Hardware Element**, and the **Devices** queries were all selected individually from the Queries listing, and are all being displayed.

**Note** The red columns in the Devices query view indicates a validation error.

Result View - Networks		Result View - Attributes in HWElement				Result View - Devices			
Device...	Device...	Vendor	Manag...	LastRevi...	LastCommS...	Status	OsDe...	Devic...	De
172.22...	1030	NORTEL	172.22...		2007-08-15 ...	Operational	3.1.4...	Nortel ...	Bus
172.23...	1055	Cisco	172.23...		2007-08-21 ...	Operational		Cisco I...	
172.23...	1056	Cisco	172.23...		2007-08-21 ...	Operational		Cisco I...	
172.23...	1057	Cisco	172.23...		2007-08-21 ...	Operational		Cisco I...	
350t	1035	NORTEL	172.22...		2007-08-15 ...	Operational	1.3.2.2	Nortel ...	Bay
ASN-1-...	1024	NORTEL	172.22...		2007-08-15 ...	Operational	15.4.2.0	Nortel ...	Ima
Adtran...	1036	ADTRAN	172.22...		2007-08-15 ...	Operational	06.01...	Adtran...	Net
BIGGlo...	1029	FOUND...	172.22...		2007-08-15 ...	Operational	06.5.1...	Foundry	Fou
C7200-...	1060	CISCO	172.17...		2007-08-21 ...	Operational	12.2(...	Cisco I...	Cis
CSS11...	1041	CISCO	172.22...		2007-08-15 ...	Operational	Conte...	Cisco ...	Cor
Cat190...	1025	CISCO	172.22...		2007-08-15 ...	Operational	Cisco ...	Cisco ...	Cis
Cat6500	1006	CISCO	172.17...		2007-08-16 ...	Operational	8.6(1)	Cisco ...	Cis

### Working with Templates

#### Best Practices when using Templates

Best Practices are recommend methods of completing tasks or tips that should be used, based on a typical scenario.

- Templates are used for new deployments and mass change, but not for ongoing policy changes in the network
- A template should be constructed from a contextual subsection of a config
- Primary templates should contain all contextual templates needed to construct a "gold standard" config
- A compliance audit for a contextual template is constructed from one or more tests.

### Additional Template Information

Network Configuration Manager allows you to create and save reusable configuration commands (known as templates). These templates can be as small as a single config line, or as large as a complete configuration file.

When creating a template you can designate **variables** in which the user can supply a value (for example, password, IP address, DLCI, host name, or community string). These variables can be of the following types:

- String - allows any alphanumeric character
- Integer - designates that only numbers can be entered in the field
- IPv4 Mask - can be a subnet mask or a wildcard mask
- IPv4 Addresses - can be any valid IP address

You can further define what the user can enter into the variable field using **validation rules**. For example, when creating a variable for a password, you might wish to set a minimum and maximum value for the number of characters allowed.

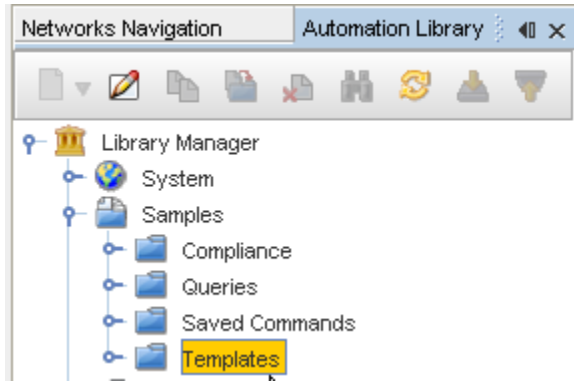
You can create **available values**, which enables the user to select from a predefined list of values. This is useful, for example, when creating a template variable for Management router IP addresses.

There are many benefits to creating variables within your templates, including:

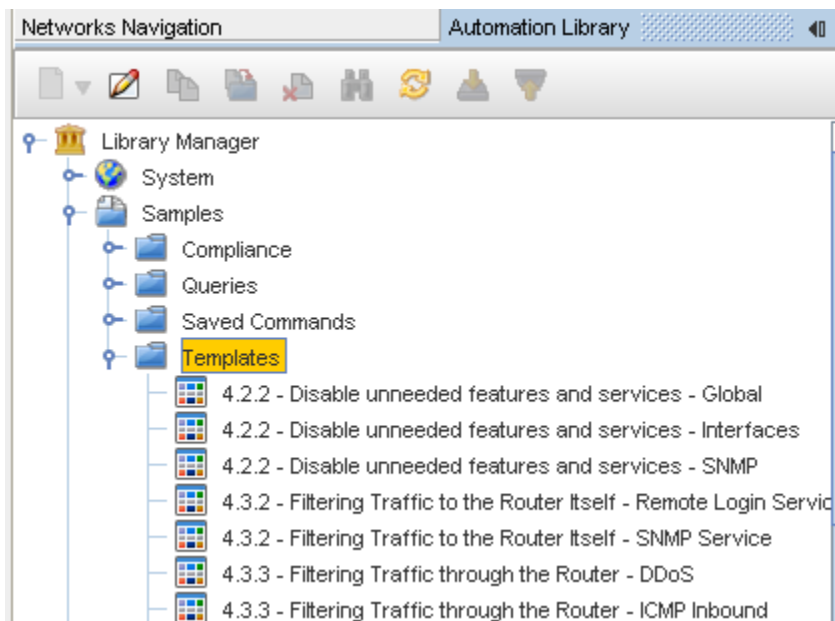
- Reduced errors
- Increased user entry speed through the use of predefined lists
- Flexibility when creating templates

### Accessing Template Samples

You can first think of using Templates by accessing the Pre-defined Templates that are stored in the **Samples** directory.



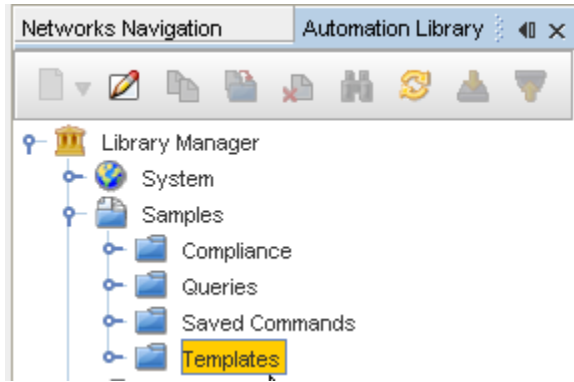
- 1 Once you have accessed the **Templates** folder, expand the folder, and review the number of pre-defined templates.



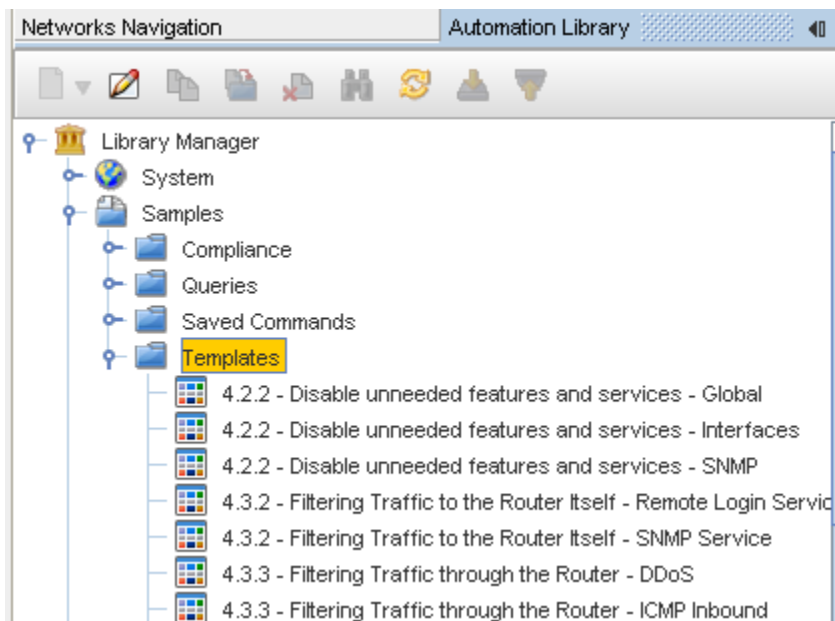
- 2 Move your cursor over each Template to get a description of the contents of the Template.
- 3 Now, select (double-click) from the various templates to review the contents.

### Copying a Pre-defined Template

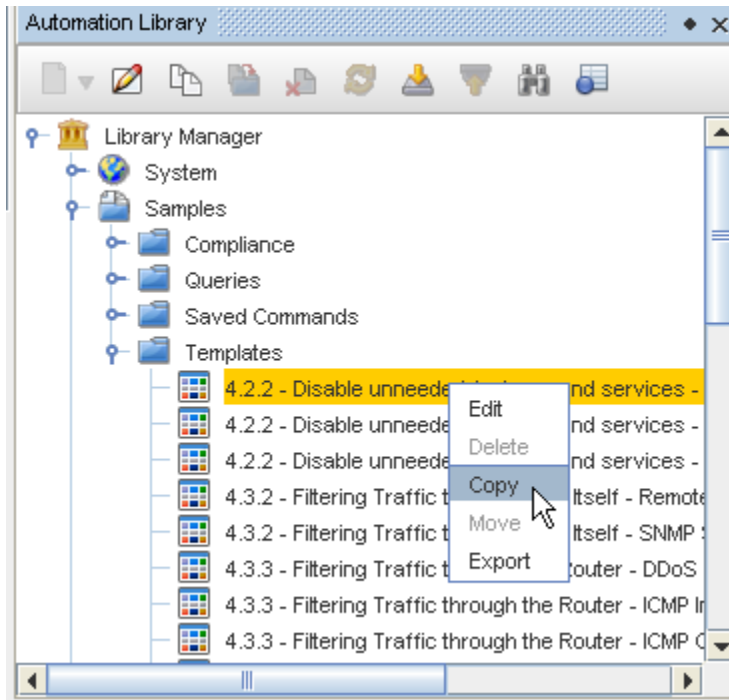
Network Configuration Manager offers a number of Templates that contain pre-defined contents. You can use a pre-defined Template to create a **customized template** .



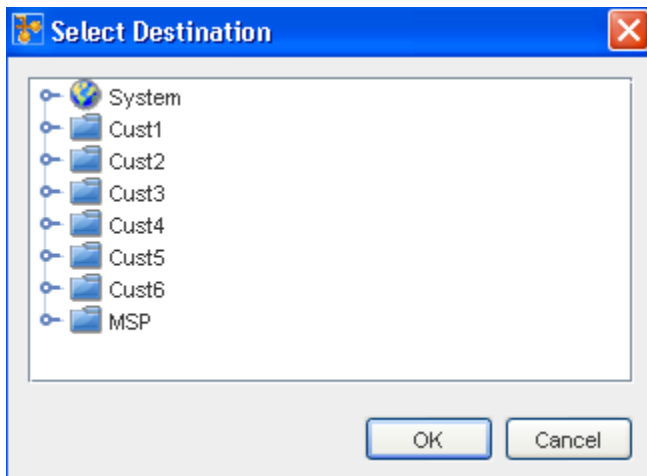
- 1 Once you have accessed the **Templates** folder, expand the folder, and review the number of pre-defined templates.



- 2 Pause your cursor over each Template to get a description of the contents of the Template.
- 3 Now, select the **Template** you want to copy. Once selected, right-click on the Template, then select **Copy**.



- At the **Select Destination** window, select where you want to store this Template. Click **Ok** when you have selected the destination.



- Now, go to the destination where you stored the template to ensure it was successfully stored.

---

**Important** When templates are created that can be used for *more than one network*, but are not suitable for *all networks*, a copy of a template can be created and placed in only those networks where that template can be used.

---

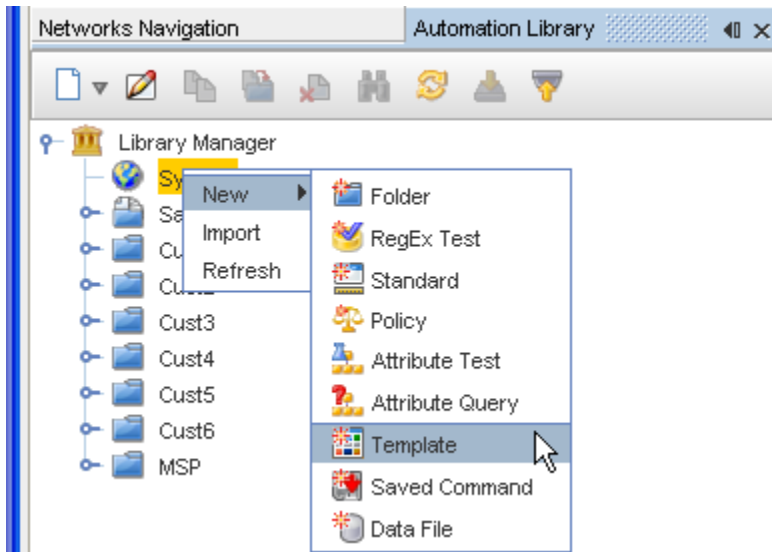
### Creating a New Template

Templates are used to streamline the configuration process, and to provide added control of variables that are used in the config files. Templates allow you to not only reduce configuration time, possible errors and down time, but also to increase network stability and optimization.

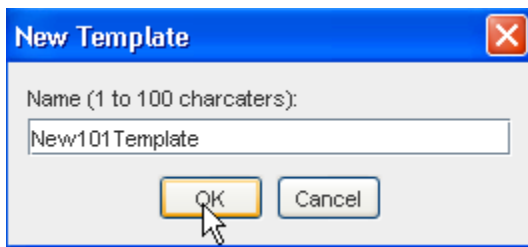
When a duplicate name is used for a template, you are prompted to change the name of the new template, or to cancel the creation on the template.

**Template Tips:**

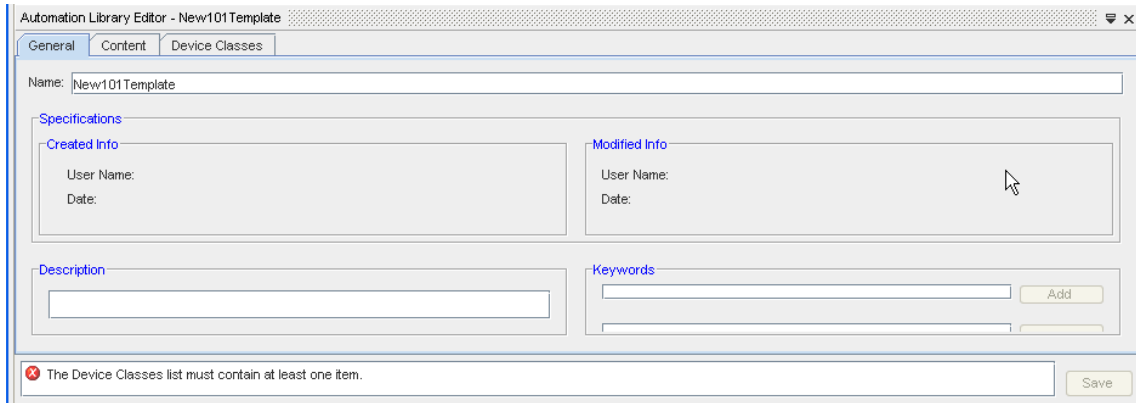
- Templates are used for new deployments and mass change, but **not** for ongoing policy changes in the network.
  - A template should be constructed from a contextual subsection of a config.
  - Primary templates should contain all contextual templates needed to construct a "gold standard" configuration.
  - A compliance audit for a contextual template is constructed from one or more tests.
- 1 To create a new **Template**, you must first select the **Automation Library**.
  - 2 When the Library Manager opens, right-click on **System** (or a folder name), then select **New** -> **Template** .



- 3 At the New Template window, enter a template **Name**, then click **Ok**.



The Automation Library Editor for the new template now displays.



- 4 At the General tab, **enter Keywords** if needed. First enter the keywords into the field, then click **Add** to add the words into the active field.

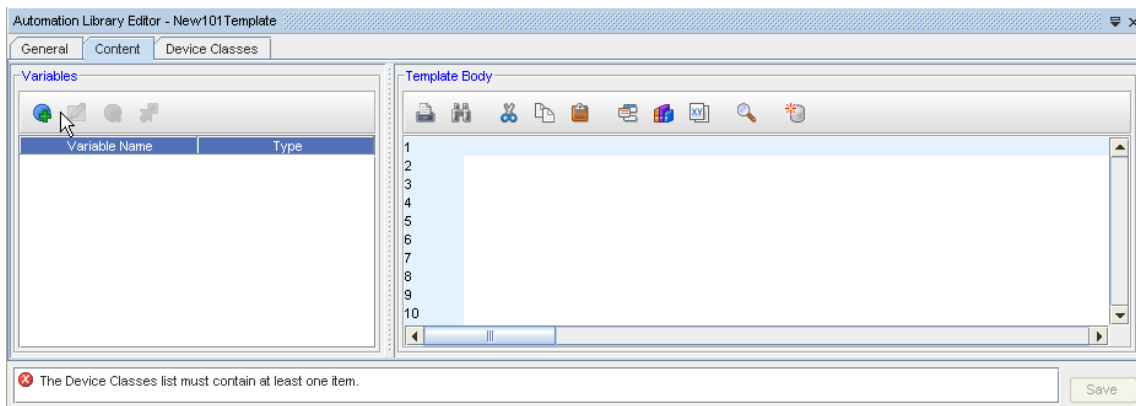
Keywords are words that are used to **define the content of the template** . For example, if you are creating a template for configuring Cisco devices with several technology types: Frame Relay, Ethernet and Private Lines, then you may want to enter the following keywords.

- Cisco
- routers
- switches
- frame relay
- ethernet
- private lines


You should enter any keyword that identifies the template when completing a search. When a search is completed on a keyword, all templates that contain the keyword are displayed. The search list can be modified in two ways: adding items to the list, and removing items from the list.

At the Contents tab,

- 1 Go to the **Contents** tab, and begin to add content to your template.





- 2 Click the **Add**  icon to add a row to the Variables section. The Template Variable window now displays, where you can enter a **Name**, select the **Type**, add Minimum and Maximum lengths if needed, and then enter the actual **value**.

When creating a template you can designate **variables** in which the user can supply a value (for example, password, IP address, DLCI, host name, or community string). These variables can be one of the following types:

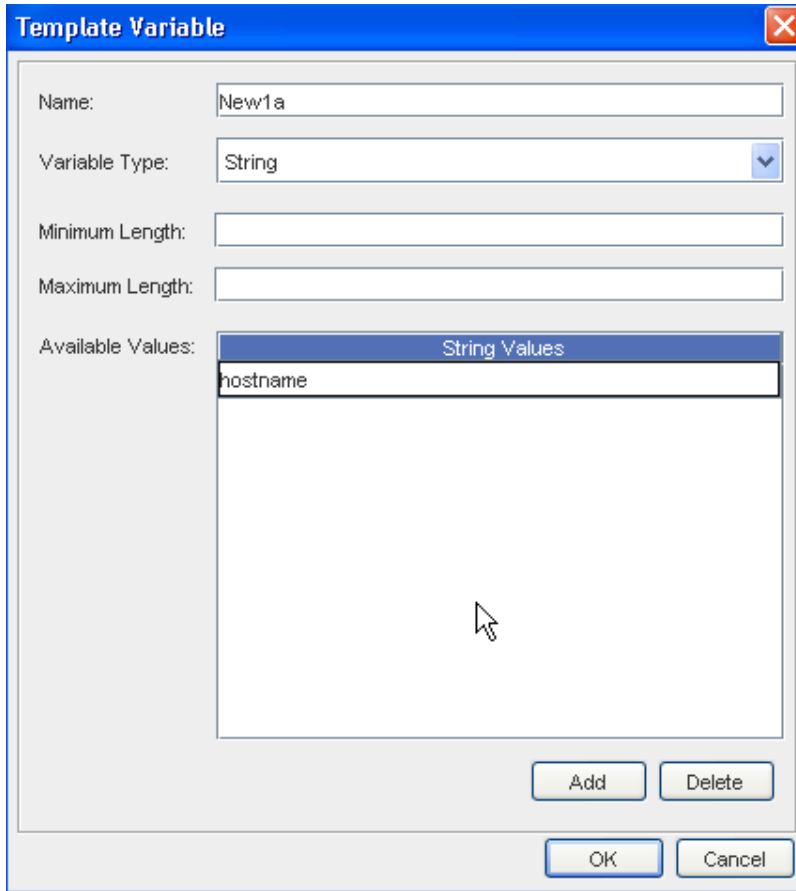
- String - allows any alphanumeric character
- Integer - designates that only numbers can be entered in the field
- IPv4 Mask - can be a subnet mask or a wildcard mask
- IPv4 Addresses - can be any valid IP address

You can further define what the user can enter into the variable field using **validation rules**. For example, when creating a variable for a password, you might wish to set a minimum and maximum value for the number of characters allowed.

You can create **available values**, which enables the user to select from a predefined list of values. This is useful, for example, when creating a template variable for Management router IP addresses.




There are many benefits to creating variables within your templates, including:

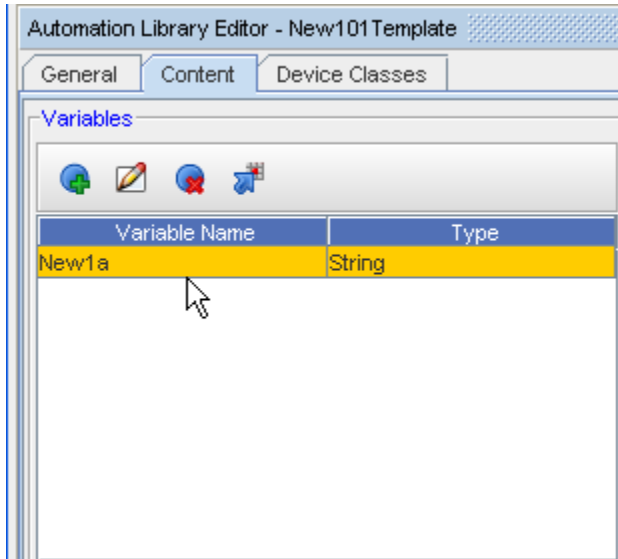
- Reduced errors
- Increased user entry speed through the use of predefined lists
- Flexibility when creating templates




- 3 Click **Ok**, and now see that the new value is added to the **Variables** section.

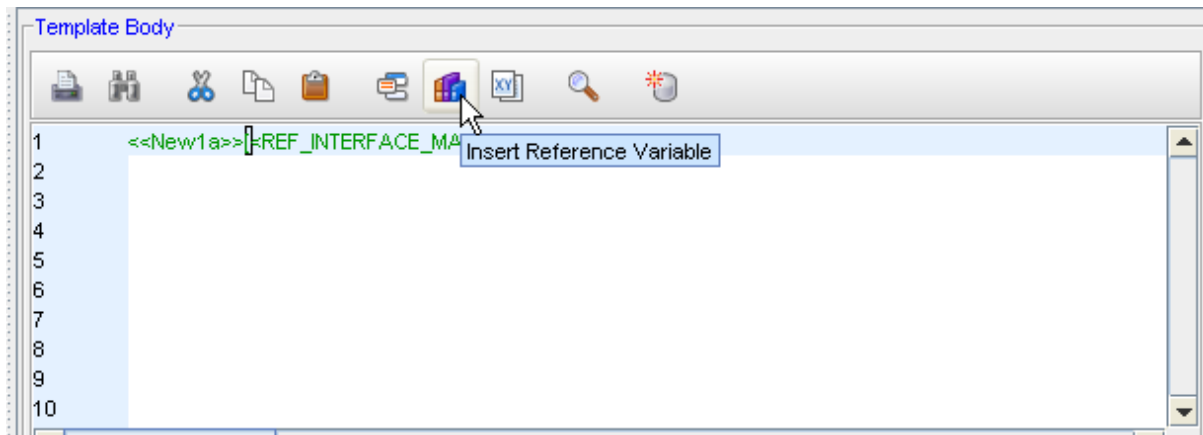
**Note** Notice the other available icons on the **Variables** section of the Editor.

Icon	Description
	Used to Edit an existing Variable in the list
	Used to Remove an existing Variable in the list
	Used to Insert the selected Variable into the Template Body section of this editor



- 4 At the **Template Body** section, run your cursor over the icons, and then select to insert or add any additional items to your template. For example, use the Insert Reference Variable icon to select and then insert a template variable into the Template you are creating.











For example, the Find  feature allows you to **locate a single alphanumeric word or word strings within a template**. It is not necessary to replace information once it is located within the template. You can complete a search to see where and how the information is used.




---


**Note** Notice the other available icons on the **Template Body** section of the Editor.

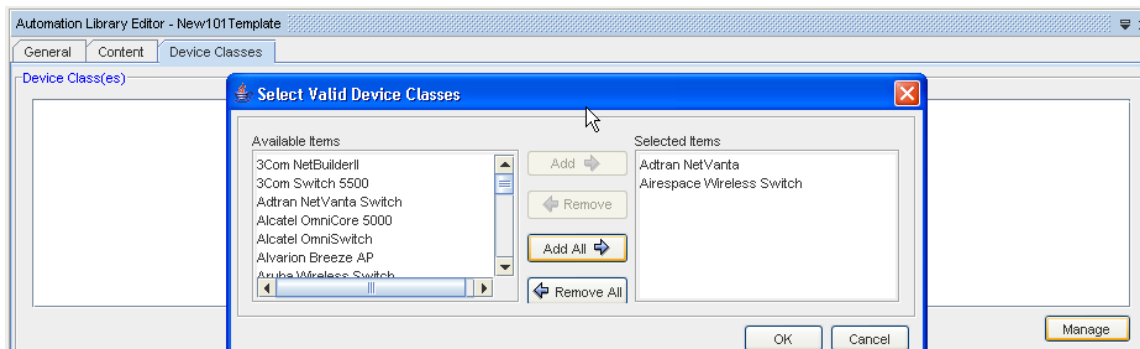
---

Template Body	
Icon	Description
	Used to Print
	Used to find words or strings
	Used to Cut words or strings
	Used to Copy
	Used to Insert Templates
	Used to Insert Reference Variables
	Used to Generate Variables
	Used to Paste what is cut
	Used to Preview the Template
	Used to create Data Files

At the Device Classes tab,

- 1 Now, go to the **Device Classes** tab, and click **Manage** to get to the Device Classes list.

**Caution** Notice the error message  displaying. During your creating the template, appropriate errors display until they are resolved by your addressing the error, and making the correct selections or insertions.



- 2 At the Select Valid Device Classes window, select the **Device Classes** you want to add by first highlighting them in the Available Items column, then using the **Add** or **Add All** arrows to move the items into the **Selected Items** column.
- 3 Click **Ok** when you have completed selecting the Valid Device Classes.
- 4 Click **Save** to save your newly created Template.
- 5 **Close** the Automation Library, and see that your Template is now stored in the folder.

---

**Caution** Notice the error warning is now gone.

---

### Removing Templates from the Automation Library

Periodically, you should cleanse the Automation Library of obsolete Templates.

- Deleting files that are in the Automation Library do not delete the same file that you have saved locally.
- You are strongly encouraged to immediately remove any files from the Automation Library that you have saved to a local drive.
- Although Network Configuration Manager does not allow you to import a non-unique name, it does not track revisions.
- You must cleanse your local Templates in the location where they are saved.

---

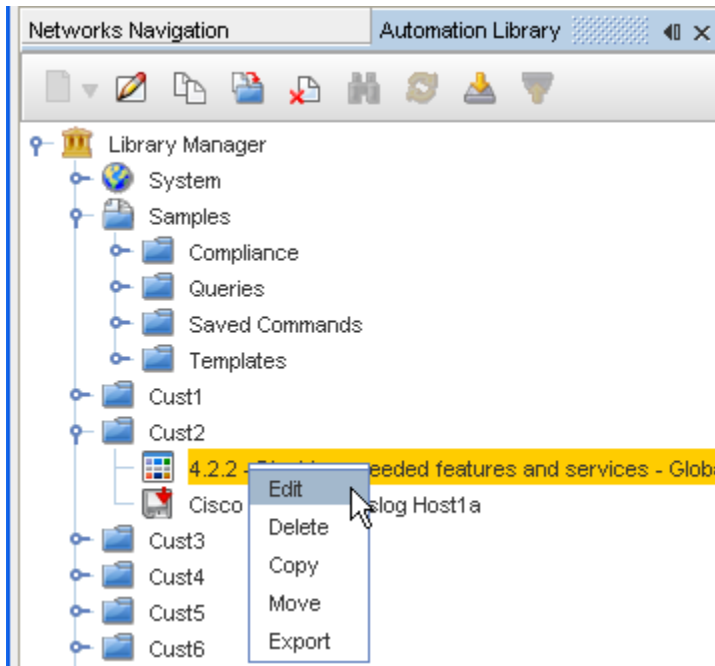
**Note** Remove Templates one at a time.

---

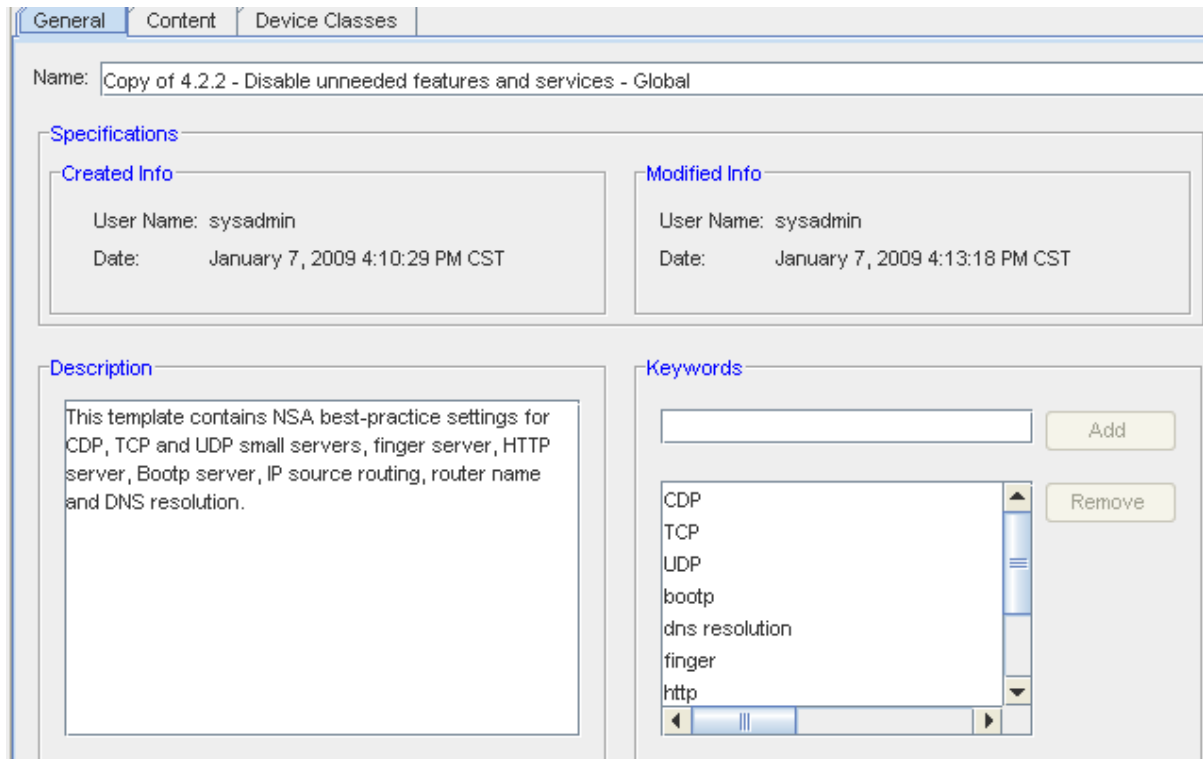
### Customizing a Pre-defined Template

Once you have copied a pre-defined Template, and have decided to make small changes to the content to create a customized Template, the steps are very similar to creating a new Template.

- 1 First, right-click on the copy of the Template, and select **Edit** from the options.



The Automation Library Editor opens.

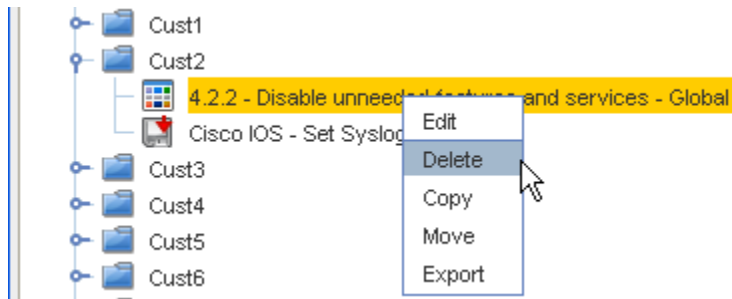


- 2 Go through the steps needed to change any existing information or to add any additional information in the **General**, **Content** and **Device Classes** tabs.
- 3 Make sure you click **Save** after making changes. Your customized Template is now completed.
- 4 **Close** the customized Template.

## Template Right-Click Options

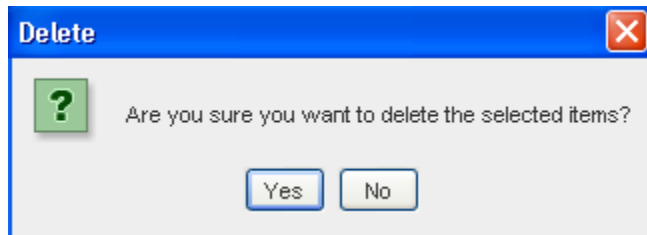
Along with the **Edit** and **Copy** options, offered in the right-click menu, you can also complete the following tasks:

- **Delete** any existing Templates
- **Move** the Template to another location
- **Export** the Template outside of the application



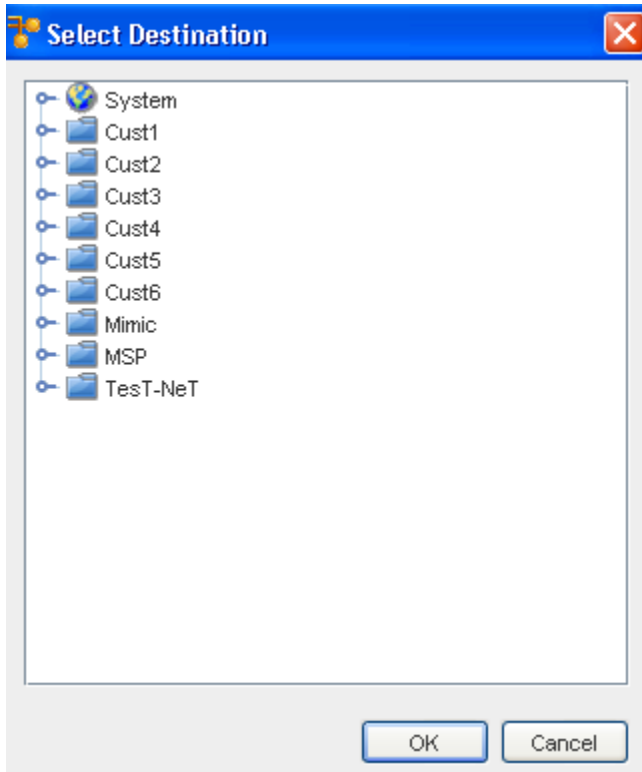
### Delete Template

If you select to **Delete** the existing template, a Delete message is displayed. Click **Yes** to delete the template.



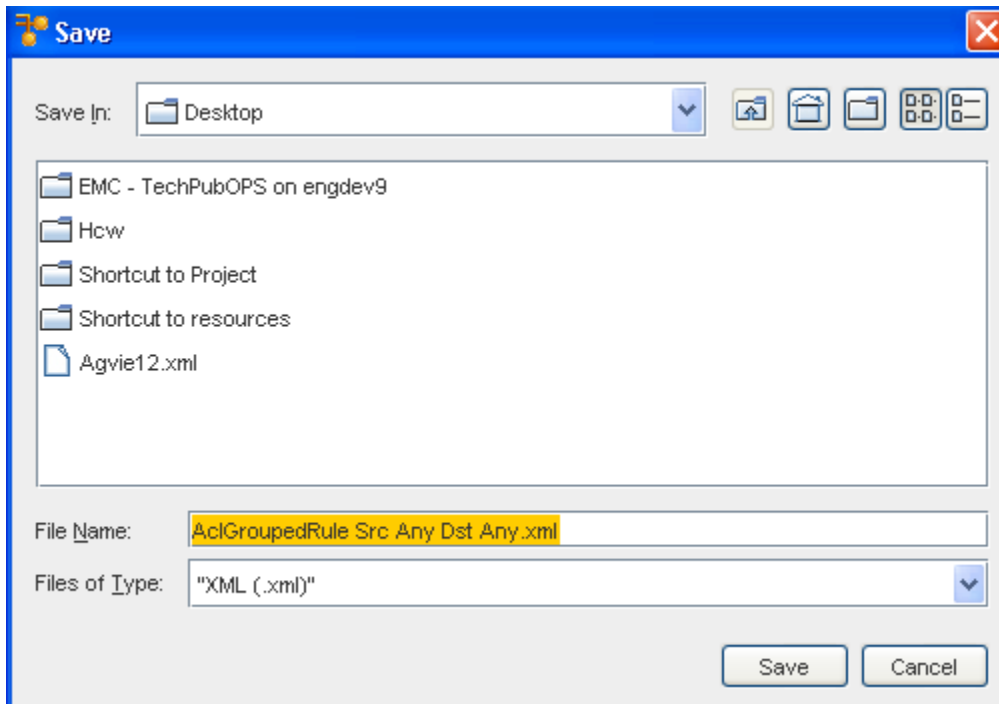
### Move Template

If **Move** is selected, the Destination Selection window opens. Make your selection of where you want the template moved to, then click **Ok**.



### Export Template

If **Export** is selected, the Save window opens. Make your selection on where you want the template exported to, along with the selecting the **File Type** , then click **Save**.

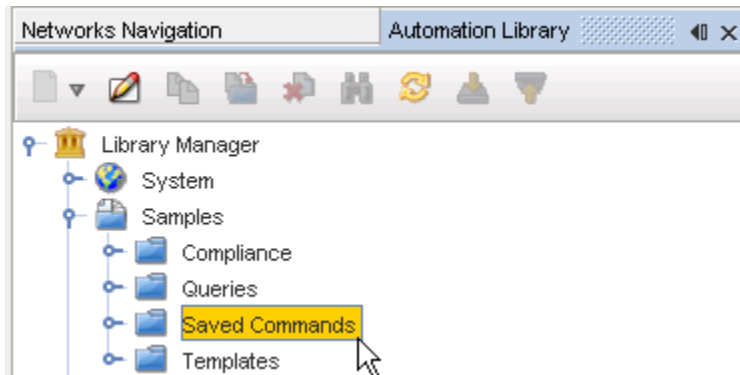


### Working with Saved Commands

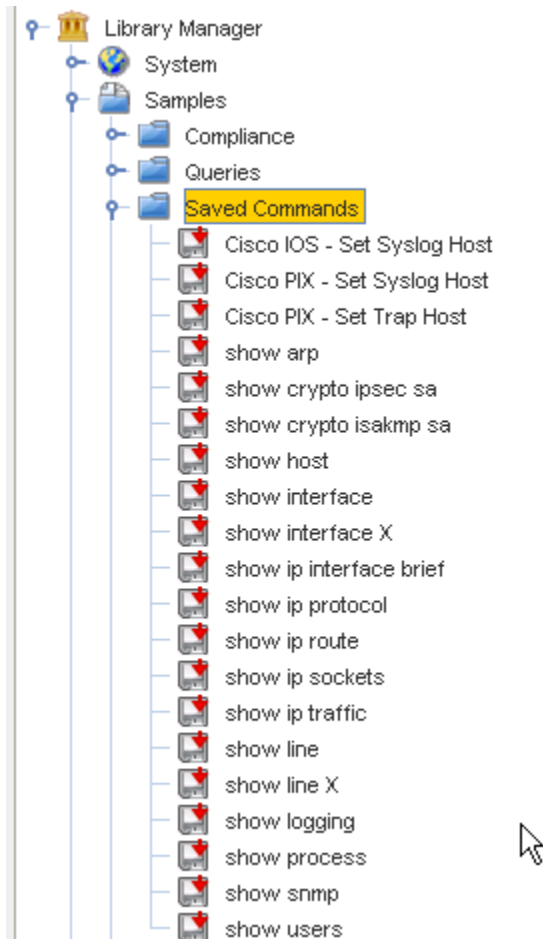


## Accessing Saved Commands Samples

You can first think of using Saved Commands by accessing the Pre-defined Saved Commands that are stored in the Samples directory.



- 1 Once you have accessed the **Saved Commands** folder, expand the folder and review the number of pre-defined commands.




---

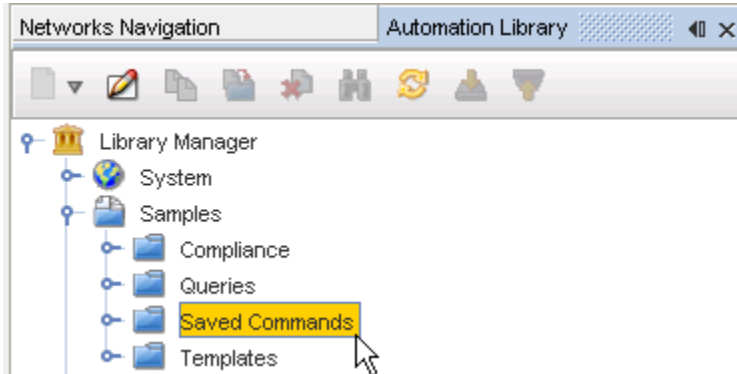
**Important** These Saved Commands are the commands that will be added if you use the right-click option when Devices are displayed in the Devices View (in Networks Navigation).

---

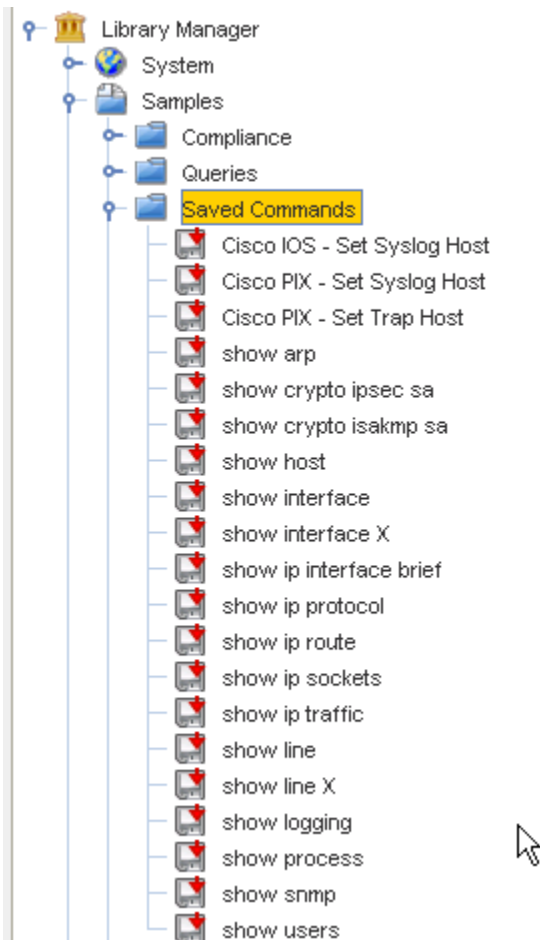
- 2 Now, select from the various commands (one at a time) to review the contents.

### Copying a Pre-defined Saved Command

- 1 Access the **Saved Commands** folder from the Samples section of the Library Manager.

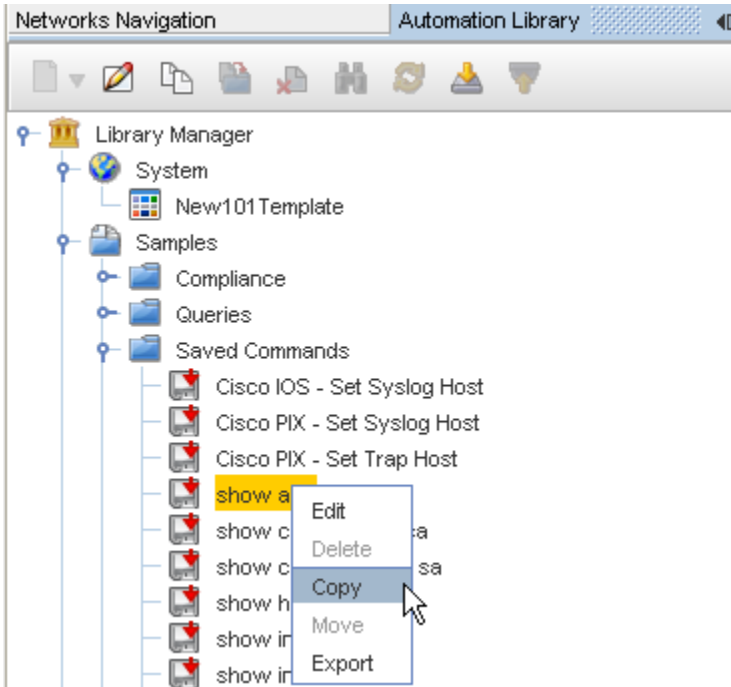


- 2 Once you have accessed the **Saved Commands** folder, expand the folder and review the number of pre-defined commands.

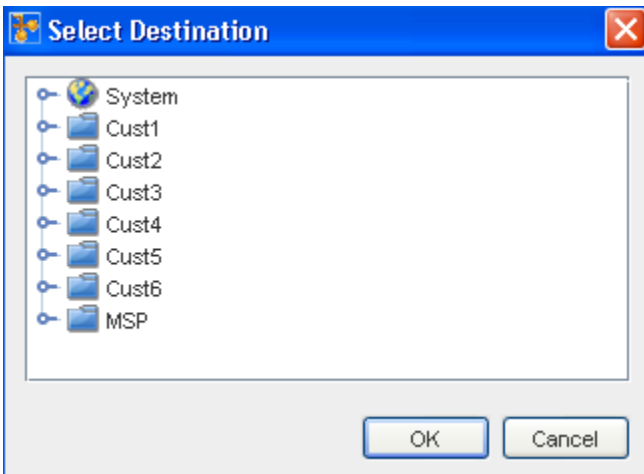


**Important** These Saved Commands are the commands that will be added if you use the right-click option when Devices are displayed in the Devices View (in Networks Navigation ).

- 3 Now, select from the various commands to review the contents.
- 4 Once you have determined the Saved Command you want to copy to use and customized, **right-click** on that command, then select **Copy**.



- 5 Select a **destination** to store the copy from the Select Destination window.

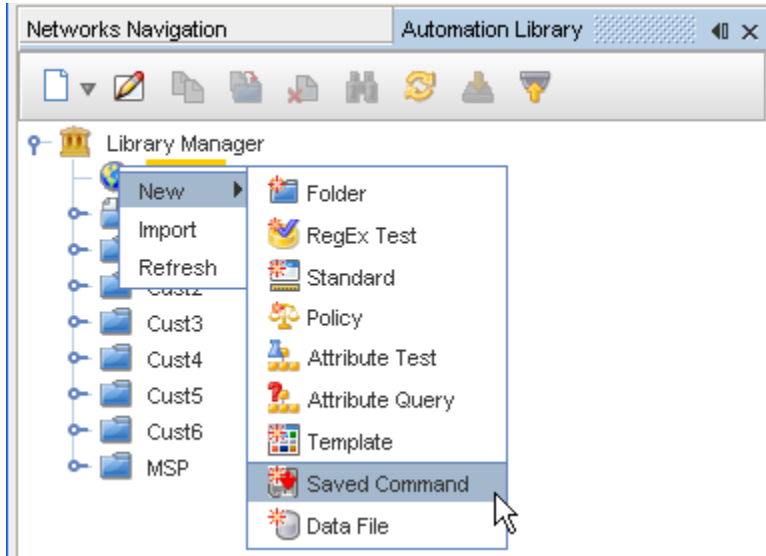


- 6 Click **Ok** when you have determined the destination.
- 7 Check the Automation Library and verify that your copied Saved Command is now in the correct destination.

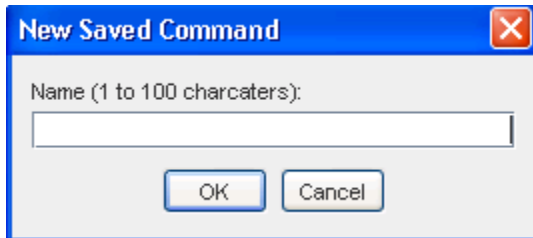
### Creating a New Saved Command

The Saved Command feature in the **Automation Library** allows you to input config command details in an editor. Once the file is properly configured, the "source" (DASL) is immediately available for edit.

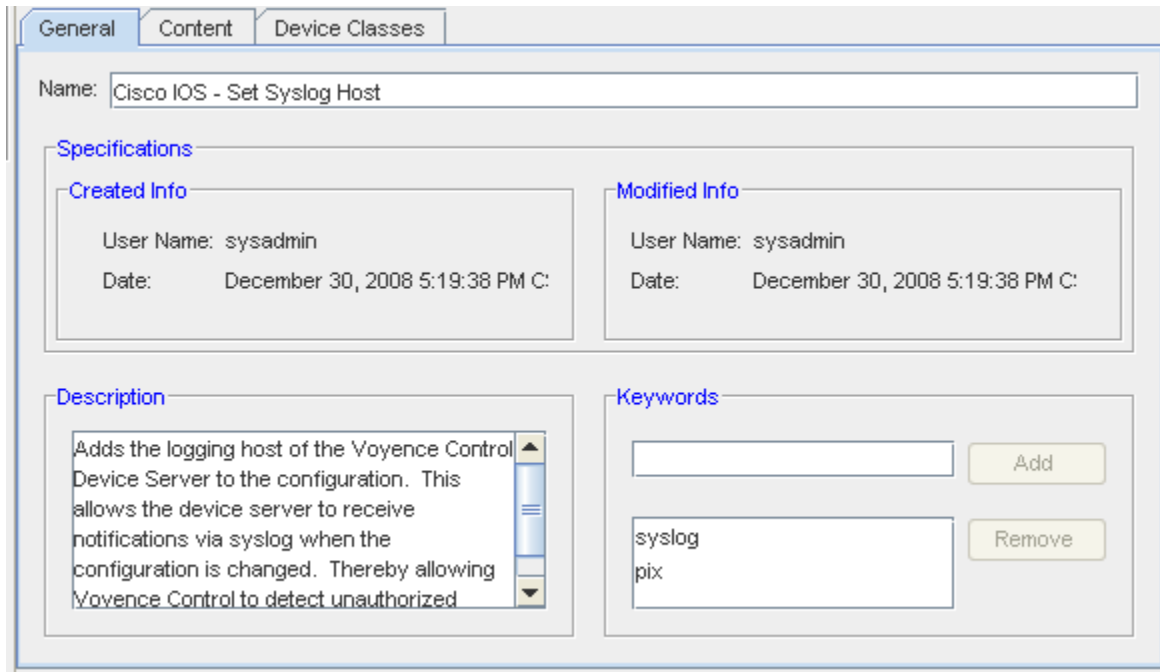
- 1 From the **System** (or a folder name), right-click, and select **New -> Saved Command**.



- 2 At the New Saved Command window, enter a **name**, then click **Ok**.



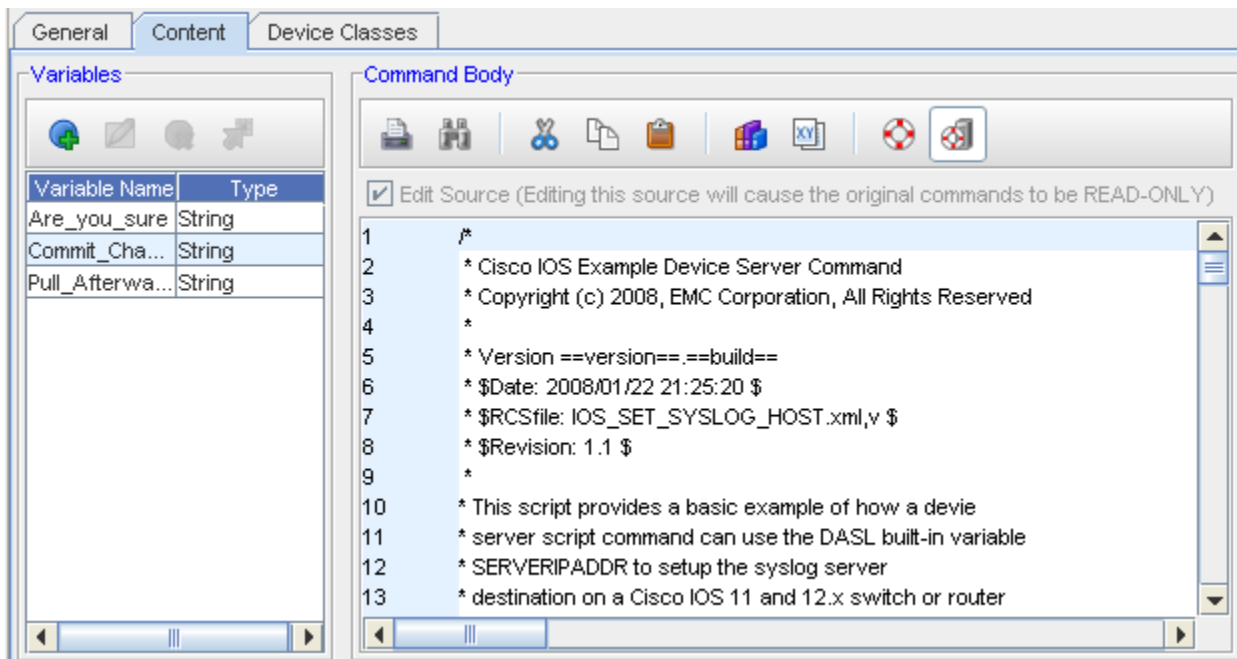
The Automation Library Editor (with the save command name) now displays.



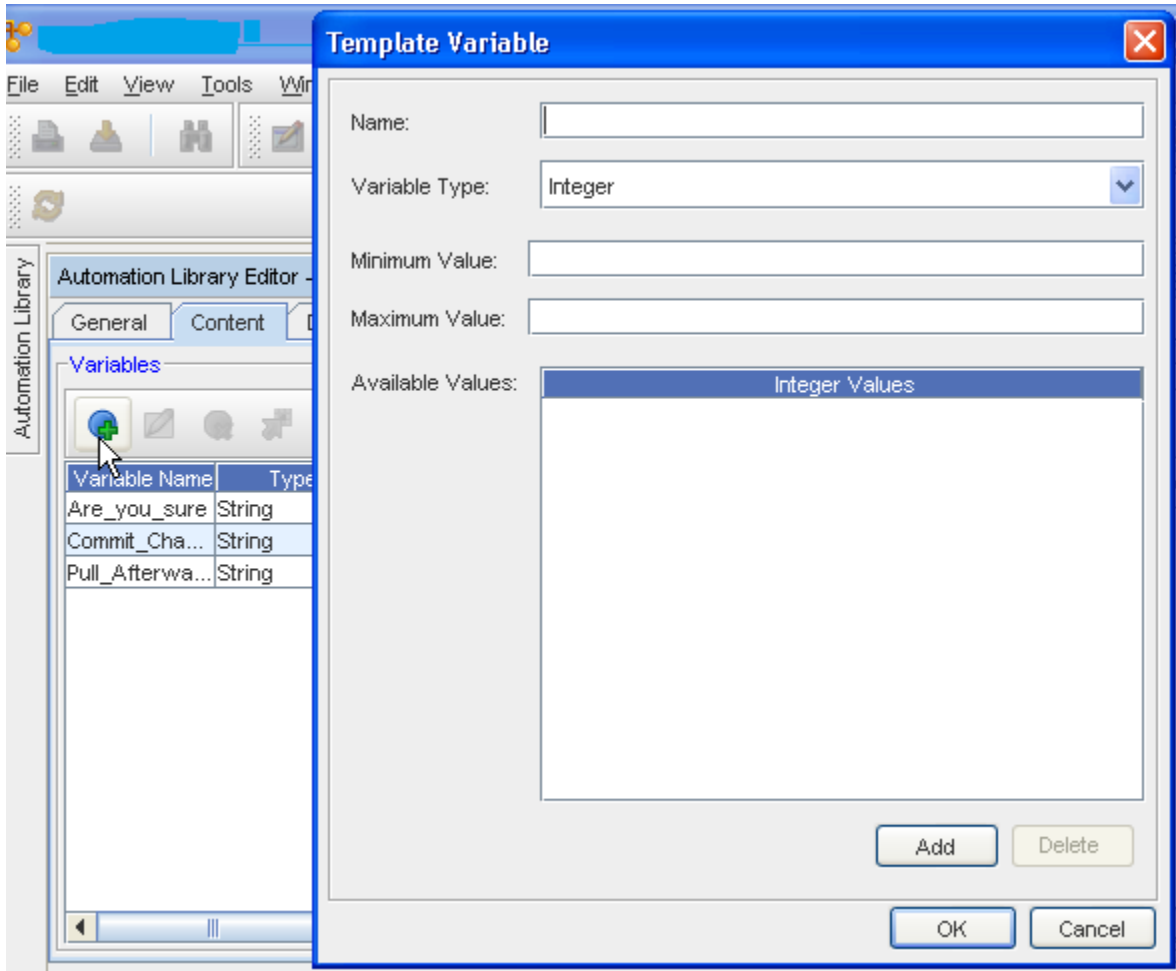
General tab,

- 1 At this tab you can add **Keywords** if needed, by first adding the keywords into the field, then clicking **Add**.
- 2 Click **Save** at this tab, then continue to the **Content** tab.

Content tab,



- 1 To add a template Variable to the content tab, click the **Add**  icon .



The Template Variable window opens.

2 Enter **variable name**. **Note that a variable name cannot have spaces**.

- Correct: "hostname"
- Incorrect: "host name"

**Remember!** You are limited in the special characters you can use to create a variable name. See [Special Characters](#) for more information.

3 Select a **variable type** from the drop-down options. Depending on the selected variable type, you can provide optional variables, such as **Minimum** and **Maximum values**.

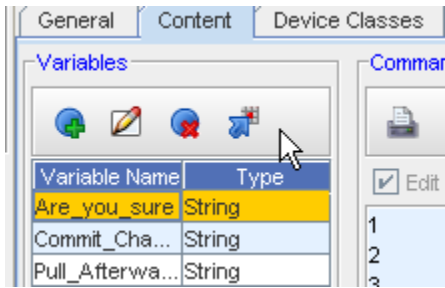
4 To create available values, which enables the user to select from a predefined list of values, click **Add**. The Available Value window opens.





5 Enter the **value**. If any data is entered in Available Values, only this data can be used to populate the variable. Continue to **add values** in this manner, as needed.

6 When finished, click **OK**. The Template Variable window closes.

The variable is now added to the **Variables** section of the Saved Command editor.




You can complete the following tasks from this section:









Icon	Task
	Used to open the Template Variable window where you can add a variable to a template.
	Edit the highlighted variable. Brings up the Template Variable window
	Removes any existing variable that is highlighted in the list
	Inserts the variable command into the Command Body section.

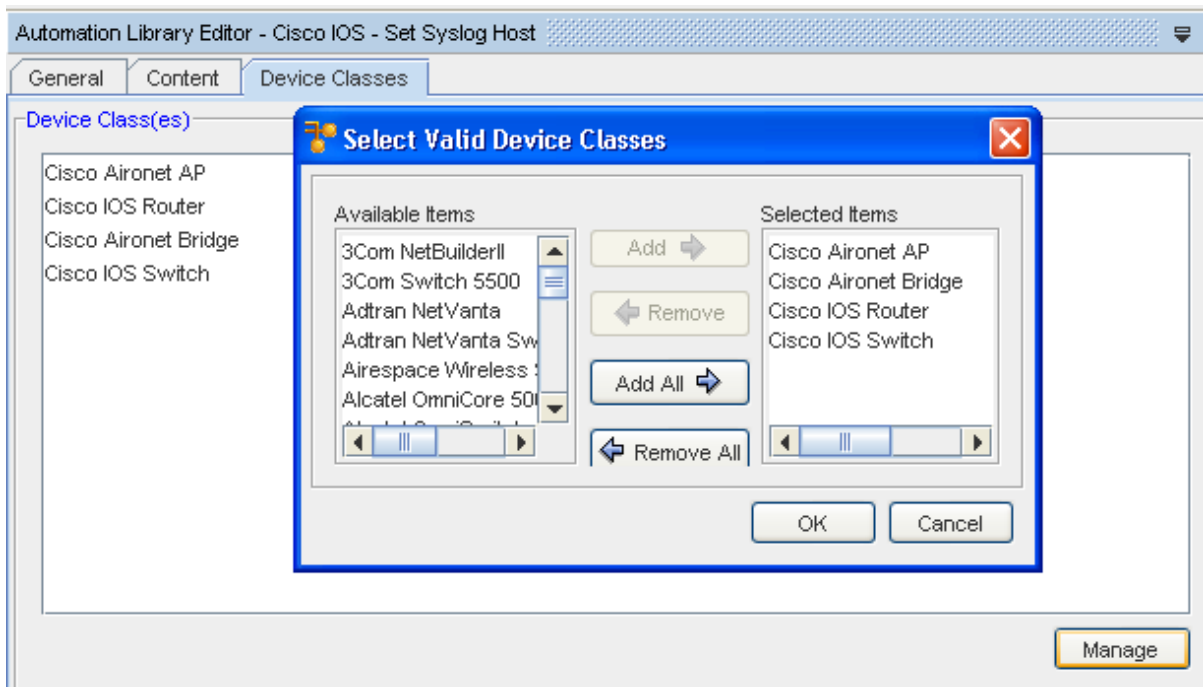



In the **Command Body** section, you can complete the following using icons:

Icon	Description
	Used to Print
	Used to Search the body content
	Used to Cut the body content

Icon	Description
	Used to copy the body content
	Used to Paste the body content
	Used to Insert Reference Variables
	Used to Generate Variables
	Used to Show Command
	Used to Show Source.

### Devices Classes tab



- 1 From the Device Classes tab, click **Manage** to view there Select Valid Device Classes window.
- 2 Make your selections by highlighting then moving the classes from the Available Items column into the Selected Items column using the **Add** or **Add All** buttons.
- 3 Click **Ok** when you have completed adding Device Classes. Notice the error  is now gone!
- 4 Click **Save**, and the **Close** the Automation Library Editor.

Your Saved Command is now listed in the Folder in the Automation Library.

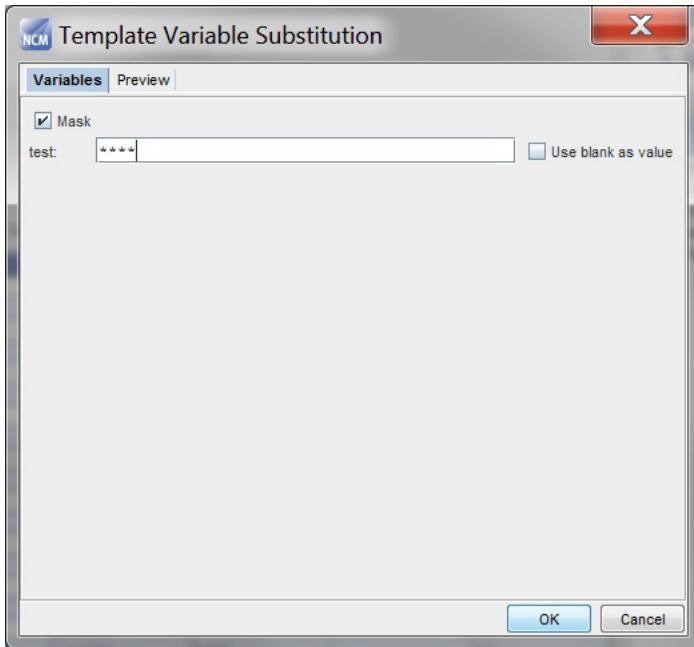
### Masking template variable values



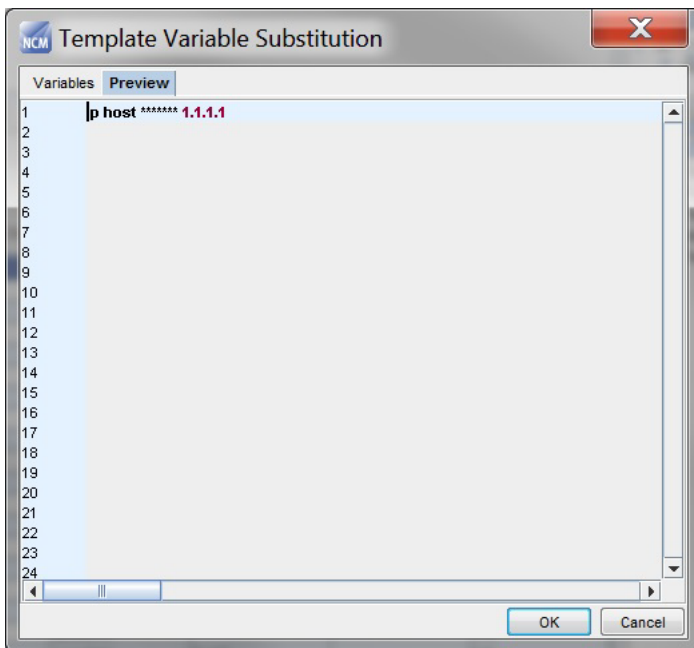
If you created a Saved command using template variables, you can mask the template variable values:

- 1 Access the **Template Variable Substitution** dialog by running the Saved command.
- 2 Enter the values of the Template variables.
- 3 Select the Mask checkbox.

When Mask is selected, the template values entered are masked with \*\*\*\* characters.



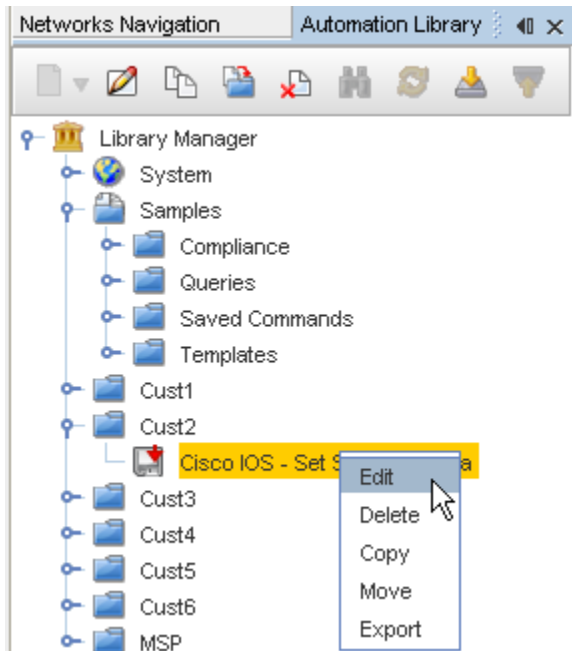
Preview can be seen by clicking on the Preview tab.



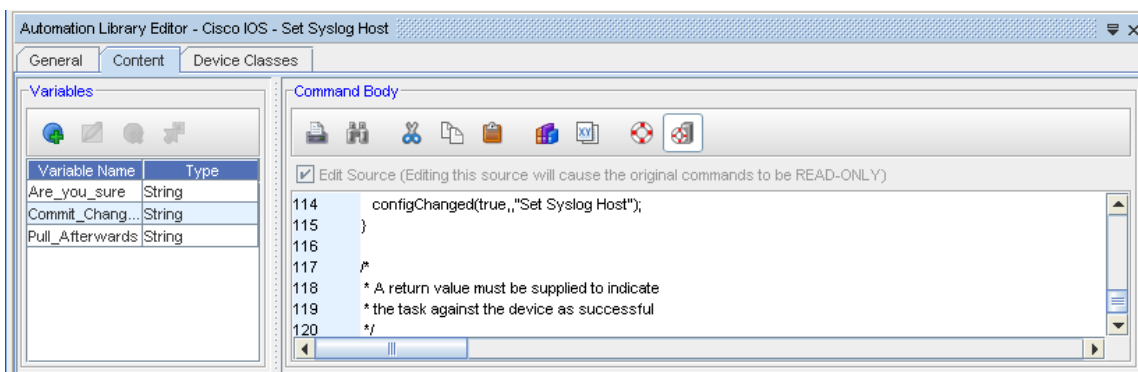
## Customizing a Pre-defined Saved Command

Once you have copied a pre-defined Saved Command, and have decided to make small changes to the content to create a **customized command**, the steps are very similar to those used in creating a new Saved Command.

- 1 First, right-click on the **copy** of the Saved Command, and select **Edit** from the options.



The Automation Library Editor opens.

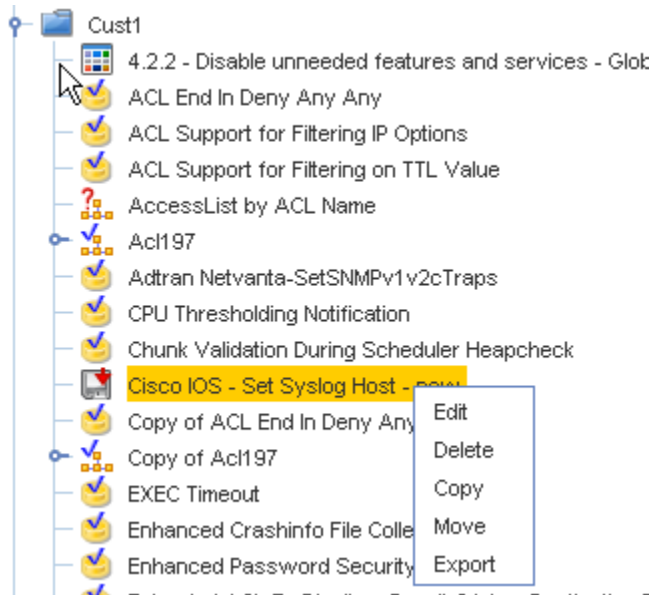


- 2 Go through the steps needed to change any existing information in the **Content** and **Device Classes** tabs.
- 3 Make sure you click **Save** after making changes. Your customized Saved Command is now completed.
- 4 **Close** the customized Saved Command.

## Saved Command Right-Click Options (Deleting a Command)

Along with the **Edit** and **Copy** options offered in the right-click menu, you can also complete the following tasks:

- **Delete** any existing Saved Commands
- **Move** the Saved Command to another location
- **Export** the Saved Command outside of the application



### Deleting a Saved Command

**Important** Periodically, you must cleanse your local Data Files and Templates in the location where they are saved. Delete your Saved Commands, one command at a time.

## Working with a Data File

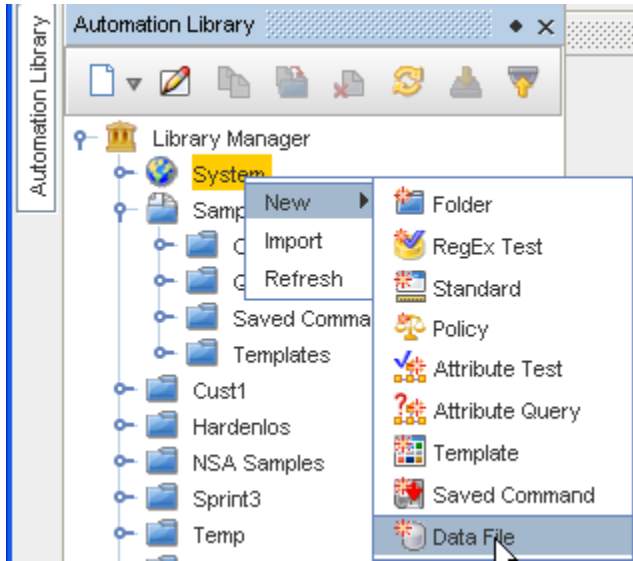
### Creating a New Data File

A Data File is created from a template's variables.

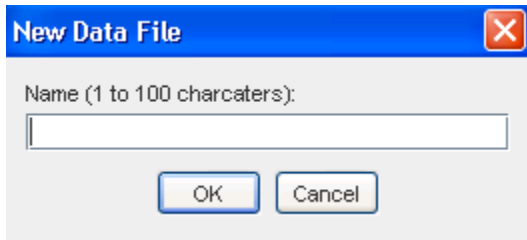
A Data File pulls all template variables into an editor and allows you to edit the details. Editing the Data File in this manner allows you to complete "mass changes" to templates, and then re-import the new content to the templates.

When saving a Data File, you have the option of saving the file internally (to the Automation Library), or externally (local drive, server, or network drive). Internally saved Data Files are always accessed from the **Automation Library**. Externally saved Data Files must be re-imported.

- 1 From the System icon, right-click and select **New**.

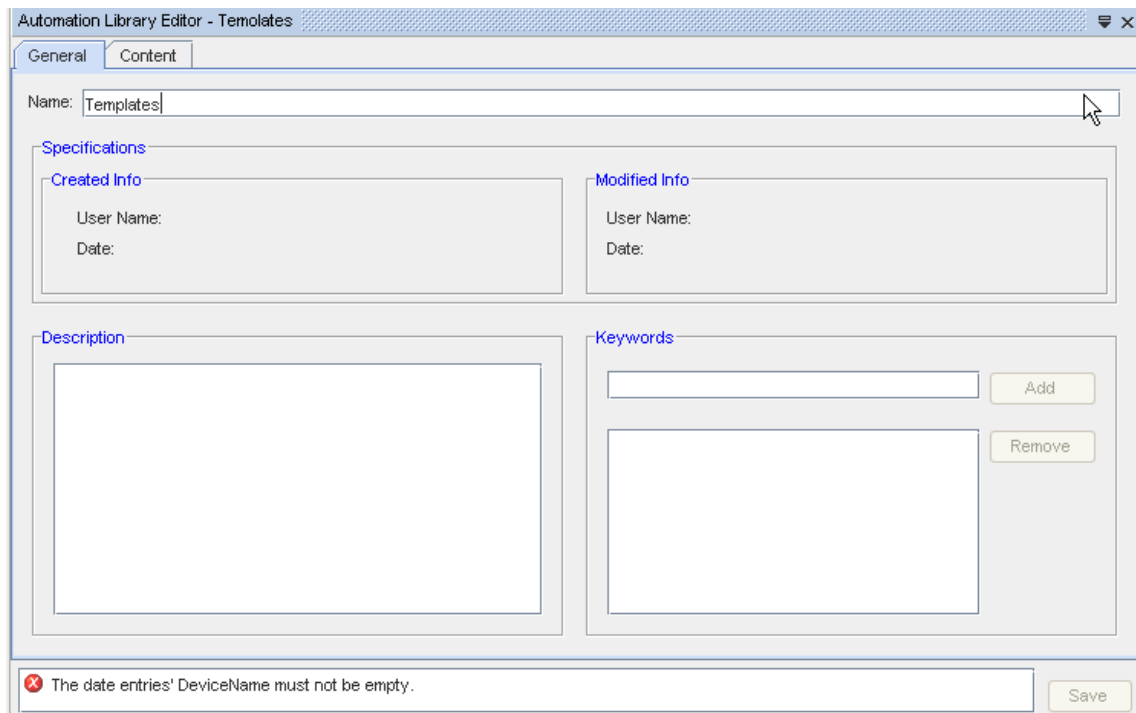



- From the New options, select **Data File**.



- At the New Data File window, enter a **name** for this data file, and click **Ok**.

The Editor opens.



Notice the error message .

General tab,








- 1 At the General tab, you can add **Keywords** by first entering the keyword or words into the first field displayed under Keywords, then click **Add**. This moves the keywords into the appropriate section.
- 2 Once any changes or additions are made to this section, click **Save**.

Content tab,

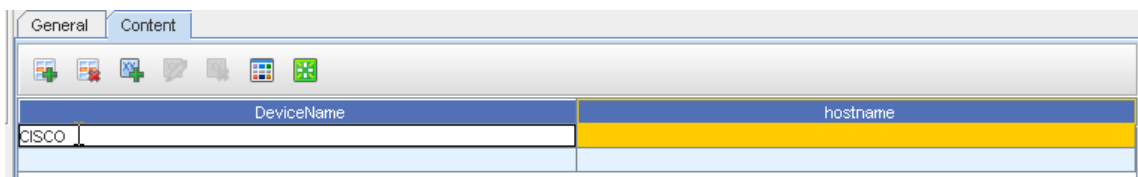
The Content tab is where you add all information for your Data File, and will select and add variables.

Options and Icons

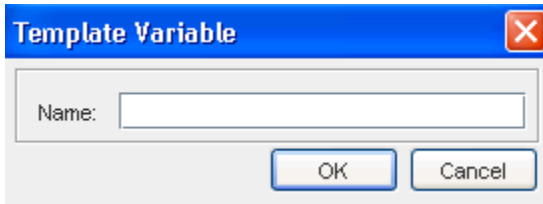


Icon	Description
	Add Row
	Used to Remove Row
	Used to Remove Variable
	Used to Edit Variable
	Used to Add Variable
	Used to Add Template Variable
	Used to Reset the window

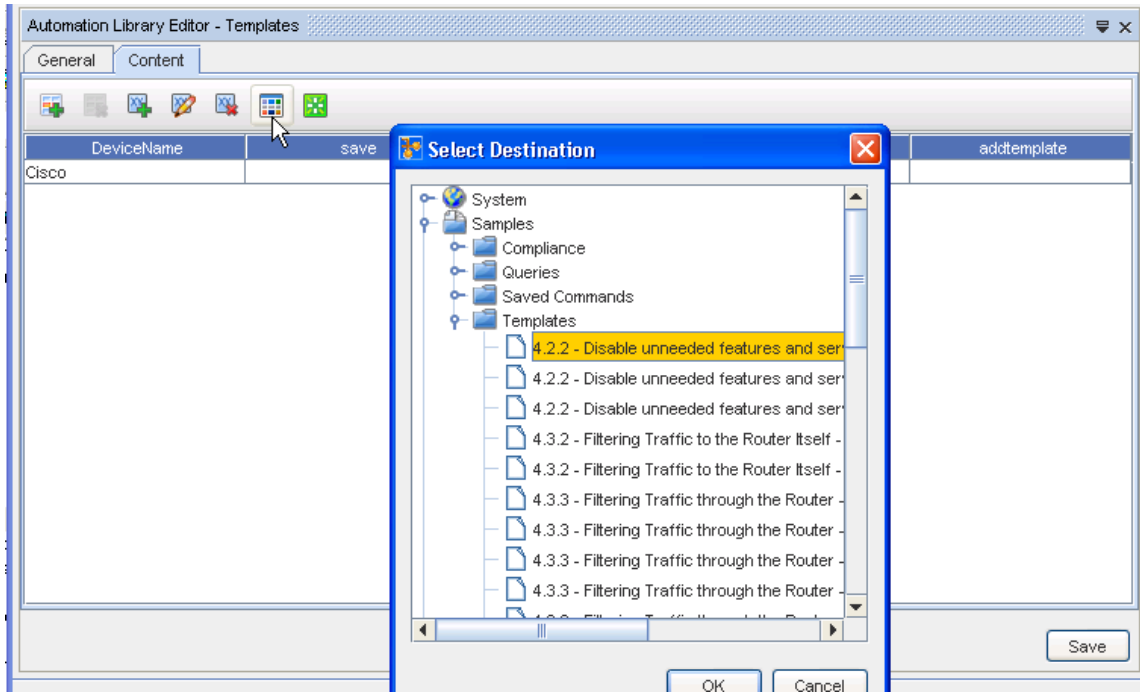
- 1 To Add a Row, click the **Add Row** icon. A new, empty row is now displayed.
- 2 Now, enter a **Device Name** in the DeviceName column.



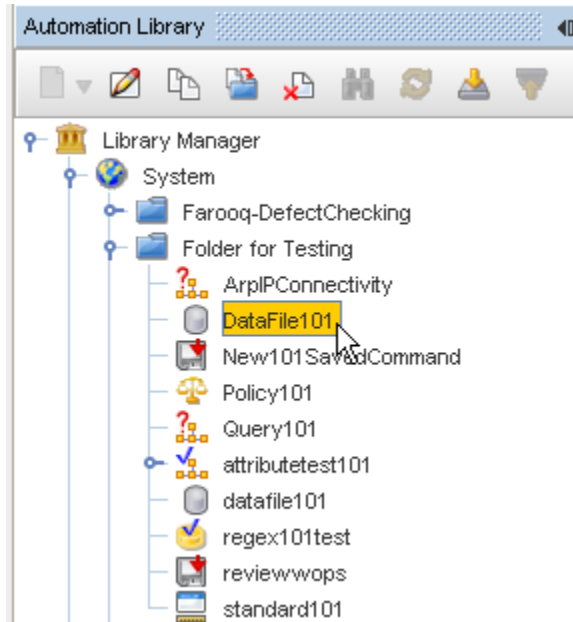
- 3 Add a Variable by selecting the **Add Variable** icon. Enter the **variable name** in the Template Variable window, and then click **ok**. You can edit the variable using the Edit Variable icon . You can also **Edit** or **Remove** an existing variable.



- 4 You must now select to **Add a Template Variable**, by selecting the icon , then select a destination for the template variable.



- 5 When you have made a selection for the destination, click **Ok**, then click **Save**.
- 6 You can now **close** the Automation Library Editor. Note that the Data File is now in the Folder on the Automation Library.



## Removing Data Files from the Automation Library

Periodically, you should cleanse the Automation Library of obsolete Data Files.

- Deleting files that are in the Automation Library does not delete the same file that you have saved locally.
- You are strongly encouraged to immediately remove any files from the Automation Library that you have saved to a local drive.
- Although Network Configuration Manager does not allow you to import a non-unique name, it does track revisions.
- You must cleanse your local Data Files in the location where they are saved.

---

**Note** When deleting Data Files, remove them one at a time.

---

## Working with Compliance Audit

### Compliance Audit Overview

The Compliance Audit tool allows you to **create standards and tests used to compare with configured devices**. By completing a Compliance Audit, prior to submission, approval, and sending changes to a device, you are able to:

- Standardize and validate deployed configurations in the network
- Find and fix variations in the network
- Define a compliance standard
- Apply a standard check against any existing device config file
- Report variations from the compliance comparison

A compliance standard consists of filters and tests. Filters allow you to define what type of device the standard is used for. A test sets up the pre-conditions and check patterns in the standard.

- Preconditions specify **config commands** that must be present before the test is run.
- Check Patterns is the **actual expression** that is searched for in the config, and the remedy for the variation.

Based on these details, any standard should follow the rules detailed in the table below.

Construct	Description
Standard	A standard must contain at least one managed device class.
Test	A test can have multiple steps and each step can have a <b>Begin With</b> and <b>End With</b> pre-condition, and must contain at least one check pattern.

A Compliance Audit can be launched from a Network, View, Site, Workspace, any of the Editors, or from the Schedule Manager.

### Supported Variables

In selecting the variables, you can view inquiries related to the variables within the templates. If two or more tests are selected that contain the same variable, the values entered are then used for the other tests.

You can select variables to use in precondition, check pattern, remedy configlet, or remedy comment for a check pattern test, and in the attributed test.

The following types of variables are supported:

#### Basic - which requires input from you

- String
- Password
- Numeric
- IPv4 Address
- Mask
- CIDR
- Regular Expression ??

#### List Entry - Requires input from you

- Strings
- Passwords
- Numerals
- IP Addresses



### Non-parameterized Reference Variables - Require no user input

**Example:** Device management IP, Device Server IP

### Parameterized Reference Variables - Requires user input in order to resolve reference variable

**Example:** Interface IP Address (requires user to select the interface)

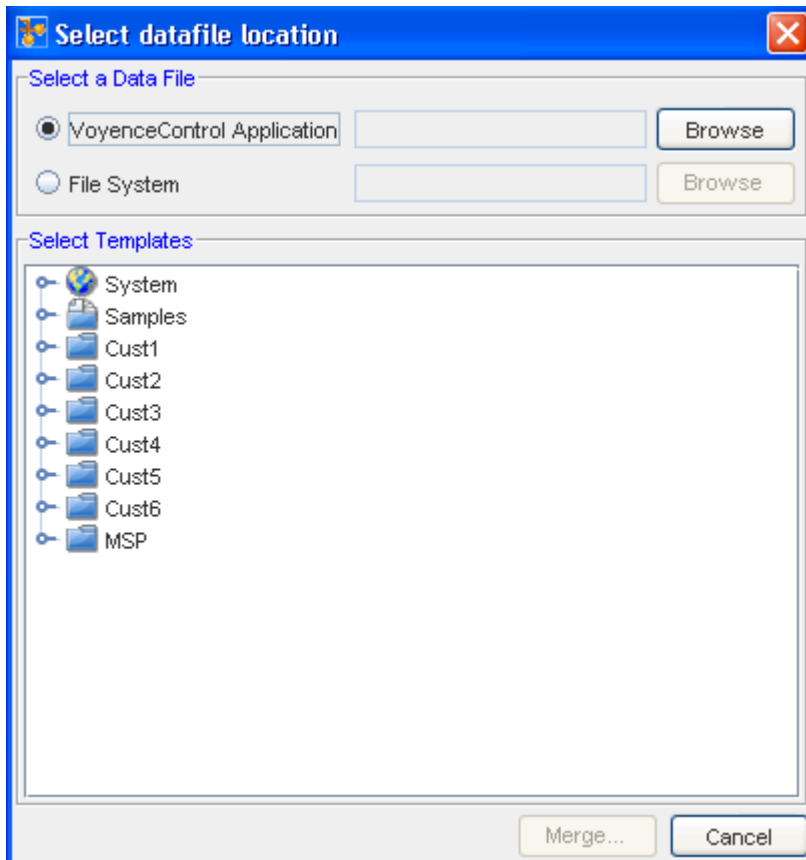
## Working with Template Merging

### Template Merging

- 1 In the menu bar, select **Tools** -> Template Merge.

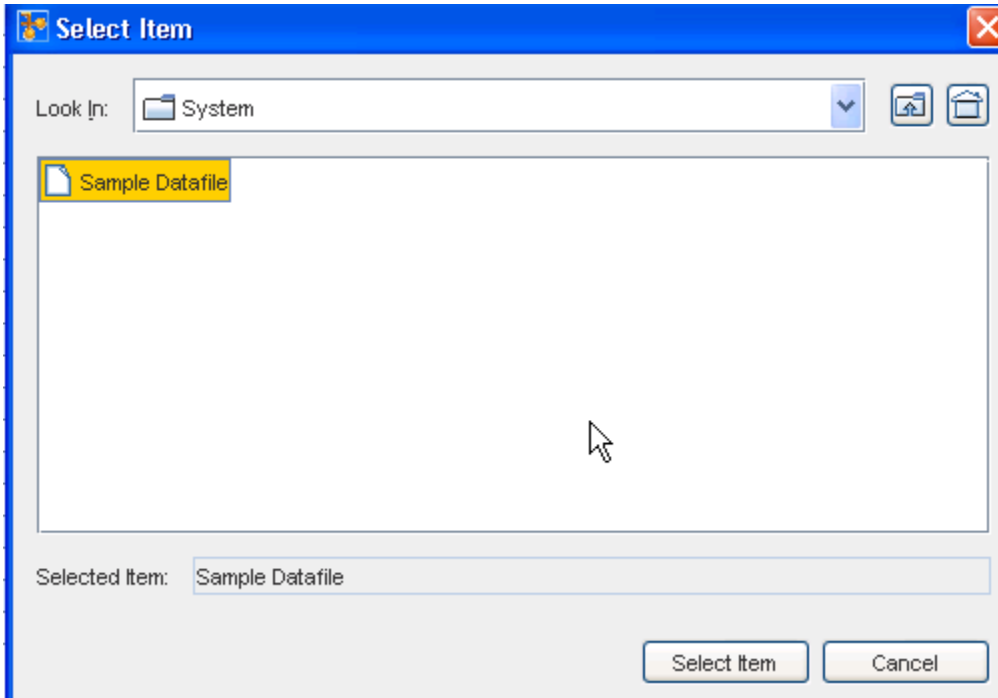


You will notice in the Select datafile location window, that you must first **Select a Data File**, then you **Select Templates**. This tells you that to complete the merge process you must have both the data file and the template already created.

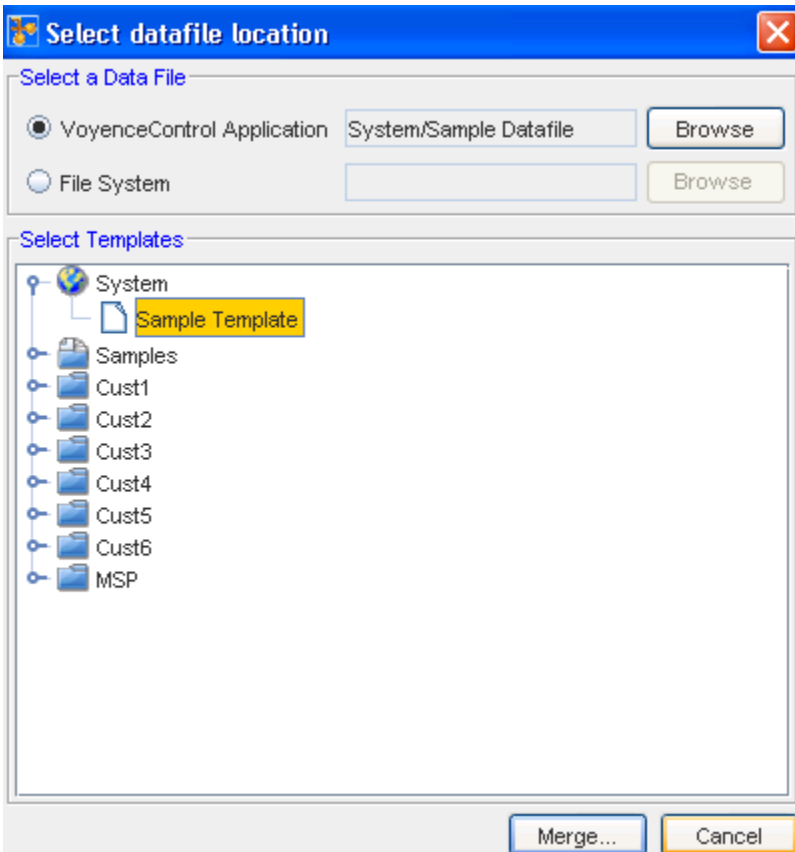


For this example of a merge, a Data File sample and a Template sample were created.

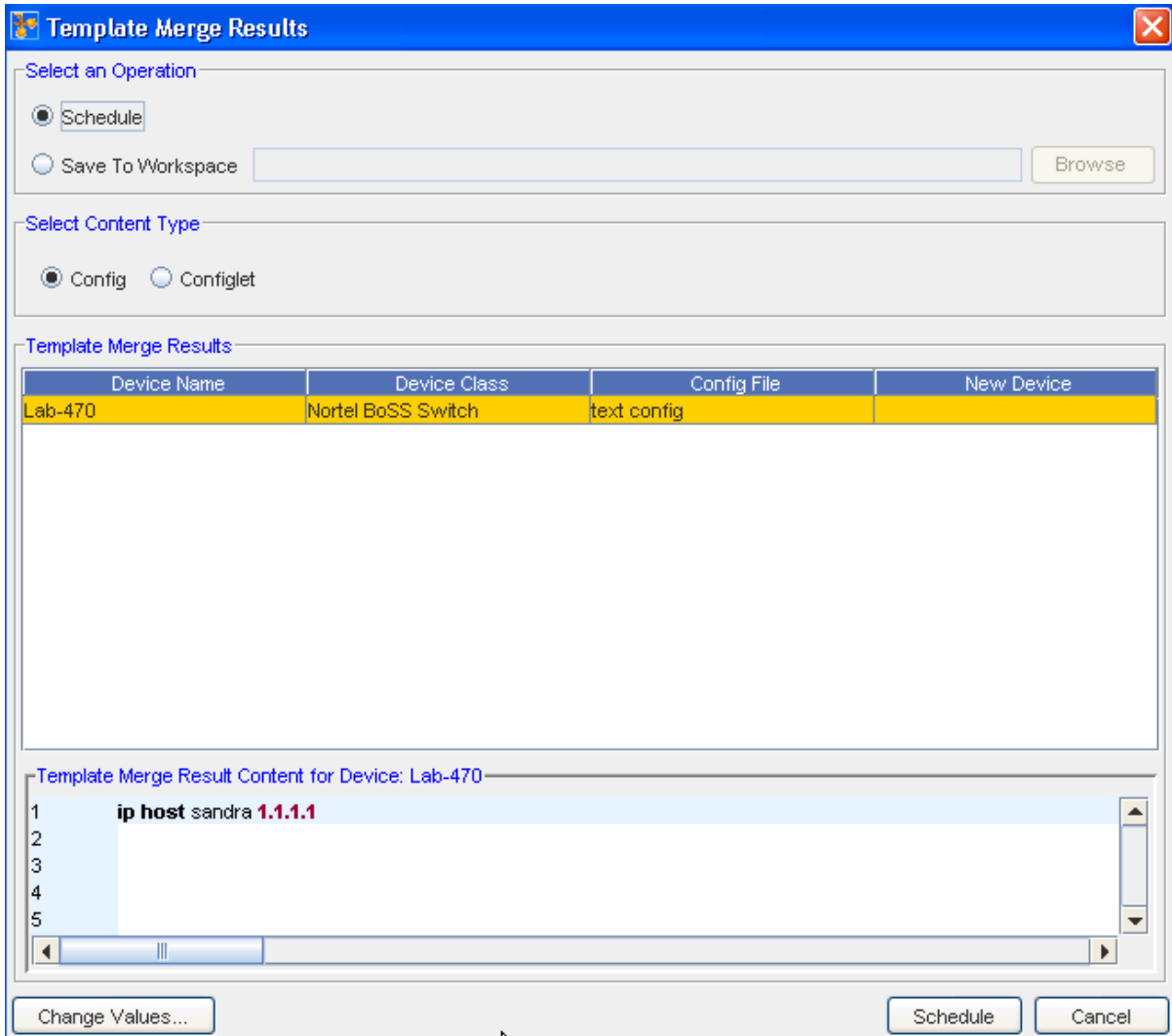
- 2 The **Select a Data File** section allows you to select the location (inside or outside) of Network Configuration Manager where the data file is located. You can use **Browse** to see your available options.
  - If you select a data file that is being managed internally by Network Configuration Manager, leave the default option, **Network Configuration Manager Application** selected.
  - If you are using a data file that has been exported externally of Network Configuration Manager, select **File System**.
- 3 Click **Browse** to select the Data File (from the Voyence Application) that you want to merge with the Template.



- 4 Now that you have selected a Data File, you can now select one or more templates to merge. At the Select Templates section, click **Browse** to locate a template you want to merge the Data File with.

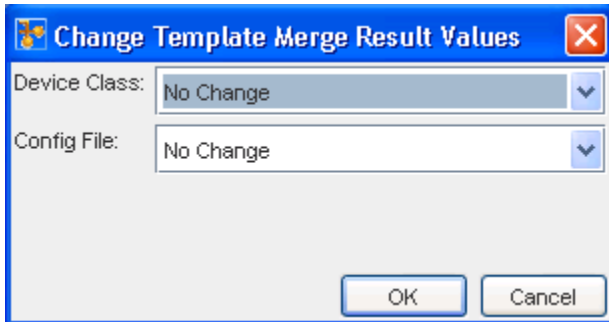


5 Once the template is selected, click **Merge**.



The Template Merge Results window now appears.

- Select an Operation - **Schedule** (click the Schedule bar) or **Save to a Workspace** (click the **Browse** button and select a Workspace).
- Select Content Type - **Config** or **Configlet**
- Change values - You can then change the Device Class or the Config file.



6 Use the drop-down arrows to select any changes to the categories shown in the window, make a selection, and then click **Ok**.

■ You can now:

Your results now have changed, based on the value changes.

## Working with OS Image Inventory Manager

### OS Image Inventory Manager Overview

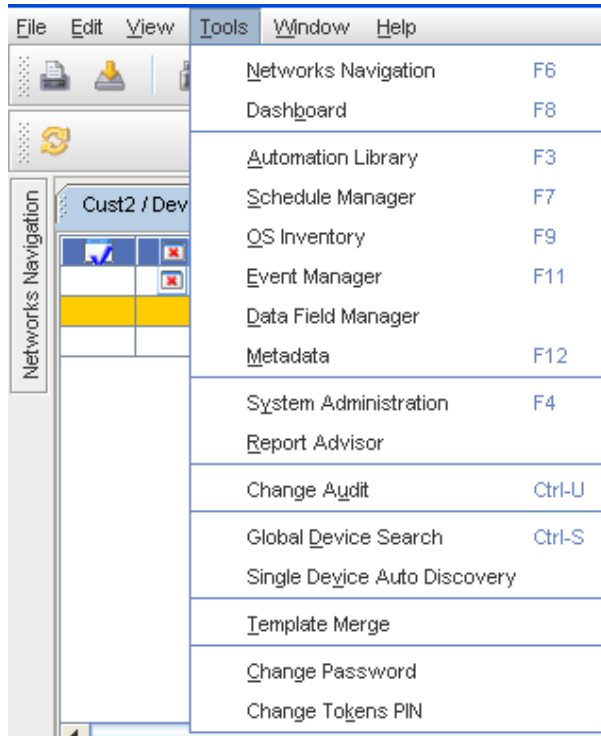
The OS Manager supports the upgrade of Cisco IOS images through the Job Scheduler.

OS images continue to be maintained on your image server. The OS Manager stores information about each image, and how to access the images. The supported image access methods include FTP and TFTP.

The **OS Image Inventory** window displays the current listing of your OS inventory, including the Name, OS Version, Device Class, Model number, Type, and Location of all inventory. This window is used as the OS Image Inventory Manager.

With the OS Inventory, you can verify network device OS details, or roll a new OS configuration.

The **OS Inventory** window can be accessed on the menu bar. Access **Tools -> OS Inventory**.



The OS Inventory window opens. To display the full range of items that can be included within columns, click within the column heading, and then select from the column listing. See [Displaying Columns in the OS Image Inventory](#) for more information.

This window is where you begin to complete OS Inventory tasks, including:

- [Adding OS \(Image\) Inventory](#)
- [Updating OS Images](#)
- [Copying OS \(Image\) Inventory](#)
- [Editing OS \(Image\) Inventory](#)
- [Deleting OS Image Inventory from the List](#)
- [Filtering the OS Inventory List](#)
- [Printing OS \(Image\) Inventory](#)
- [Exporting Inventory Information from the OS Inventory Listing](#)
- [Displaying Columns in the OS Image Inventory](#)

## Adding OS (Image) Inventory

The OS Inventory window displays the current listing of your OS Images, including the Name, OS Version, Device Class, Model number, Type and Location of the inventory.


The OS Inventory window can be accessed by completing this step.

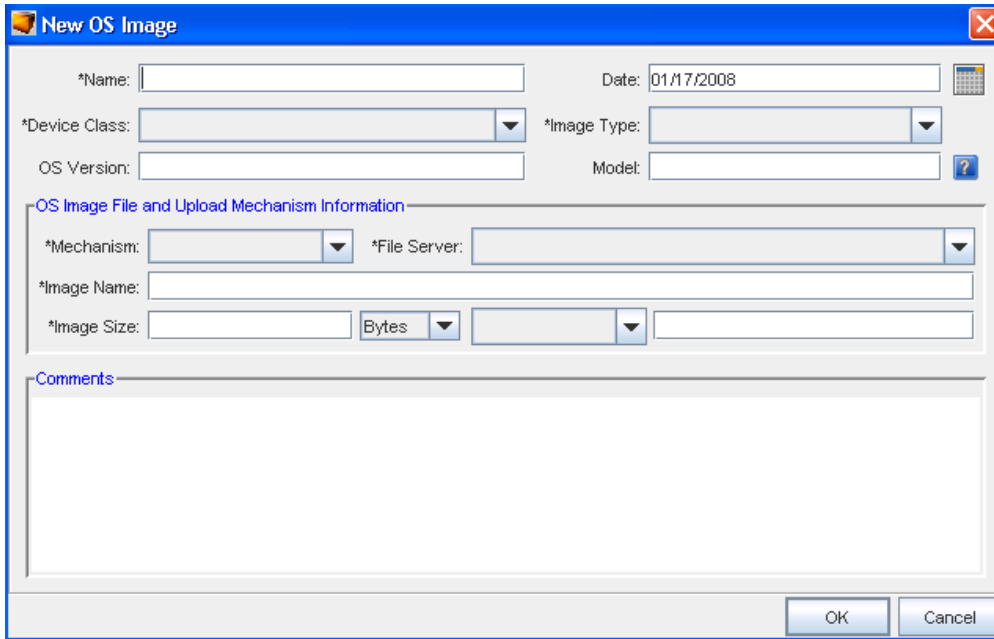
- 1 On the menu bar access **Tools -> OS Inventory**.

Tools Window Help	
Networks Navigation	F6
Dashboard	F8
Automation Library	F3
Schedule Manager	F7
OS Inventory	F9
Event Manager	F11
Data Field Manager	
Metadata	F12
System Administration	F4
EMC M&R	
Change Audit	Ctrl-U
Global Device Search	Ctrl-S
Single Device Auto Discovery	
Template Merge	
Change Password	
Change RSA Tokens PIN	

The OS Inventory window displays.

Name	Type	OS Version	Device Class	Model	File Server	Mechanism
Boss Image	OS Image	3.1.6.2	Nortel BoSS Switch	Business Policy Switch 2000	Dennis TFTP Server	TFTP
350/450	Firmware Image	301	Nortel Baystack	350/450	Dennis TFTP Server	TFTP
Baystack 450 FW image	Firmware Image	4.4.1.1	Nortel Baystack	BayStack 450-24T	Dennis FTP Server	FTP
Baystack 450 SW image	Software Image	4.4.1.1	Nortel Baystack	BayStack 450-24T	Dennis FTP Server	FTP
cisco2600	OS Image-IOS	12.19	Cisco IOS Router	2600	Dennis TFTP Server	TFTP
ciscoiosrouter	OS Image-IOS	12.29	Cisco IOS Router	3640	Dennis TFTP Server	TFTP
HP5314	OS Flash Image	10.02	HP Procurve Switch	5314	Dennis TFTP Server	TFTP
tasman1001	OS Image	1002	Tasman Router		Dennis TFTP Server	TFTP
tasman1450	Interface Image		Tasman Router		Dennis TFTP Server	TFTP
tasman1450-2	OS Image		Tasman Router		Dennis TFTP Server	TFTP

- Click the **New** icon  to go to the OS Image window, and enter information into the fields to create a new OS Image.



- At the New OS Image window, enter information into at least the fields that are marked with an asterisk (\*).

When you are creating a new OS Image, the following fields can be used for defining the OS Image information.

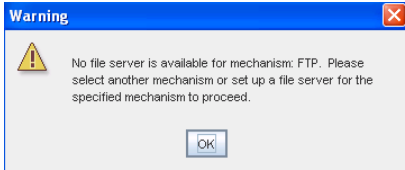
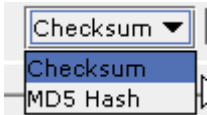
#### New OS Image - Fields and Descriptions

- Click **Ok** when you have completed all the fields to add this new Inventory to the OS Image Inventory listing.

Field	Description
Name	The Name of the OS Image. This can be any name you choose.
Date	You can select a <b>date</b> (when to upgrade the OS Image) using the calendar.
Device Class	From this listing (using the drop-down arrow) you can select the appropriate <b>Device Class</b> . This listing includes <b>all device classes supporting OS Image upgrades</b> . See the Network Configuration Manager Installation Guides for more information.
Image Type	Make a selection from the drop-down arrow listing. Some device classes may have more than one type (for example, the Cisco IOS Device Class has more than one type of image).
OS Version	This is the actual <b>version number</b> of the OS Image.
Model	This is the valid model number of the <b>device</b> that can use this image, and can support Regular Expressions. Click the question mark to see the RegEx choices.



OS Image File and Upload Mechanism Information

Mechanism	<p>Select the Mechanism from the available options shown in the drop-down arrow list. If the File Server is not present, the following message displays.</p>  <p>Click <b>Ok</b> to continue.</p>
File Server	Select the File Server from the drop-down listing.
Image Name	Enter an appropriate Image Name.
Image Size	Enter the Image Size, and select either Bytes, KB or MB from the Bytes drop-down arrow list.
Checksum	<p>You can use the drop-down arrow in this field to make a selection.</p>  <p><b>Note:</b> This field may not be displayed for all Device Classes. Currently, this field is only available for CISCO IOS Routers and CISCO IOS Switches.</p> <p>After making your selection, you must enter the Checksum or MD5 Hash for the OS image. The vendor's web site should supply you with this information.</p>
Comments	Here you can enter any comments that you think are needed to provide <b>additional information</b> on this image.

## Copying OS (Image) Inventory

The OS Inventory window displays the current listing of your OS Images, including the Name, OS Version, Device Class, Model number, Type, and Location of the inventory. To include new inventory (that is an exact match for existing inventory) you can use the Copy feature.

**Important** You must have previously defined a **File Server**.

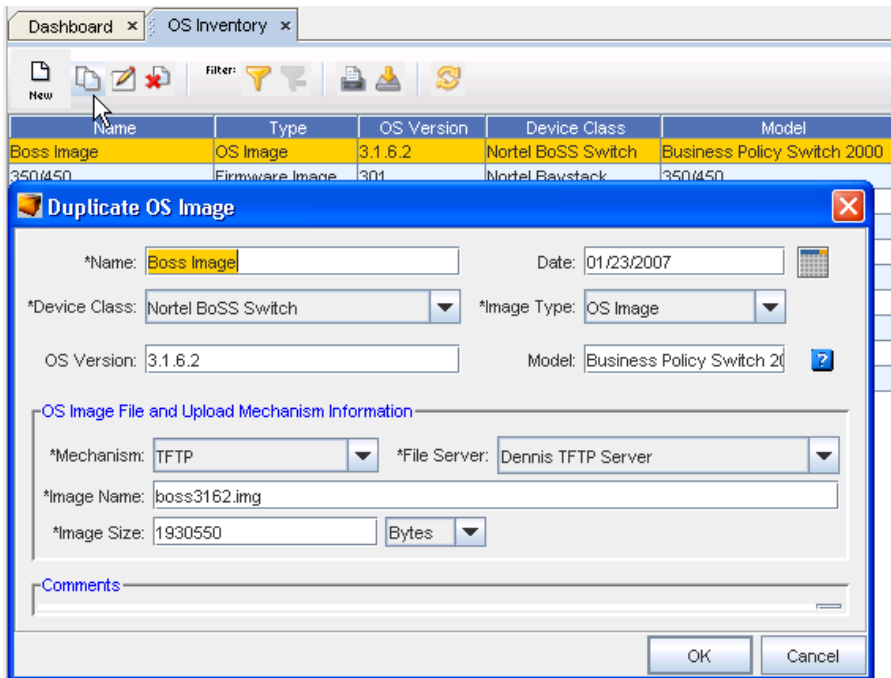
To copy existing OS Inventory,

The OS Inventory window can be accessed:

- 1 On the menu bar access **Tools -> OS Inventory**. The OS Inventory window appears.

Tools Window Help	
Networks Navigation	F6
Dashboard	F8
Automation Library	F3
Schedule Manager	F7
OS Inventory	F9
Event Manager	F11
Data Field Manager	
Metadata	F12
System Administration	F4
EMC M&R	
Change Audit	Ctrl-U
Global Device Search	Ctrl-S
Single Device Auto Discovery	
Template Merge	
Change Password	
Change RSA Tokens PIN	

- 2 Select the OS Images you want to use as a "copy" to add additional OS Images. This is a quick way to create images containing similar information.



- 3 Click the **Copy** icon on the tool bar. The Duplicate OS Image window opens.

- 4 Enter or change any existing information, and be sure to use a **new name** for this copy of the images. If you attempt to keep the same name, a warning message displays reminding you to use a new name. Click **OK** at the message to continue.
- 5 To make changes to the newly created copy, use the [Editing OS \(Image\) Inventory](#) icon.

## Editing OS (Image) Inventory

The OS Inventory window displays the current list of your OS Images, including the Name, OS Version, Device Class, Model number, Type and Location of the inventory.


To display the full range of items that can be included within columns, click the **column icon** and select from the column listing. See [Displaying Columns in the OS Image Inventory](#) for more information.

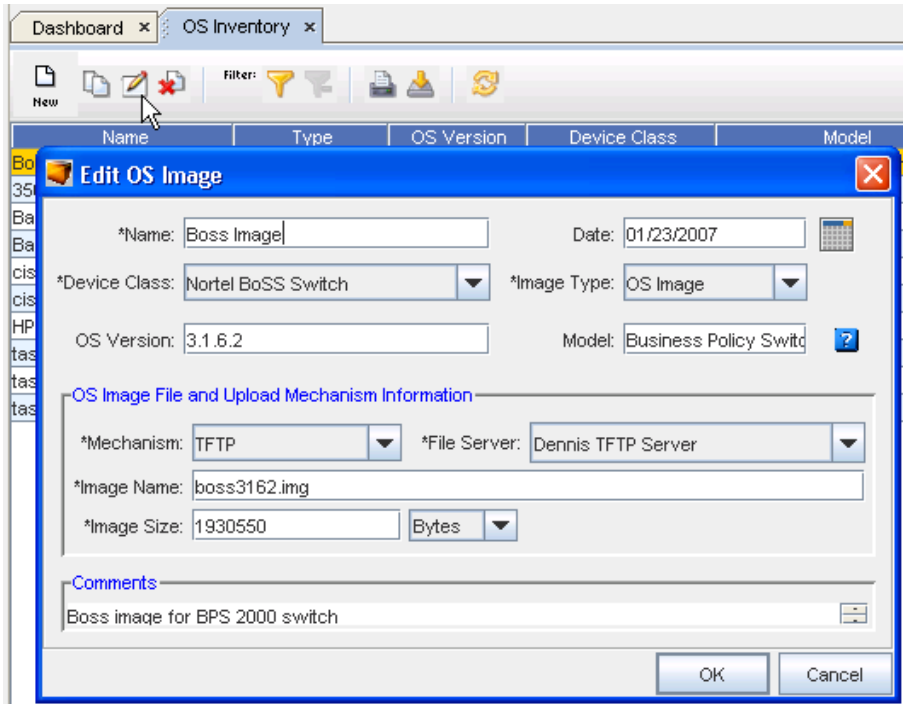
The OS Inventory window can be accessed:

- 1 On the menu bar access **Tools** -> OS Inventory.



The **OS Inventory** window displays.

- 2 Select the item you want to edit from the list of existing images, and click the **Edit** icon  . The Edit OS Image window displays. To see a listing of the fields and their descriptions, go to [Adding OS \(Image\) Inventory](#).

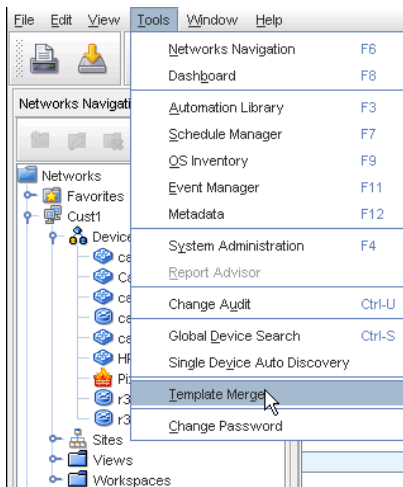


- 3 In this window, make the necessary changes to the existing information.
- 4 Click **OK** to save your changes.

To edit OS Image Inventory,

## Printing OS (Image) Inventory

- 1 To access the OS Inventory window, on the menu bar access **Tools -> OS Inventory** .



The **OS Inventory** window displays.

- 2 From the OS Inventory window, select the image data you want to print, then click the **Print**

icon  in the tool bar.

Name	Type	Version	Device Class	Model
Boss Image	OS Image	3.1.6.2	Nortel BoSS Switch	Business Policy Switch 2000
350/450	Firmware Image	301	Nortel Baystack	350/450
Baystack 450 FW image	Firmware Image	4.4.1.1	Nortel Baystack	BayStack 450-24T
Baystack 450 SW image	Software Image	4.4.1.1	Nortel Baystack	BayStack 450-24T
cisco2600	OS Image-IOS	12.19	Cisco IOS Router	2600
ciscoiosrouter	OS Image-IOS	12.29	Cisco IOS Router	3640
HP5314	OS Flash Image	10.02	HP Procurve Switch	5314
tasman1001	OS Image	1002	Tasman Router	
tasman1450	Interface Image		Tasman Router	
tasman1450-2	OS Image		Tasman Router	

3 At your browser's Print menu, make your selections, then click **OK**.

To print OS Inventory,

## Deleting OS Image Inventory from the List

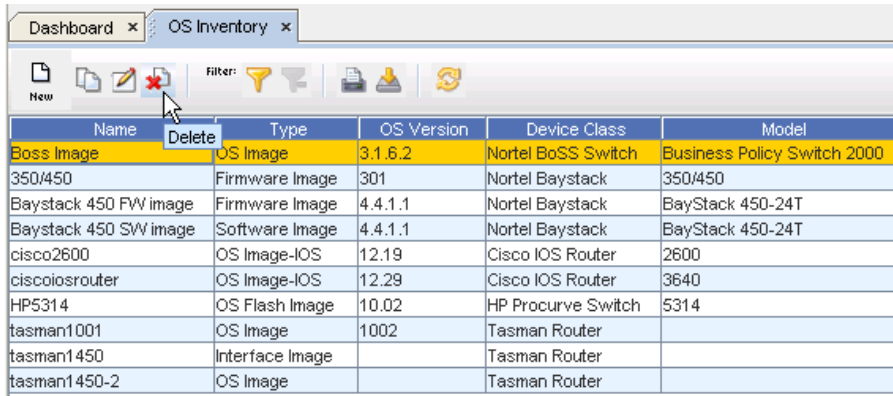
The OS Inventory window displays the current listing of your OS images, including the Name, OS Version, Device Class, Model number, Type and Location of the image.

1 To access the OS Inventory window, on the menu bar access **Tools -> OS Inventory** .

Tools	Window	Help
Networks Navigation	F6	
Dashboard	F8	
Automation Library	F3	
Schedule Manager	F7	
<b>OS Inventory</b>	<b>F9</b>	
Event Manager	F11	
Data Field Manager		
Metadata	F12	
System Administration	F4	
EMC M&R		
Change Audit	Ctrl-U	
Global Device Search	Ctrl-S	
Single Device Auto Discovery		
Template Merge		
Change Password		
Change RSA Tokens PIN		

The **OS Inventory** window displays.

2 Select the inventory you want to delete.



- 3 Select the **Delete** icon on the tool bar.
- 4 At the confirmation message, click **Yes**. The image is now permanently deleted from your OS Inventory listing.

To Delete existing OS Image Inventory from the list,

## Exporting Inventory Information from the OS Inventory Listing

The OS Inventory window displays the current listing of your OS inventory, including the Name, OS Version, Device Class, Model number, Type and Location of the inventory.

- 1 To access the OS Inventory window, on the menu bar access **Tools -> OS Inventory** .



- The **OS Inventory** window displays.
- To Export OS Inventory information from the list,

Name	Type	Version	Device Class	Model
Boss Image	OS Image		Nortel BoSS Switch	Business Policy Switch 2000
350/450	Firmware Image	301	Nortel Baystack	350/450
Baystack 450 FW image	Firmware Image	4.4.1.1	Nortel Baystack	BayStack 450-24T
Baystack 450 SW image	Software Image	4.4.1.1	Nortel Baystack	BayStack 450-24T
cisco2600	OS Image-IOS	12.19	Cisco IOS Router	2600
ciscoiosrouter	OS Image-IOS	12.29	Cisco IOS Router	3640
HP5314	OS Flash Image	10.02	HP Procurve Switch	5314
tasman1001	OS Image	1002	Tasman Router	
tasman1450	Interface Image		Tasman Router	
tasman1450-2	OS Image		Tasman Router	

The Save window displays.

## Filtering the OS Inventory List

The OS Inventory window displays the current listing of your OS inventory, including the Name, OS Version, Device Class, Model number, Type, and Location of the inventory.

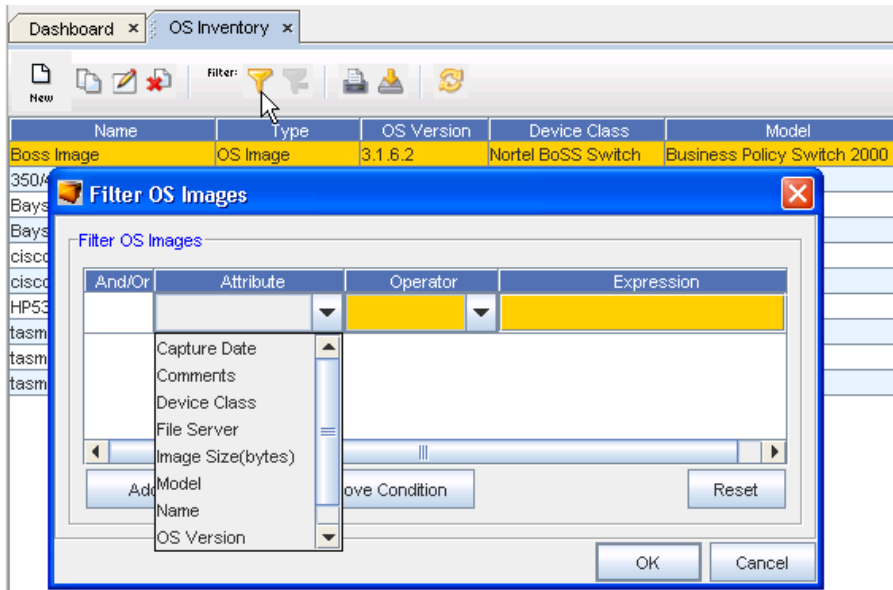
- 1 To access the OS Inventory window, on the menu bar access **Tools -> OS Inventory** .

Tools	Window	Help
Networks Navigation	F6	
Dashboard	F8	
Automation Library	F3	
Schedule Manager	F7	
OS Inventory	F9	
Event Manager	F11	
Data Field Manager		
Metadata	F12	
System Administration	F4	
EMC M&R		
Change Audit	Ctrl-U	
Global Device Search	Ctrl-S	
Single Device Auto Discovery		
Template Merge		
Change Password		
Change RSA Tokens PIN		

The OS Inventory window displays.

- 2 Click the **Apply** icon in the Filter section of the menu bar. The Filter OS Image window displays.
- 3 To clear existing filtering criteria from the fields, click **Reset**, then, click **Yes** at the confirm window to remove the existing filtering selections.

- To use the filtering criteria for the first time, click the **Add Condition** button.



- Enter or Select the filter criteria:
  - Enter **And** or enter **Or** (in the first column) .
  - Using the drop-down arrows, select the **Attribute** and **Operator** criteria.
  - Click the ellipses ( ...) in the **Expression** field to make a selection from the drop-down list.
- Click **OK** when you have made your filtering selections. You can remove any existing conditions by first selecting the condition, and then clicking the **Remove Conditions** button. You can now select new conditions for filtering.

To Filter the OS Inventory list,

---

**Note** At the OS Inventory window you can "un-apply" filters you have just applied by clicking the **Cancel** icon (located to the right of the **Apply** icon).

---

## Displaying Columns in the OS Image Inventory

The OS Inventory window displays the current listing of your OS inventory, including the Name, OS Version, Device Class, Model number, Type and Location of the inventory. To display other, additional available columns, use this procedure.

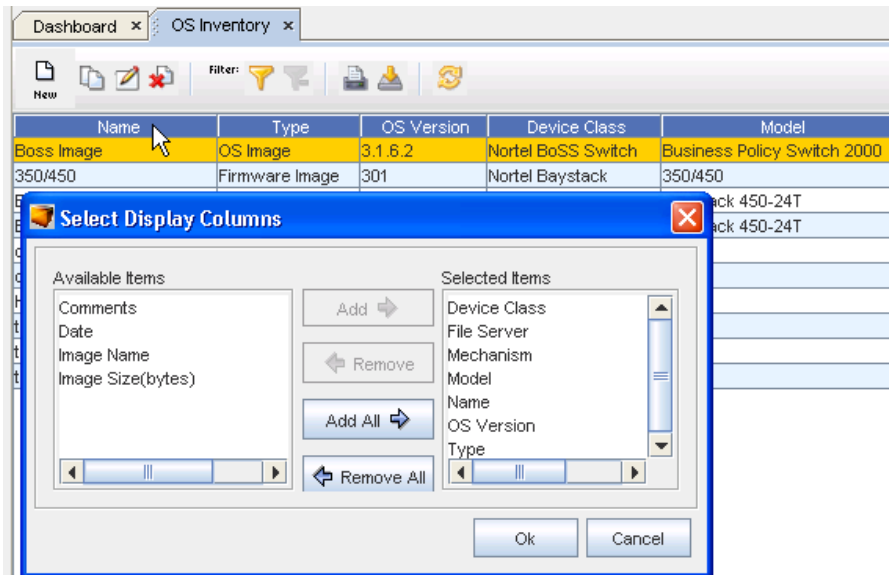
- To access the OS Inventory window, on the menu bar access **Tools -> OS Inventory** .



Tools Window Help	
Networks Navigation	F6
Dashboard	F8
Automation Library	F3
Schedule Manager	F7
OS Inventory	F9
Event Manager	F11
Data Field Manager	
Metadata	F12
System Administration	F4
EMC M&R	
Change Audit	Ctrl-U
Global Device Search	Ctrl-S
Single Device Auto Discovery	
Template Merge	
Change Password	
Change RSA Tokens PIN	

The **OS Inventory** window displays.

- 2 Click within the **column heading** (in this example, the Name column was selected) to display the Select Display Columns window.



- 3 From this window, you can either **Add** or **Remove** the columns you want displayed on the OS Inventory listing.

- 4 Use the right arrows to **Add** (move) the column headings from the **Available items** pane into the **Selected items** pane. Any column you have in the Selected Column pane indicates that information will be displayed in the OS Inventory listing. You can use the left arrows to **Remove** any columns you do not want displayed on the OS Inventory window.
- 5 Click **OK** when you have completed adding or removing column headings.

To select the columns you want to display,

## Managing Credentials

### Credential Manager Overview

Credential management permits the secure abstraction of User ID and Password pairs from those who use them. There are four credential types; Account, Community String, SNMPV3, and Privilege Password. Account credentials can consist of a User ID/Password pair and a Privilege Password reference.

Bulk load utilities permit the mass association and change of credential to devices, or from device properties and the right-click menu.

Credential associations show the devices that are currently assigned to each credential.

Additional internal auditing enhancements are now available allowing a System Administrator more insight into who is accessing devices, and what tasks are being completed within the system.

- As the System Administrator, you now have a method of dynamically controlling the credentials used for any device operation, as well as being offered the flexibility to deal with special and exception scenarios to manage certain devices.
- As a System Administrator, you can now determine if credentials are to be governed by Global Credential Configuration settings, or allow Credential Configurations at the Network level to override the Global Configuration settings.

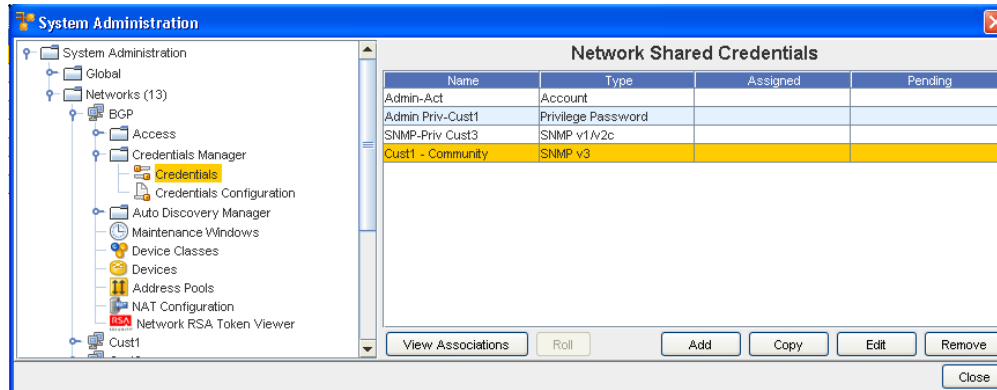
---

**Important** The Network credentials can override the Global configurations providing the user the ability to set Credential Policies for an individual Network.

---

The Credentials Manager has two options that you can view and work with:

- Credentials
- Credentials Configuration



From **Credentials** you can:

- View Associations
- Roll
- Add
- Copy
- Edit
- Remove

From **Credentials Configurations** you can select configuration options:

- Use Static Device Assignment
- Use Login Credentials
- Prompts User

## Credentials Best Practices

- Use credential management to specify how to secure your device communications.
- Use Credentials Configurations to determine the credentials that need to be used for communication with the devices.
- Manage credentials on a network or global basis, **not per device** . This allows you to make changes to a single credential, rather than make changes to each of many individual devices.
- If your Device Server and its devices are within a secured private network, then using unsecured protocols such as Telnet, FTP, and SNMP provides better overall performance and management ease, as well as better device coverage.
- If your Device Server and its devices are not within a single secured private network, then use credential management to disable non-secure protocols, and allow only secure protocols, such as SSH and SCP.

## When using SNMP Communications

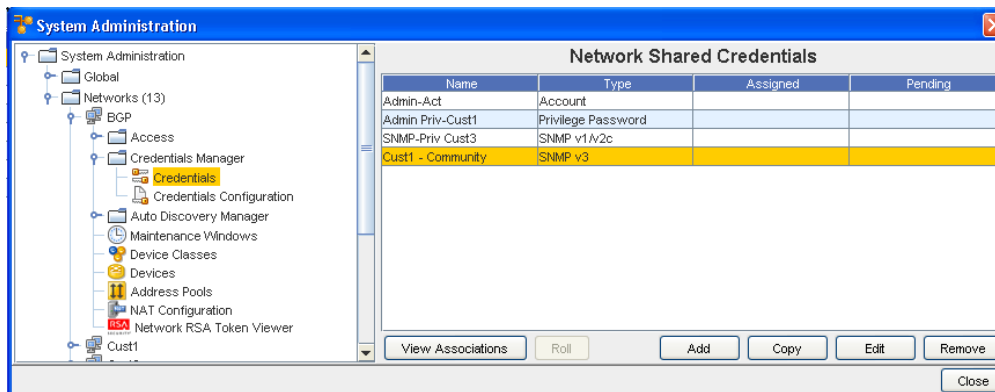
- Enabling SNMP communications provides the best overall quality of device information, with the greatest span of device coverage. The cost is a lower network security on traffic between the Device Servers and the monitored devices.
- Disabling SNMP communications gives you improved network security (by disabling non-secure SNMP traffic). The cost is having less device-specific information available, from a fewer number of device types. Information that is lost could include connection information, memory availability, and system information.

## Setting Network Level Credentials

To set credential access,

- 1 From the menu bar, access **Tools -> System Administration**.
- 2 In the navigation pane, select **Networks**.
- 3 Expand the Networks folder and select the appropriate **network**.
- 4 Expand the Network's folder, then select **Credentials Manager, and then Credentials**.

The Network Shared Credentials window appears similar to the following:

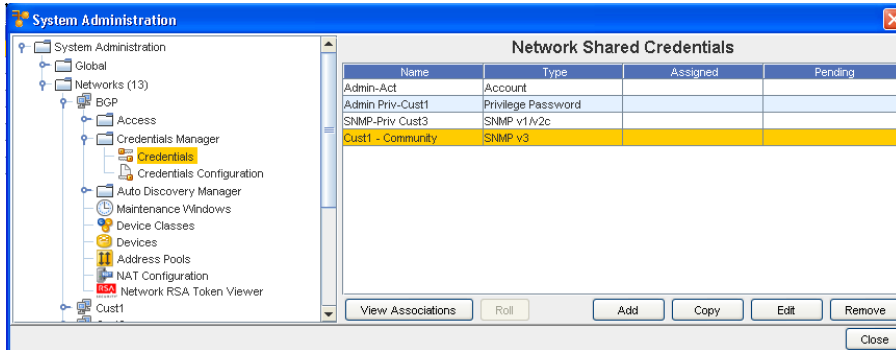


- 5 From here, you can **Add** a new credential, or if there are existing network credentials, you can complete the following actions:
  - [Viewing Network Credentials Associations](#) - to view the associations and review the Devices and the Auto Discovery information
  - [Rolling Credentials](#) - to go to the Roll Candidate Selection screen and select a candidate. Then go to the Credential Roll Job window to schedule the roll.
  - [Copying Network Shared Credentials](#) - to make an exact copy of this credential
  - [Adding Global Shared Credentials](#)- to add a credential
  - [Editing Network Credentials](#) - to make changes to existing information
  - [Remove Network Credentials](#) - to remove (delete) the credentials
  - **Close** - to leave this window

## Viewing Network Credentials Associations

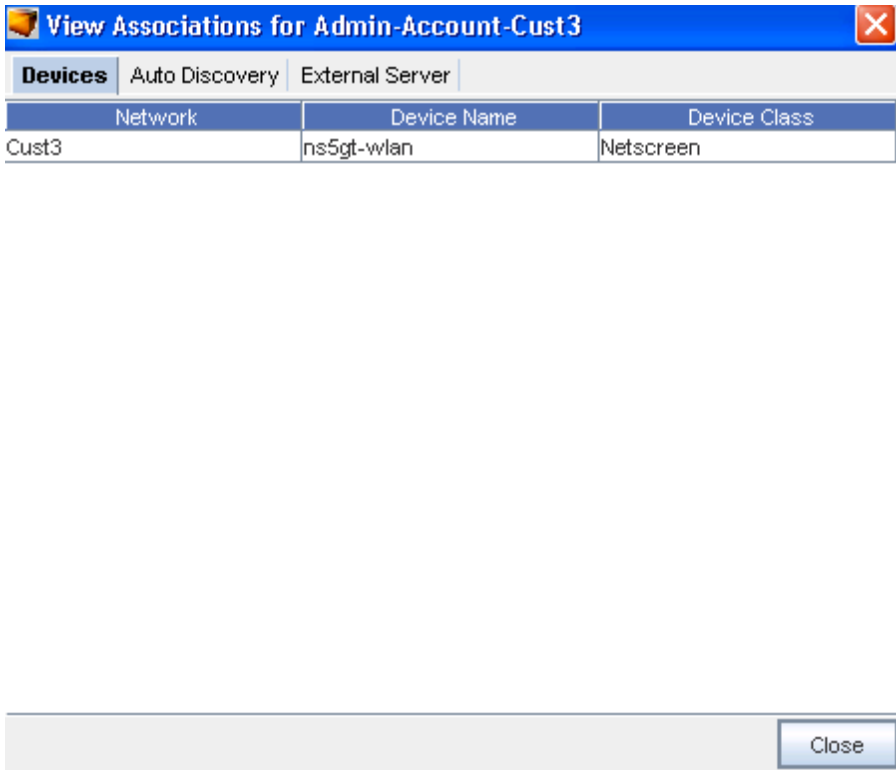
Credential management is provided at the Network level, as well as at the Global level. Network credentials are only available for devices within that specific Network. There is only one credential set used for a device, which can be associated from the list of Network or Global credentials. When assigning credentials, both Network and Global credentials are available in the credential window.

When using the **Network Shared Credentials** window, you can select to complete tasks using the option buttons located at the bottom of the window.



These options include **View Associations**, Roll, Add, Edit, Copy, Remove, and Close.

When you select to **View Associations**, you go to the View Associations window for the Name and Account you selected.



From this View Associations window you can see the:

- Network, Device and Device Class information for that account from the **Devices** tab
- Network, Name and Type from the **Auto Discovery** tab.
- Server Name and Server Type from the **External Server** tab.

---

**Note** After reviewing the information contained within each tab, click **Close** to close this window and return to the Network Shared Credential window.

---

## Rolling Credentials

To simplify account and password updates, credentials can be rolled within Network Configuration Manager. Rolling credentials updates all devices associated with one credential to the login and passwords on a second credential. You can roll credential information for devices, as well as create a job to update the devices configurations with the new login and password.

When using the **Network Shared Credentials** window, you can select to complete tasks using the option buttons located at the bottom of the window.

Using **Roll**, you can now:

- Select to roll from one credential to another credential
- Manage credentials on devices
- View a history of the credentials and their devices

These options include View Associations, **Roll**, Add, Edit, Remove and Close.

When you select **Roll**, you go to the Roll Candidate Selection, where you can select the Account you want to assign. Using Roll allows you to assign the Account before it is actually scheduled. Once scheduled, the status changes from Assigned to Pending until the scheduled job is run.

You can select to **Roll** from one credential to another credential.

- 1 Click the **Account** name (one or more) in the Roll Candidate Selection window to assign, then click **Ok**.
- 2 At the Credential Roll Job window, make your selections, and complete the information contained within the [Using the Schedule Tab](#) and [Using the Notification Tab to Send an Email](#) tabs. You must also complete and make selections in the **Schedule Job** section.

- 3 Click the appropriate action to **Approve and Submit** or **Submit**.

## Viewing the Credentials Roll Out Log

- 1 In a telnet window, verify your command results by entering change directory ( **cd** ) to **\$VOYENCE\_HOME / logs**, then pressing **Enter**. The log file to review is **credential-rollout.log**.
- 2 You can also go to the System Administrator **Credential** screen in Network Configuration Manager to verify that the credentials on the devices have been changed (rolled).

## Adding Network Shared Credentials

There are five classes of Shared Credentials:

- Account
- Privilege password
- SNMP V1/V2c
- SNMP v3
- RSA

---

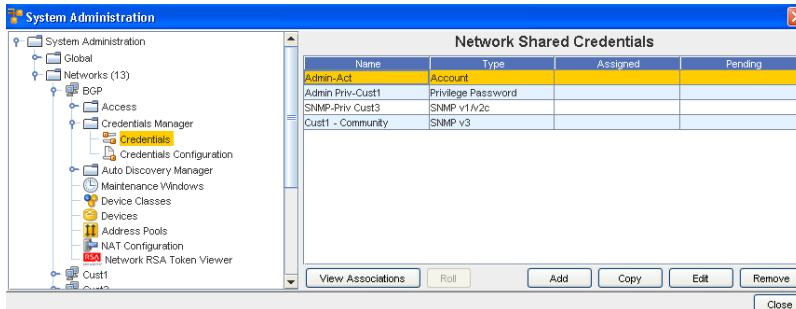
**Note** To import credentials in bulk, see [Using the Command Line Interface](#) for more information.

---

## Creating Shared Credential - Account Class

To Create a shared credential with the class type of Account, follow these steps:

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Credentials**.



The **Network Shared Credentials** window displays, with a listing of pre-assigned, shared credentials.

At the bottom of the window are the View Associations, Roll, Add, Copy, Edit, and Remove buttons, along with the Close option.

- 3 Click **Add** to display the Add Credential window.
- 4 Enter the **Credential Name** .



- 5 From the **Credential Type** section, select **Account** type from the options shown (using the drop-down arrow to display your selection).

**Important** Depending on the credential type you select, additional information is displayed in the lower portion of the window. For example, when you select Account as the credential type, additional fields display where you enter information. See [Unique Credentials](#) for more

information.

- 6 Complete the following steps:
  - Enter the **User Name** .
  - Enter a **Password**. Confirm the Password.
  - Select the check box if this account is managed by an external authentication server.
- 7 Click **OK** when you have completed these steps.

### Creating Shared Credential - Privilege Password Class

With the **Network Shared Credentials** window displayed showing a listing of pre-assigned, shared credentials:

- 1 Click **Add** to display the Add Credential window.
- 2 Enter the **Credential Name**.
- 3 From the **Credential Type** section, select **Privilege Password** from the options shown (using the drop-down arrow). See [Unique Credentials](#) for more information.

- 4 Enter a **Password**. Confirm the Password you just entered. **Note:** You can also click the **Secure** check box, then click **Generate** to have the application generate a system-only-known password.
- 5 Click **OK** when you have completed these steps.

#### Creating Shared Credential - SNMP v1/v2c

With the **Network Shared Credentials** window displayed showing a listing of pre-assigned, shared credentials:

- 1 Click **Add** to display the Add Credential window.
- 2 Enter the **Credential Name**.
- 3 From the **Credential Type** section, select **SNMP v1/v2c** from the options shown (using the drop-down arrow). See [Unique Credentials](#) for more information.
- 4 Complete the following steps for the **Read-Only** section:
  - Enter the Community String.
  - Confirm the Community String entered.
- 5 Complete the following steps for the **Read-Write** section:
  - Enter the Community String.
  - Confirm the Community String entered.
- 6 Click **OK** when you have completed these steps.

**Add Credential**

\*Credential Name:

Credential Type:

Voyence Unique Credentials    Length:

**Read-Only**

\*Community String:

\*Confirm Community String:

**Read-Write**

Community String:

Confirm Community String:

### Creating Shared Credential - SNMP v3

With the **Network Shared Credentials** window displayed showing a listing of pre-assigned, shared credentials:

- 1 Click **Add** to display the Add Credential window.
- 2 Enter the **Credential Name**.
- 3 From the **Credential Type** section, select **SNMP v3** from the options shown (using the drop-down arrow). See [Unique Credentials](#) for more information.

The screenshot shows the 'Add Credential' dialog box with the following fields and options:

- \*Credential Name: [Text Input]
- Credential Type: **SNMP v3** (Dropdown)
- Voyence Unique Credentials Length: [Text Input]
- Security** Context (Tabbed)
- \*User Name: [Text Input]
- Security Level: **AUTH\_PRIV** (Dropdown)
- Authentication Protocol: **HMACMD5** (Dropdown)
- Privacy Protocol: **DES** (Dropdown)
- \*Authentication Password: [Text Input]
- \*Reenter Auth. Password: [Text Input]
- \*Privacy Password: [Text Input]
- \*Reenter Privacy Password: [Text Input]
- Generate... (Button)
- OK (Button) Cancel (Button)

When **SNMP v3** is selected as the Credential Type, the information you need to select and enter is divided between two tabs; **Security** and **Context**.

- From the **Security** tab, complete the following steps:
- Enter a User Name
- From the drop-down arrow, select Security Level. Depending on the Security Level you select, Authentication Protocol and Privacy Protocol may not be selectable.
- From the drop-down arrow, select a Authentication Protocol (if appropriate).
- From the drop-down arrow, select a Privacy Protocol (if appropriate).

---

**Note** You can select **AES192W3DESKEYExt** and **AES256W3DESKEYExt** protocols, only for the Cisco specific device(s).

---

- Enter an Authentication Password, then re-enter the password once again.
- Enter a Privacy Password, then re-enter the password once again. Note that you can click Generate to have Voyence create passwords for you.
- Once your passwords are verified, click **Ok**.

The screenshot shows a dialog box titled "Security" with a "Context" tab selected. The dialog contains several input fields and a dropdown menu:

- Context Name: [Text Input]
- Context Engine ID: [Text Input]
- User Group Name: [Text Input]
- View Name: [Text Input]
- View Access: [Dropdown Menu] (Currently set to WRITE)
- Included MIBs/OIDs: [Text Input]
- Excluded MIBs/OIDs: [Text Input]

At the bottom of the dialog, there is a "Generate..." button. Below the dialog box, there are "OK" and "Cancel" buttons.

---

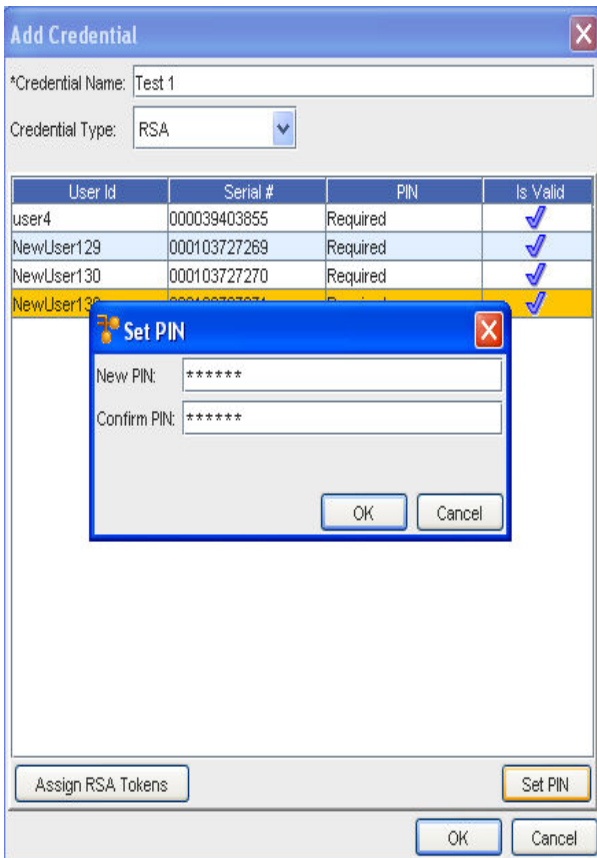
**Note** MIBs refer to **Management Information Bases** , and OIDs refer to **Object Identifiers** .

---

- From the **Context** tab, complete the following steps:
- Enter the Context Name.
- Enter the Context Engine ID.
- Enter a User Group Name.
- Enter a View Name.
- Select a View Access from the drop-down arrow.
- Enter the MIBs/OIDs you want included.
- Enter the MIBs/OIDs you want to be excluded from these credentials.
- Click **Ok** to keep your selections.

### Setting RSA Token PINs

- 1 From the list of RSA tokens, select an **RSA token**. RSA tokens that have not had the PIN set, show as Required under the PIN column.
- 2 At the bottom of the Manage RSA Tokens pane, select **Set PIN** . The Set PIN window (for the user you selected) now opens.



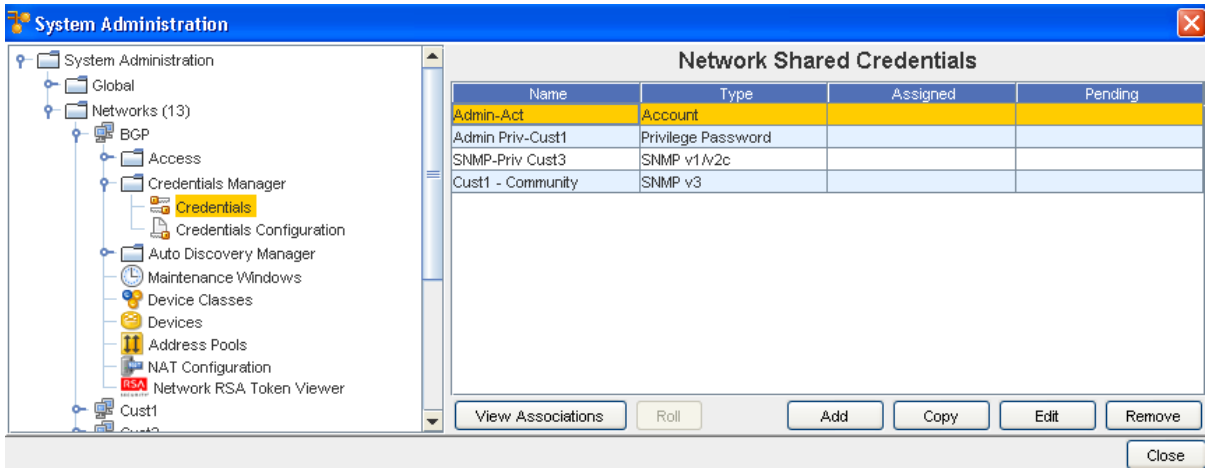
- 3 At the Set PIN screen, enter a **valid PIN** in the New PIN field.
- 4 Enter the PIN again in the **Confirm PIN** field.
- 5 Click **Ok**.

## Copying Network Shared Credentials

### Creating Shared Credential - Account Class

To Copy a shared credential with the class type of Account, follow these steps:

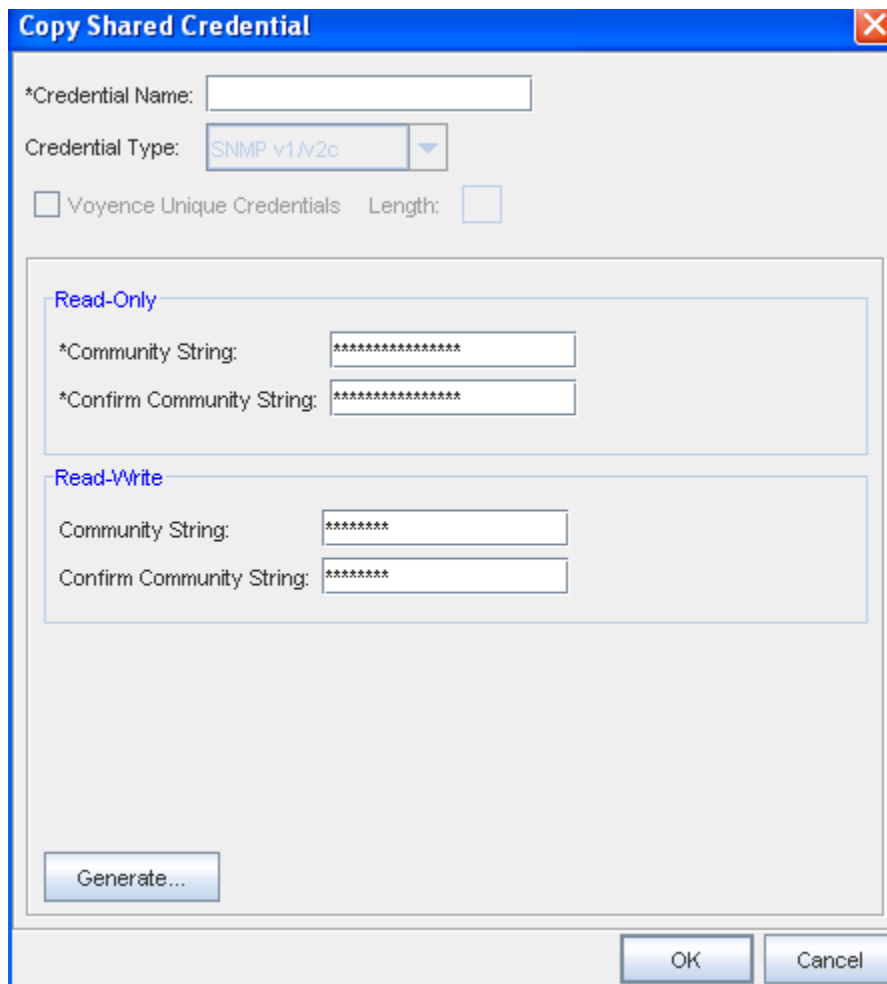
- 1 From the menu bar, select **Tools -> System Administration**.



The **Network** Shared Credentials window displays, with a listing of pre-assigned, shared credentials.

At the bottom of the window are the View Associations, Roll, Add, Copy, Edit, and Remove buttons, along with the Close option.

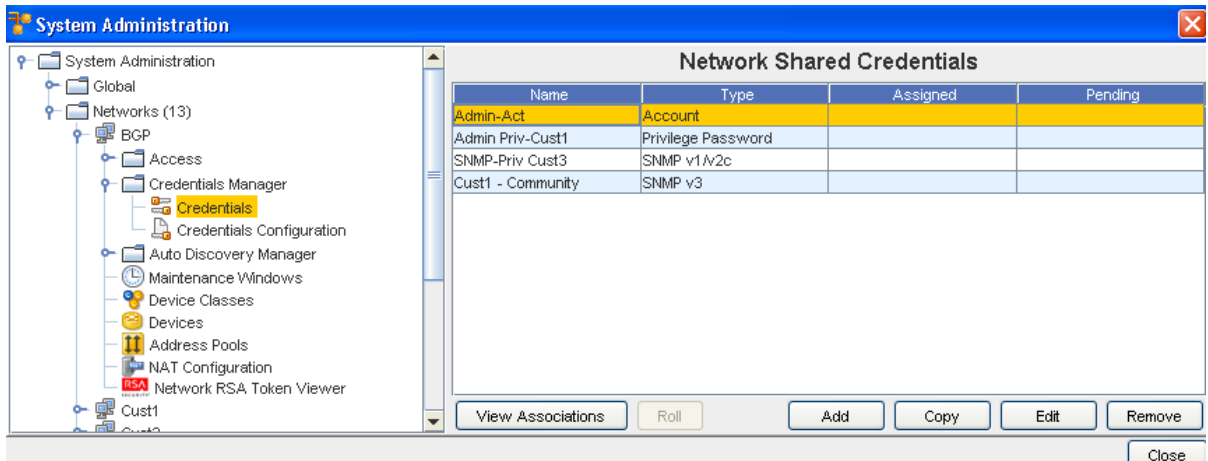
- 2 Click **Copy** to display the Copy Credential window.
- 3 Enter the **Credential Name** .
- 4 Click **Ok**. Now, the copy of the Credential you selected is now in the list of Network Shared Credentials.



## Editing Network Credentials

To edit Network Shared Credentials,

- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Credentials**.





The **Network Shared Credentials** window displays, with a listing of pre-assigned, shared credentials.

- 3 Select a credential from the list, then click **Edit** to display the Edit Shared Credential window.
- 4 Make any changes to the existing information, based on the Credential Type you selected when you created the credential.
- 5 Click **OK** to save your edits.

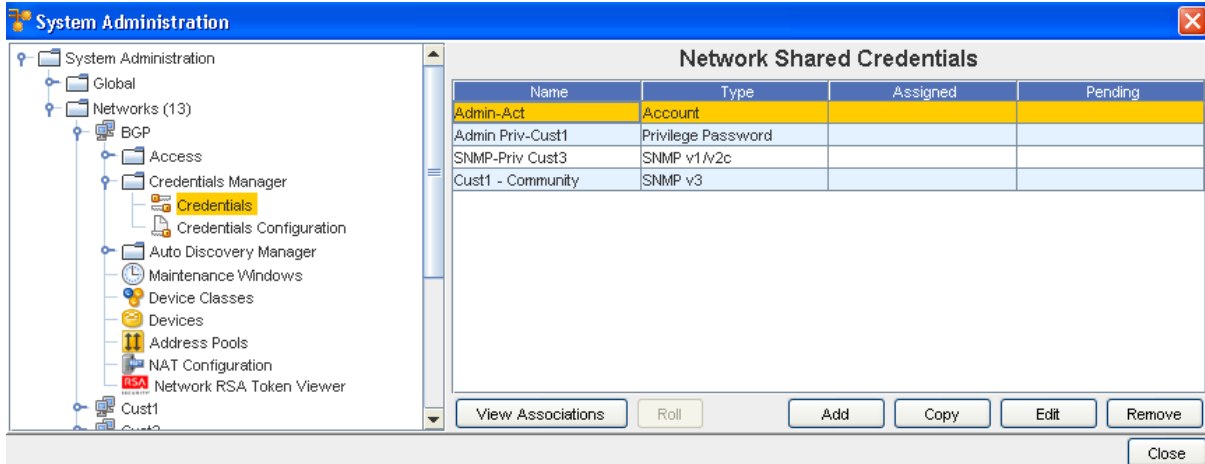
#### Notes:

- The updating credentials process requires that an account be associated with a device. This account is used to establish the initial session into the device to make the credential updates.
- This manual process creates an association with the credential and the local device to represent the username/password that is present on the device.
- If an Autodiscovery is made with an established account credential, the manual process of association is not required. The Communication tab on a device contains the account association for the Primary In-Band mechanism.

## Remove Network Credentials

To remove Network Shared Credentials,

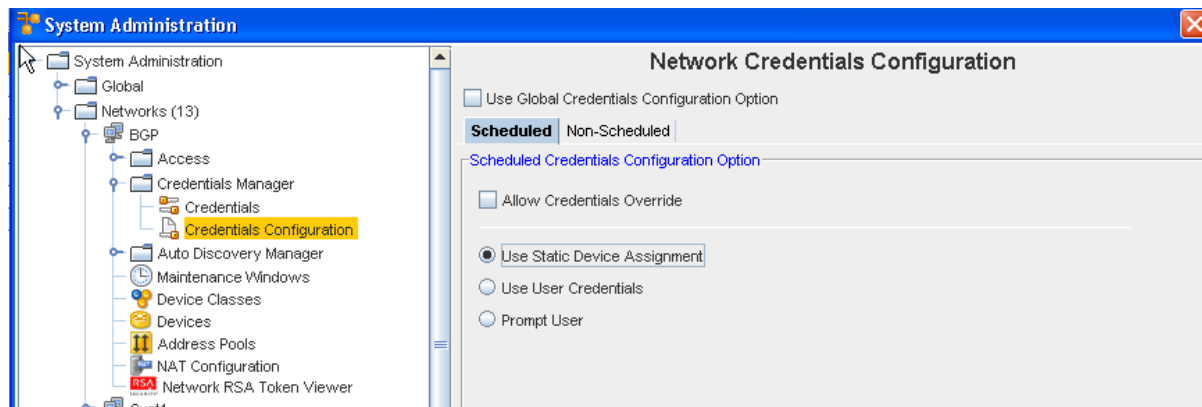
- 1 From the menu bar, select **Tools -> System Administration**.
- 2 Next, select **Network -> Credentials**.
- 3 The **Network Shared Credentials** window displays, with a listing of pre-assigned, shared credentials.



- 4 Select the Network you want removed, then click the **Remove** button.
- 5 Select **Yes** at the confirmation message.

## Using Network Credentials Configuration

Access to the Credentials Configuration is through the **Credentials Manager**.



### At the Network Credentials Configuration Level

At this level, you are provided the options to determine the credentials that need to be used for communication with the device. This includes scheduled jobs, as well as synchronous operations targeted on a device, such as cut-through, quick commands, and more.

- The **Scheduled** tab refers to the jobs that can be scheduled to run (with the exception of Auto Discovery and Pulls).

- The **Non-Scheduled** tab refers to those operations (Cut-Through, Quick Commands, and Save Commands, for example) that are not scheduled.

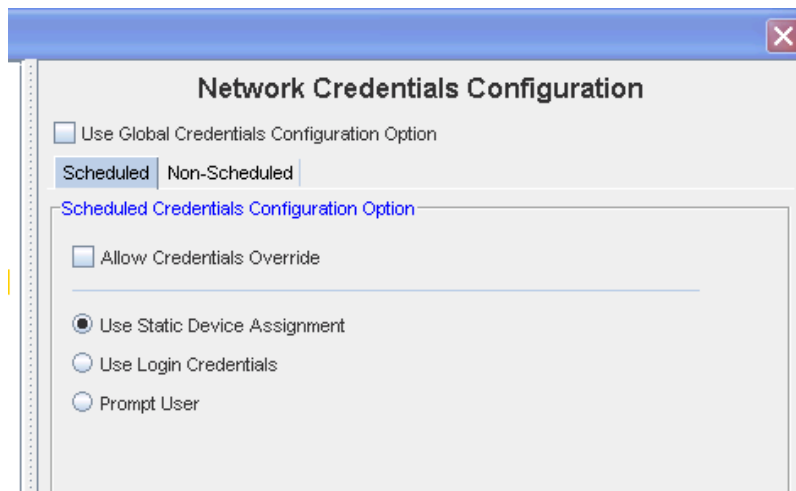
When the **Use Global Credentials Configuration Option** is not selected, your options can be selected from the Scheduled and Non Scheduled tabs. If selected, there are no other options available to you from these tabs.

You can select from the following options:

## The Scheduled Tab

### Users Static Device Assignment

- **Uses Static Device Assignment** - If Uses Static Device Assignment is selected- this indicates to the system to use the Shared Credentials assigned at the device level within a network. This is the default option.

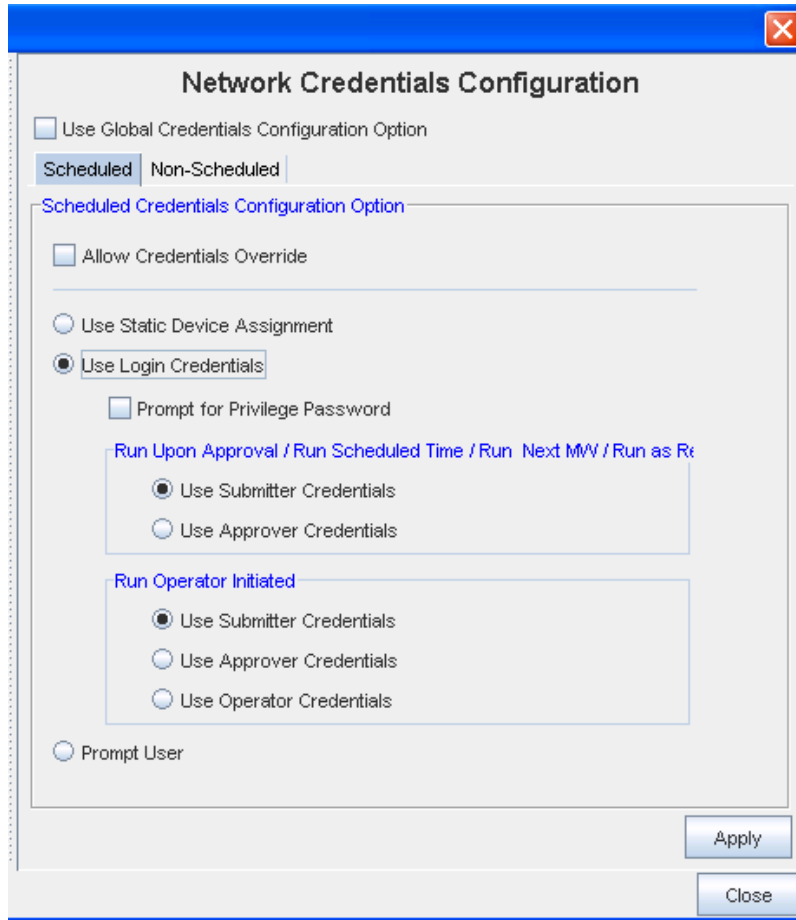


### Use Login Credentials

- **Use Login Credentials** - When **Use Login Credentials** is selected - this indicates to the system to use the user's application login account as the device credentials (the account name/account password).

You have the choice to select any of the options of when the user's are now prompted to enter account and password information before completing tasks.

- You can select to **Use the Global Credentials Configuration Option**
- You can also select to **Allow Credentials Override**



**Important** In some cases where a job may be scheduled in the future, the user's login credentials may need to be preserved until the job executes (to construct the device server request). These credentials must be discarded immediately after the task request is sent to the device server. You must pay attention to jobs with "Preserve Order" selected, as each task execution depends on the success of the previous task in the list (the credentials must be preserved until the last task executes).

- You can select to **Prompt for Privilege Password**

To determine whose credentials are to be used for jobs, the following options are available for each run option as applicable, **one** of which must be selected:

- **Use Submitter Credentials** – In case of scheduled operations, the system uses the submitter's credentials. This includes any job submission through "Submit" button on the scheduler.
- **Use Approver Credentials** – In case of jobs, the system uses the approver's credentials. This includes any job submission through –Approve&Submit– button on the scheduler or the "Approve" icon on the Schedule Manager.
- **Use Operator Credentials** (in case of jobs whose run option is "Run Operator Initiated") – In case of jobs, the system uses the credentials of the user attempting to manually execute the job.

In case of non-scheduled operations, the login credentials of the user executing the operation will be used and above options are redundant.

If Prompt User is selected from this window , see the following information.

### Prompt User

- **Prompts User** - When Prompts User is selected - this indicates to the system that the user is to be prompted for the credentials before the device operation , based on the following options: Account Password, and Privilege Password.

To determine whose prompts are to be used for jobs, the following options are available for each run option as applicable, **one** of which must be selected:

- Run on Approval
- Prompts on Submit - Prompts at the time the job is submitted for "Pending Approval"
- Prompts on Approval - Prompts at the time the job is Approved
- Run Operator Initiated
- Prompts on Submit - Prompts at the time the job is submitted for "Pending Approval"

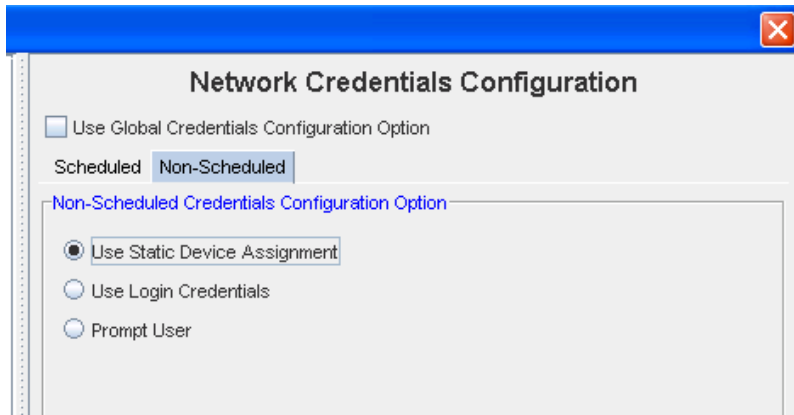
- Prompts on Approve - Prompts at the time the job is Approved
- Prompts on Manual Execute - Prompts at the time the job is manually executed.
- Run Scheduled Time / Run Next MW / Run as Recurring Series
- Prompts on Submit - Prompts at the time the job is submitted for "Pending Approval"
- Prompts on Approval - Prompts at the time the job is Approved

**Note** You also have the option of selecting **Invalidate Credentials on Job Modification** . If this is selected, after a job is **edited**, any credential associated with that job is now invalid.

- 1 After making your selections from the various options, click **Apply** to apply your credential choices.
- 2 Read the system message carefully to fully understand your selection to apply the changes you have made, then select **Yes to Continue**.
- 3 If applicable, click **Yes** at the Confirmation message.

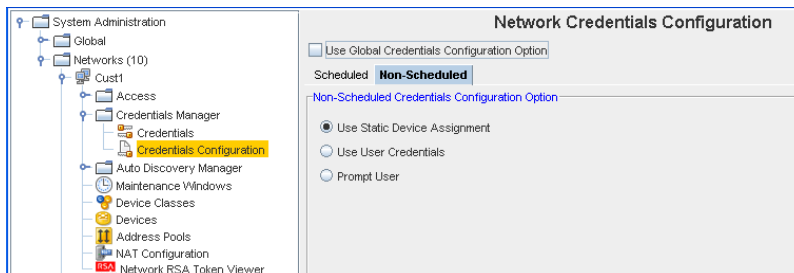
## The Non-Scheduled Tab

The **Non-Scheduled** tab refers to those operations (Cut-Through, Quick Commands, and Save Commands, for example) that are not scheduled to run.



## Users Static Device Assignment

- **Uses Static Device Assignment** - If Uses Static Device Assignment is selected- this indicates to the system to use the Network Shared Credentials assigned at the device level within a network. This is the default option.

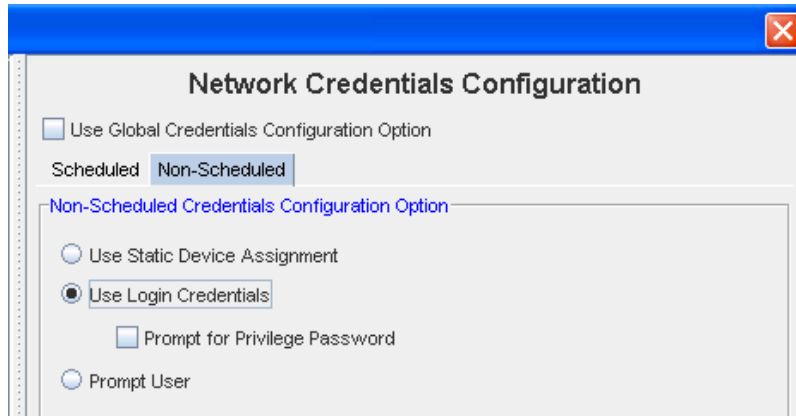


## Use Login Credentials

- **Use Login Credentials** - When **Use Login Credentials** is selected - this indicates to the system to use the user's application login account as the device credentials (the account name/account password).

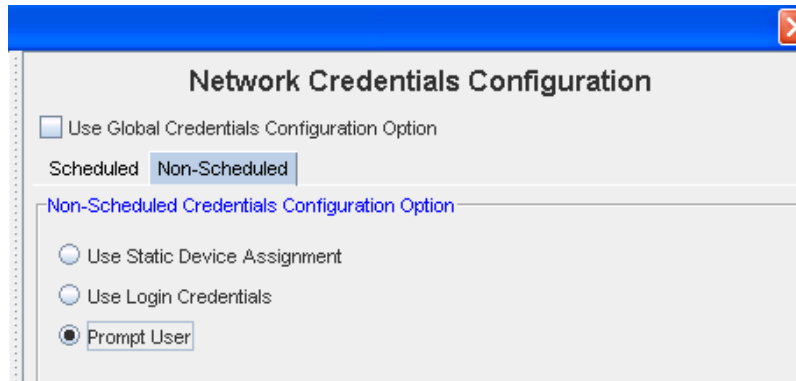
You can select to have the user prompted for their **Privilege Password** information before completing tasks.

- You can also select **Prompt User** from this window.



## Prompt User

**Prompt User** - When **Prompt User** is selected - this indicates to the system that the user is to be prompted for the credentials before the device operation , based on the following options: Account Password, and Privilege Password.



## Working with Update Credentials

### Update Credentials Overview

You can Update Credentials from the **Communication Tab** in the Device Properties.

State	Device Name	IP	Device Class	Model	OS Version	Last Updated	Co
	r1720.lab.voyen...	172.17.1.2	Cisco IOS Router	1720	12.0(7)T, BASIC...	02/12/2008 03:0...	
	cat4006.lab.voy...	172.18.5.6	Cisco CatOS S...	Catalyst 4006	8.4(7)	02/12/2008 03:3...	

Selected Devices: 1

Properties for Device: cat-3524.lab.voyence.com

**Properties** | History | Audit Trails | Jobs

General | Configuration | Operational | **Communication** | Baseline | Site | Comments | Attachments

Communications	
In-Band	
Management	
Account	
Admin-Account-Cust1	TELNET/FTP
SNMP	Port: 161
Cust1-CommunityString	SNMP v1
Cust1-CommunityString	SNMP v2 (Active)
Privilege Password	
Admin-Priv-Cust1	
Cut-Through	
Account	
Admin-Account-Cust1	TELNET
Privilege Password	

[Update Credentials](#)

For more information, see [Updating Credentials](#).



# Glossary - Terms and Definitions



This section details terms and acronyms you may encounter while using Network Configuration Manager.

## **Access authority**

A range of possible authority levels that control access to protected resources, tasks or views.

## **Access Control List**

A list associated with an object (resource, task or view) that identifies all users having access to the object and their access rights.

## **Access level**

The level of authority a user has while accessing a secured file or library.

## **Address Pool**

The Address pools allow you to setup flat address pools using Network Configuration Manager. The IP Addressing feature uses a flat topology, but it contains multiple blocks. These flat pools are only seen in the network for which they are created. The pools are then used in the Workspace, Sites and Views of the network.

## **Administrator (admin)**

The person responsible for administrative tasks such as access authorization and content management. Administrators can also grant levels of authority to users.

## **Alias**

An alternative name used instead of a primary name.

## **Angle bracket**

Either the left angle bracket (<) or the right angle bracket (>). In the portable character set, these characters are referred to by the names <less-than-sign> and <greater-than-sign>.

## **Application Programming Interface (API)**

An interface that allows an application program (written in a high-level language) to use specific data or functions of the operating system or another program.

## **Application server**

Software that handles communication with the client requesting an asset and queries of the Content Manager.

## **AS**

Application Server

Ascending sequence

The arrangement of data in order from the lowest value to the highest value, according to the rules for comparing data

## **Asynchronous**

Events that are not occurring at the same time

## **Attribute**

Data associated with a component. For example, a server component may have attributes such as host name, IP address, operating system version, and network domain.

## **Attributed Compliance Tests (ACTs)**

Tests that are run for Compliance against query results.

## **Attributed Model (AM)**

This term is used because a Device is represent as a collection of Objects, each with certain attributes that describe the current state of the Object. For example a Device will have a ManagementIp address, and a collection of Interface objects, each of which contains an InterfaceName. Each Interface object may contain one or more InterfaceIpAddress objects, which have IpAddress as one of their attributes. The AM facilities do not replace the textual, configuration-based, model of Devices within Network Configuration Manager. Rather, the AM facilities are an extension to the existing facilities, allowing you to use the most appropriate tool for the task. The AM provides an easy way to look-up and combine information from the model in a Device class- independent fashion.

## **ARP (Address Resolution Protocol)**

Protocol that associates an interface IP address to its hardware Media Access Control (MAC) address. ARP tables provide information to Network Configuration Manager Layer 2 network devices, such as switches.

## **Attachments - Device Properties**

The Attachments tab allows you to associate an external file to the network.

## **Attachments - Sites**

The Attachments tab in Sites allows you to associate an external file to the site. This can include worksheets, documents, or .html files. Any document that can be opened in a web browser can be mapped as an attachment. Multiple attachments can be added to each site.

## **Audit**

A process of inspection, correction, and verification that is used to check an activity or process and to confirm that an activity is being carried out according to a common standard or in accordance with a recognized best practice.

### **Authenticated user**

A user who has logged into the application with a valid account (user ID and password). Authenticated users have access to all public places.

### **Auto Discovery**

The process by which devices are entered into the application for management is known as Auto Discovery. Auto Discovery associates network devices with a Network Configuration Manager device server and your networks. A type of discovery where a program automatically detects the resources that were not previously known.

### **Auto Discovery - Single Device**

While in the Devices view, you can run an Auto Discovery job on a single Device.

### **Automation Library**

Where the user creates and saves standardized templates, commands, or engineering data files used to enforce policy standards within a network.

### **Authentication**

For validation and access into Network Configuration Manager, prior to being setup in Network Configuration Manager each user must be created on the **authentication server**. When a user is created, the method of authentication is selected. Based on this selection, when the user attempts to log into Network Configuration Manager, the user's User ID, and if needed, Password are validated via the selected server.

### **Backslash**

The character \. The backslash enables a user to escape the special meaning of a character. That is, typing a backslash before a character tells the system to ignore any special meaning the character might have.

### **Back up**

To create a copy of computer data that can be used to restore data that has been lost, mislaid, corrupted or erased.

### **Baseline**

A network-level tag that is applied to the current revision of all devices in the network. A baseline is applied when the network is at a known, production state. Comparing the current revision to the baseline, and rolling back to the baseline revision can be completed from the device properties pane.

### **BASH**

Bourne Again Shell (UNIX/Linux)

## **Boolean**

Characteristic of an expression or variable that can only have a value of true or false.

## **Boot**

To load an operating system or start the system.

## **Browser**

A program allowing users to view (but not alter) data.

## **BNF**

Backus Normal Form

## **Bulk import**

The process of adding or loading a large number of items (credentials, devices, sites, users, or groups) into the application.

## **Change Audit**

The Change Audit Report generates a report or summary of devices that have been changed, based on search criteria you determine. You can see all the changes using an array of search filters to generate this report.

## **Class path**

A list of directories and JAR files that contain resource files or Java classes that a program can load dynamically at run time. CLASSPATH - In the execution environment, a variable that specifies the directories in which to look for class and resource files.

## **Client/Server**

Interaction in distributed data processing where a program on one computer sends a request to a program on another computer and waits for a response. The requesting program is called a **client**; the answering (or responding) program is called a **server**.

## **Cluster**

A group of application servers that collaborates for workload balancing.

## **Command**

Similar to a configlet, a command is a snippet of device diagnostic commands. Commands can be used in a job to provide validation, or on their own for diagnostics. They also can be stored in the Automation Library to form a diagnostic toolkit.

## **Command Editor**

The intent of the Command is not to change or update a device's configuration, although, a Command can be used for this purpose. The intent is to provide access within our product, interactively or scheduled, to other device features for performing actions. For example, providing a verification if a previous configuration change was completed correctly, completing operations on the router for verifying the integrity of the network, and completing router verification and diagnostics.

## Command Line Interface

The Command Line Interface allows you to use *command line operations* to import and export credentials, and to decrypt Credential Logs generated by password roll outs. It also allows you to import devices and Auto Discover devices.

## Comparing Hardware Revisions

From the Properties tab, you can select the **Hardware Tab** to view the Hardware information, and to select two versions to run a comparison.

## Compare Run/Start

While viewing the Devices in either the Table or Diagram view, you can compare the Run vs. the Start configuration on devices.

## Compliance Audit

You can determine which of the configurations are Compliant or Non-Compliant using this audit.

## Compliance Severity

Five levels of compliance severity include, Critical, Major, Minor, Warning, and Information.

## Configlet

A snippet of device configuration code equaling one or more configuration commands, but less than a complete config file. Configlets can be scheduled for push to one or more devices in the network.

## Configlet Editor

A text editor for constructing configlets, selecting target devices, and scheduling pushes. It is convenient for pushing quick, identical changes to many network devices.

## Config Editor

A text editor that provides a means for contextual editing and comparison of 1 - *n* device configurations. Each device config is opened in a separate window pane, and is changed through traditional editing and template insertion.

## Configuration

The manner in which the hardware and software of a network are organized and interconnected.

## Configuration Change Management System (CCMS)

A data store of profiles that contain configuration data that is used by system management applications to make configuration changes on networks.

## Configuration Management Database (CMDB)

A database that contains details about the attributes and history of each configuration item and the details about the relationships between configuration items.

## Configuration Pull

When you select this Pull Config option, what you are pulling is the running volatile configuration, and then storing that configuration onto the database.

### **Configuration unit (file)**

A configuration unit is a logical set of information that describes or controls the behavior of a device in the context of a network and its relationship with other devices. A configuration unit may simply be available as read-only data in which case it may simply contribute to the state of a device but it is not available for modification. On the other hand, most of the time configuration units are available for modification that network administrators often modify to control the higher level services offered on that network.

### **Container**

A data storage location: for example, a Network, View or Site.

### **Contextual Launch**

Using a pre-defined URL, a user or external application can launch the Network Configuration Manager application. Users must have proper authorization and authentication permissions to use this feature.

### **CPU**

Central processing unit

### **Credentials**

For added security, credentials can be set at a network level. This action provides connection validation at the network level. Only users with adequate permissions can log on to the specific network. Credentials can include, the devices local username, the devices local password, the devices local privilege-access password, the device username and password(s) from TACACS+, SNMP community strings (Read-Only and Read-Write), Telnet and SSH terminal access, and more!

### **CS**

Combination Server

### **Cut-through**

A terminal session initiated through Network Configuration Manager that utilizes assigned system credentials and maintains a log of keystrokes. Cut-through sessions can be initiated using telnet, SSH or via a modem. The user must have the View Passwords and Modify Device permissions to enter in Privilege mode, and Edit Device and View Password permissions to enter in User mode.

### **Cut-Through Tunnel**

The Device cut-through allows you to create a secure, 128-bit encrypted connection tunnel to a device. The secure tunnel uses a single port pair from client through application sever and device server to the end device.

For most clients, you can establish which Telnet client you want to execute, such as PuTTY, CRT, or Secure\_CRT. Cut-through also supports creating recorded Save Commands.

## **Daemon**

A program that runs unattended to complete continuous or periodic functions, such as network control.

## **Dashboard**

A view or container that contains one or more views and access to additional information and links.

## **DASL**

Device Access Scripting Language

## **DASLlets**

A DASLlet is a DASL routine typically written by the end-user, similar to writing a TERMlet or a Configlet.

## **Data Fields**

Data Fields are used to create attributes, and to assign values to devices.

## **Data File**

A data file pulls all template variables into an editor, and allows you to edit the details. Editing the data file in this manner allows you to complete "mass changes" to templates, and then re-import the new content to the templates. Data files can be pdf, cvs, xml or txt.

## **Default**

An attribute, value, or option that is assumed when none is explicitly specified.

## **Descending sequence**

The arrangement of data in order from the highest value to the lowest value, according to the rules for comparing data.

## **Desired state**

The state that a user wants a device to have.

## **Device**

A piece of equipment. **Devices** include routers, switches, firewalls, VPN concentrators, and OS images.

## **Device address**

A unique identifier for each device so it is recognized by the system.

## **Device class**

The generic name for a group of device types. Each device class has a unique name and represents a device type.

## **Device name**

The symbolic name of an individual device.

## Device Package

A device family or class is represented by a device package. A device package is a collection of driver code and class metadata that is used to manage all devices of that class. Device packages are field deployable.

## Device Properties

A tabbed display of device-specific information, including History, Hardware, Communications, Interfaces, General device information, Configuration files, and more. Accessed from the Devices View.

## Device Search

The Global Device Search feature allows you to search through your network at the Global level. You can search for Device Class and Network, narrowing your search to produce faster search results.

## Device Server

The appliance that is responsible for all communications with the network devices. As part of a scalable architecture, a network can employ multiple device servers to isolate overlapping address spaces, limit WAN traffic over slow connections, and balance the device load of a large environment.

## Device State

The device state is defined by a collection of configuration units pulled from the device at any point of time.

## Device type

The generic name for a group of devices

## Device IDX keys

Integer keys provided by Device Services that uniquely identify a device.

## DHCP

Dynamic Host Configuration Protocol.

## Diagnostic

Pertaining to the detection and isolation of an error.

## Diagnostic Tool

With this tool, you can track Configuration Revisions, as well as any changes made to Devices.

## Distributed Deployment

Which includes:

- **Application Server** The primary server that handles the Graphical User Interface (GUI), and coordinates with the device server to communicate with discovered devices. This server also serves as the repository for device configuration files.



- **Device Server** The communication portal between the application server and the network devices under management

## **DNS**

Domain Name System.

## **Domain**

A part of a network that is administered as a unit with a common protocol.

## **Domain name**

A name of a host system. A domain name consists of a sequence of subnames that are separated by a delimiter character, for example, www.voyence.com.

## **Download**

To transfer data from a computer to a connected device, such as a workstation or personal computer.

## **Drag**

Using a pointing device to move an object. A user can drag a window border to make it larger by holding a button pointing device while moving the pointing device.

## **Drop-down**

A list or menu that opens when clicked and stays open until the user selects a list item or clicks elsewhere in the user interface.

## **DS**

Device Server

## **EOL**

End of life

## **EOS**

End of Service

## **Event Manager**

The Event Manager feature allows you to view activities that have transpired on the network. For example, you can access the log and view the Event, the Owner (or user), the Network that was accessed, the Date/Time the event was logged, and more!

## **Export**

A function or process that converts an internal file to some standard file format for use outside of an application.

## **Expression**

A string that evaluates to a value of a particular type. Expressions consist of terms (literal strings, function calls, and symbols), and zero or more operators.

## **Favorites**

Designated favorites (you select) are listed in the navigation pane, allowing you to quickly access the Views and Workspaces you use most often.

## **Filters**

There are two filter types: Display filters and Device Membership filters.

- **Display** filters set by users to specify the details that the user wants displayed. Display filters are set per session, and are saved per user.
- **Device Membership** filters provide dynamic membership in a view, based on the device attributes and static membership through a user-defined device list. Device Membership filters are saved as part of the view's properties.

## **Firewall**

A network configuration, usually both hardware and software, that prevents unauthorized traffic into and out of a secure network.

## **Fix**

A software maintenance package such as an interim fix, test fix, or program temporary fix, that solves a customer problem.

## **Folder**

A container (such as a Network) used to organize objects.

## **Form Editor**

The Automation Library's pre-set form used to create Queries, Tests, Standards and more.

## **FQDN**

Fully qualified device name. A qualified name that includes all names in the hierarchical sequence above the structure member to which the name refers, as well as the name of the member itself.

## **Free space**

The total amount of unused space in a page, data set, file, or storage medium. Free space is the space that is not used to store records or control information.

## **FTP**

File Transfer Protocol. Application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

## **Global Device Rights**

Security permissions set at a device level that override all other security settings.

## **GMT**

Greenwich Mean Time

## **Group**

A collection of users who can share access authorities for protected resources.

### **Group name**

A name that uniquely identifies a group of users to the system.

### **Graphical User Interface (GUI)**

A type of computer interface that presents a visual metaphor of a real-world scene, often of a desktop, by combining high-resolution graphics, pointing devices, menu bars and other menus, overlapping windows, icons and the object-action relationship.

### **Hardware**

The physical components of a computer system.

### **Hierarchical**

Data that is organized on computer systems using a hierarchy of containers, often called folders (directories) and files. In this scheme, folders can contain other folders and files. The successive containment of folders within folders creates the levels of organization, which is the hierarchy.

### **High availability (HA)**

The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

### **Hypertext Transfer Protocol (HTTP)**

An Internet protocol that is used to transfer and display hypertext and XML documents on the Web.

### **IEEE**

Institute of Electrical and Electronics Engineers

### **Internationalization (I18N)**

The process of designing and developing a software product to function in multiple locales. In software engineering, the process of producing a product that is independent of any particular language, script, culture, and coded character set.

### **In-Band**

In-Band communications using a Telnet session is where you can make needed changes or enter information. Notice that this is a secure site, and you must have permission to work within this feature.

### **Interface Editor**

The Interface Editor is used to make changes to multiple interfaces on multiple devices. The editor uses configlets to insert the changes. The Interface Editor works in two ways. It allows you to filter a device's interfaces to include only the interfaces that are affected by the configlet. It also allows you to make changes to devices globally, which affects all interfaces on multiple devices. At this time, only Cisco devices are supported with this functionality.

## **IP**

Internet Protocol. This is a network layer protocol in the Internet protocol suite and is encapsulated

in a data link layer protocol (e.g., Ethernet).

### **IP address** (Internet Protocol address)

A unique address for a device or logical unit on a network that uses the IP standard.

### **IP Security Architecture** (IPSec)

A collection of Internet Engineering Task Force (IETF) standards that define an architecture at the Internet Protocol (IP) layer to protect IP traffic by using various security services.

## **IMAP**

Internet Message Access Protocol.

### **Internet Security Association and Key Management Protocol (ISAKMP)**

A protocol that provides the mechanism to establish Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP establishes the security characteristics and cryptographic keys to be used in a virtual private network (VPN).

## **Inventory Report**

A report that provides inventories of software products, patches, and hardware.

## **J2EE application**

Java 2 Platform, Enterprise Edition. Any deployable unit of J2EE functionality. This unit can be a single module or a group of modules packaged into an enterprise archive (EAR) file with a J2EE application deployment descriptor.

## **Java**

An object-oriented programming language for portable interpretive code that supports interaction among remote objects. Java was developed and specified by Sun Microsystems, Incorporated.

## **Javadoc**

A tool that parses the declarations and documentation comments in a set of source files and produces a set of HTML pages describing the classes, inner classes, interfaces, constructors, methods, and fields. (Sun)

## **Java file**

An editable source file (with .java extension) that can be compiled into bytecode (a .class file).

## **JNDI**

Java Naming and Directory Interface

## **JMX Console**

Java Management Extensions Console

## **Job**

A collection of one or more tasks, associated with an editor session that is sent to the scheduler.

## **Joins**

The join specifies the tables used in constructing a Query and the relationship between the tables. Database joins specify how to link any entry in one table with another table.

## **LDAP**

Lightweight Directory Access Protocol

## **Library Manager**

The Library Manager contains the Queries and the Tests.

## **Lightweight Directory Access Protocol (LDAP)**

An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

## **Listener**

In JDK, a class that receives and handles events.

## **Local Database**

A database that is located on the workstation in use. See also **remote database**.

## **Log file**

The file where the log of events is recorded.

## **Loop**

A sequence of instructions performed repeatedly.

## **Maintenance Window**

Network Configuration Manager allows you to set a window of time in which updates to your networks can be scheduled. This can be designated by time of day, days of the weeks, or scheduled to run on a regularly scheduled event until changed basis. A maintenance schedule can be set for the entire network, or for separate networks that are managed by Network Configuration Manager.

## **Memory**

From the Device Properties, you can select the **Hardware Tab** to view the Current Memory Allocation.

### **Management Information Base (MIB)**

In the Simple Network Management Protocol (SNMP), a database of objects that can be queried or set by a network management system.

### **Meta Data**

Data that describes a particular piece of information and that helps that information be retrieved (by search), browsed (by category), or filtered (by interest). Metadata is often part of a taxonomy or classification scheme.

### **Megabyte (Mbyte, MB)**

For processor storage, real and virtual storage, and channel volume, 2 to the 20th power or 1,048,576 bytes. For disk storage capacity and communications volume, 1 000 000 bytes.

### **Megahertz (MHz)**

A unit of measure of frequency. One megahertz equals 1 000 000 hertz.

### **MIB**

Management Information Base

### **Migrate**

To install a new version or release of a program to replace an earlier version or release.

### **Mount**

To make a file system accessible.

### **MSP**

### **Multi-hop**

To pass through one or more intermediate queue managers when there is no direct communication link between a source queue manager and the target queue manager.

### **Multi-Config**

This entails support for storing and revisioning multiple configuration files - per device.

### **MMDDYYYY**

Month-month-day-day-year-year format of a date (for example 04282007 for April 28, 2007).

### **Navigation pane**

The pane (left section of the user interface) that displays icons for views, folders, and other application features or functions. Network Configuration Manager has the Networks Navigation pane and the Library Manager Navigation pane.

### **NCM**

Network Configuration Management

## **Network**

Within Network Configuration Manager a network is defined as a logical partitioning of the devices that are in a physical network. Networks can be created to best model your business environment. For example, networks can be created and defined by customer, region, subsidiary, or responsibility. For example, they can be defined at corporate vs. division. Within networks, devices can be further organized logically and physically. In addition, you can design and stage modifications to the devices in user-defined workspaces.

### **Network Access**

When a network is created by the System Administrator, users/groups must be assigned permissions to the network prior to being able to complete any network tasks.

### **Network Address Translation (NAT)**

Network Address Translation (or NAT) modifies the source and destination IP addresses of information that flows through the system.

### **Network Administrator**

Any user that has Network Management permissions in Network Configuration Manager. Network Admin's can create, manage, and delete networks and network properties within the application. network administrator

A person who defines the network configuration and other network-related information. This person controls how an enterprise or system uses its network resources.

### **Network Navigation (tree)**

The section of the application's user interface where you can access to the menu bar (containing Tools, Windows and more), and where you can work with Favorites, Networks, Sites, Views and Workspaces.

### **NOC**

Network Operations Center (NOC)

### **NTP**

Network Time Protocol. A protocol built on top of TCP/IP that assures accurate local timekeeping with reference to radio, atomic or other clocks located on the Internet.

### **Object identifier (OID)**

A hierarchical sequence of numbers that uniquely identifies an object.

### **OIDs**

Object identifiers

### **OS**

Operating System

### **Out-of-Band Servers**

Network Configuration Manager provides an option for setting up *alternative communication methods* using out-of-band servers. For example, if there is a problem with a device and traffic cannot flow through the network, an *alternate path* can be set using a terminal server to reach the network nodes, even when the network is down.

### **Override**

To specify attributes at run time that change the attributes specified in the file description or in the program.

### **PDU**

Protocol Data Unit. A packet of data passed across a network.

### **Perl**

Practical Extraction and Report Language

### **Permissions**

Permissions allows Users and Groups access to information and tasks within Network Configuration Manager.

This includes the authority granted to users to give them access to an application's features and functions.

### **PHP**

PHP is a server-side HTML embedded scripting language.

### **Policy**

A policy is a set of user-define guidelines for any device configuration change. These guidelines can only be defined by a Network or System Administrator.

### **Postfix Mail Server**

If there is no DNS server available, you will need to select Postfix as your mail server.

### **Primary Network**

Network Configuration Manager allows devices to be managed by multiple networks . The first network that the device is associated with becomes its primary network.

### **Privilege Password Levels**

Privilege Password levels associated with Devices determines the level of access and activity a user can have pertaining to any one device. User's are limited to the device tasks they can complete, based on their Privilege level.

### **Privileged Password Mode (during Installation)**



There are two supported privileged password modes: Single-Level and Multi-Level. Use Single-Level if you are unsure which mode to use.

- **Single-Level mode** is the most widely used method and provides the highest privilege level credential used within the Network Configuration Manager application. Most users select Single-Level mode to manage authentication and maintain privileged credentials.
- **Multi-Level mode** allows multiple levels of privileged passwords to be created and associated with each device within the Network Configuration Manager application. Multi-Level mode requires devices capable of specifying multiple privilege level modes using the privileged password. Do not use this mode if you are using TACACS+, LDAP or similar external systems for authentication management.

### **Privilege class**

A level of authority that is granted to an administrator. The privilege class determines which administrative tasks the administrator can perform. For example, an administrator with system privilege class can perform any administrative task.

### **Privileged user**

A user logged into an account with root user authority.

### **Product Serial Number**

Each license key has a product serial number associated with it.

### **Promote to Baseline**

A Baseline must have already been set for the Network. Using this feature you can Promote a Baseline for a Device without a Baseline defined for the Network to the current configuration version.

### **Protected Resource**

Any section of the application or object in the application that is protected by a security permission. Examples of protected resources include networks, workspaces and devices.

### **Proxy**

An application gateway from one network to another for a specific network application such as Telnet or FTP, for example, where a firewall's proxy Telnet server performs authentication of the user and then lets the traffic flow through the proxy as if it were not there. Function is performed in the firewall and not in the client workstation, causing more load in the firewall.

### **Proxy Feature**

Using the Proxy feature, you can access your Networks and Devices without having Network Configuration Manager on the Client machine. You can use any SSH client to connect to the application.

### **Pull Hardware Spec**

When the **Pull Hardware Spec** option is selected, the hardware specifications for the specific device are pulled back into the device. The hardware that is pulled into the device is the running volatile hardware.

### **Query**

A request for information from a database based on specific conditions.

### **Queries**

A set of pre-defined queries (or tables populated with device information) is shipped with this release. Queries are similar to reports where the contents are displayed in a spreadsheet-like fashion.

### **Quick Commands**

The Quick Commands option allows you to access quick commands , including Ping, Trace route, assorted Views, and more. Quick Commands can be used with Devices, Sites, and Workspaces.

### **RADIUS**

RADIUS is an authentication and accounting server for terminal servers that speak to the RADIUS protocol. Network Configuration Manager works with RADIUS to validate user access. All user/ password details are stored on your RADIUS server. Network Configuration Manager is then mapped to the server to retrieve this information for validation.

### **RAID**

Redundant Array of Independent Disks

### **RDN**

Relatively Distinguished Name. The relative key used within Devices Services to distinguish one attribute from another in the Attributed Model.

### **Real time**

The processing of information that returns a result so rapidly that the interaction appears to be instantaneous.

### **RegEx**

Regular Expression

### **Remote Database**

1) A shared database that is accessed by a program running on a different computer. The shared database is considered remote with respect to the program accessing it.

(2) A database to which a connection is made by using a database link, while connected to a local database. See also local database.

### **Report Advisor**

Where various reports can be viewed. These reports included Inventory, Device, Credentials, and more. With the Reports Advisor, you can track and identify crucial activity on your networks. You can also create Ad Hoc Reports.

## **Repository**

The core of the Network Configuration Manager application server is where all device configuration data is stored and revisioned. It also maintains the relational database for all device and connection data.

## **Revision**

An updated device config file, differing from the last known config file.

## **Resync Device Configurations**

While viewing the Devices in either the Table or Diagram view, you are alerted (by the out-of-sync icon) that you have devices that are out-of-sync. This indicates that the running configuration for a specific device is not "in sync" with the saved device configuration, and should be brought back into sync to preserve the running configuration when the application is rebooted.

## **RHEL**

Red Hat Enterprise Linux

## **RHN**

RedHat Network

## **RME**

Resource Manager Essentials (CISCO)

## **R/O**

Read only

## **Roll back**

To return to a previous stable condition.

## **Roll Back to Baseline**

A Baseline must have already been set for the Network. From the Baseline tab in the Device Properties, you can Roll Back any changes you have made to an existing baseline.

## **Roll Credentials**

When using the Network **Shared Credentials** window, you can Roll from one credential to another credential, manage credentials on devices, and view a history of the credentials and their devices.

## **Root user**

A system user who operates without restrictions. A root user has the special rights and privileges needed to perform administrative tasks.

## **Row Limit**

Located in the Options tab on the Form Editor for Templates. By default, the server displays a maximum of 10,000 rows of data in a Query Result. You can increase or decrease the row limit.

## **RS**

Responding Server

## **RSA**

An algorithm used for public-key cryptography.

## **RSA Credentials**

A Device RSA credential or a User RSA credential used in Network Configuration Manager.

## **RSA Token Server**

The server used to store RSA tokens used for RSA authentication.

## **RSA Token Service**

A Network Configuration Manager global service built on the RSA API to enumerate soft tokens and generate pass codes.

## **RSA Two-Factor Authentication**

RSA SecurID– two-factor authentication is based on something you know such as a password or PIN, and something you have such as an authenticator. This provides a more reliable level of user authentication than a typical reusable passwords.

## **Run Time**

A designated time or interval when a job is pushed to the network. This is determined in the Schedule Manager.

## **RW**

Read/write.

## **SAR**

Mail Integration Module Service ARchive (SAR)

## **Saved Commands**

The Saved Commands option allows you to access saved commands you have previously created, and execute those commands immediately.

## **Scalability**

The ability of a system to expand as resources, such as processors, memory, or storage, are added.

## **Scheduler**

The Scheduler allows you to designate when jobs are pushed to the network.

## **Schedule Manager**

Where the user reviews, approves, rejects, cancels, holds, and checks job status and history.

## **Schema**

A collection of database objects such as tables, views, indexes, or triggers that define a database. A database schema provides a logical classification of database objects.

### **Search criteria**

Attribute values that are used to retrieve a stored item.

### **Single Device Auto Discovery**

The option selected from Tools to auto discovery a single device.

### **Sites**

Sites allow users to segment devices into a physical hierarchical structure that is user-defined and managed. Sites are viewed and updated in the Site View of a network by authorized users only.

### **Secure Sockets Layer (SSL)**

A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

### **Server-side**

Pertaining to an application or component of an application that runs on a server rather than on the client.

### **SMTP**

Simple Mail Transfer Protocol (internet email)

### **Snapshot**

A record of the current state of the database environment.

### **Simple Network Management Protocol (SNMP)**

A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

### **Single Server Deployment**

Which includes the **Combination Server** One physical box serves as both the application and device server.

### **SOAP**

A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

### **Special character**

A character other than a digit, a letter, or one of these characters: \$, #, @, ., or \_. For example, the following characters are special characters: \*, +, and %.

### **Standards**

A Standard allows you to set up filters and tests that are run against specific device classes.

### **String**

A sequence of text characters.

### **Subnet Mask**

A 32-bit address mask used to differentiate the network and host portions of an IP address. Represented as either a dotted decimal or as an integer that specifies the number of network bits. (This format is commonly known as CIDR.)

### **Sub-network**

Any network that is part of a larger IP network, and is identified by a subnet address. A network administrator segments a network into sub-networks to provide a hierarchical, multi-level routing structure of networks that are attached. Also known as a subnet.

### **Symbolic Device**

A convenience representation of a device in a network other than its primary network. Symbolic devices represent devices that are primarily managed in one network, but are used or represented in another network (such as a management router). Unless global device rights are specified for the device, the network security permissions for the subsequent networks apply to the symbolic devices.

### **System Admin**

Any user that has global System Management permissions within Network Configuration Manager. System Admin's can complete any function within the application, including network management and user management.

### **System Groups**

System Groups is a defined group of users that have the same permission levels in networks. System groups can be nested within other system groups. Nesting allows one group to "inherit" the permissions of the group in which it is nested. The nesting helps ensure that access permissions remain consistent, and decreases the time required to manually assign each user individual permissions.

### **System Management Console**

The System Management Console has control features allowing you to complete basic monitoring tasks, and to make adjustments to the services running on Network Configuration Manager.

### **System Users**

System users are users that are authorized to have access to the application for the purpose of network configuration and maintenance. Before any user can be included in a System Group, they must first be added to Network Configuration Manager. Once entered into the system and assigned privileges, the user is given access to specific networks and their devices.

### **TACACS**

## Terminal Access Controller Access Control System

### Task

A task is a scheduled event for a single device.

### Template

An object used to create new objects of the same type. The newly created object has the same characteristics as the template.

### Templates

During installation, you can access folders with examples of Templates and Tests containing pre-loaded data. These can be used as examples to create your own Templates and Tests to use in your network.

### Trivial File Transfer Protocol (TFTP)

In Internet communications, a set of conventions that transfers files between hosts using minimal protocol.

### Template Variables

When creating a template you can designate **variables** in which the user can supply a value (for example, password, IP address, DLCI, host name, or community string). A variable specifies names, properties, and the number of named variables.

TERMIlet

### Tests

Tests allow you to set preconditions and check patterns that validate the config file. Tests are then linked to Standards. Tests must be linked to a Standard to run. When the criteria for a Standard is met by a config, the Test validates against the content of the config.

### UID

Unique identifier

### up2date utility

Red Hat Enterprise Linux 4.0 up2date utility packaged. This utility requires that you have an account set up through the Red Hat Network at <http://rhn.redhat.com/>.

### Unmanaged Devices

Discovered devices that are not to be managed in the application are designated as unmanaged. Revisions and device data are not retained for unmanaged devices.

### Unclassified Devices

Devices that are not associated with, or managed within a network. If a device associated with only one network is unmanaged, it will return to an unclassified state. Revisions and device data are retained for devices in an unclassified state.

### URL

Uniform Resource Locator

### **User Admin**

Any user that has User Management permissions in Network Configuration Manager. User Admin's can create, manage, and delete users within the application.

### **Variable length**

The length of a record or field that can be changed.

### **Variables Tab**

Located on the Form Editor for Templates. This tab allows you to define variables that are initialized from the output of the result set. These variables are used the Attributed Compliance Tests.

### **Vendor**

A person or company that provides a service or product to another person or company.

### **Views**

User-defined, logical segmentations of devices in a network. The devices contained in a view may be specified through an explicit device list, and/or by specifying a filter on device attributes. Views are non-hierarchical, and may be managed using folders.

### **Virtual Devices**

New device placeholders that can be created in workspaces. They represent future devices not yet deployed in a network.

### **Wizards**

A design-based automation utility for constructing intelligent configlets used in adding connections, routing protocols, and other functionality in device configurations. Wizards assist in enforcing network best practices.

### **W/O**

Write only

### **Workspaces**

A sandbox for storing device configurations that are used in longer duration projects requiring access by multiple users, interim saves, and/or custom settings before being scheduled. Workspaces can be used for designs and complex changes. Workspaces are non-hierarchical, and can be managed using folders.

### **WSDL**

Web Services Description Language

### **XML**

Extensible Markup Language