Copyright © 2015 SolarWinds Worldwide, LLC. All rights reserved worldwide.

No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SOLARWINDS and SOLARWINDS & Design marks are the exclusive property of SolarWinds Worldwide, LLC and its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks, registered or pending registration in the United States or in other countries. All other trademarks mentioned herein are used for identification purposes only and may be or are trademarks or registered trademarks of their respective companies.

Version 7.4, revised 1/25/2016
About SolarWinds

SolarWinds, Inc. develops and markets an array of IT management, monitoring, and discovery tools to meet the diverse requirements of today’s IT management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in IT management and discovery technology. The SolarWinds customer base includes over 85 percent of the Fortune 500 and customers from over 170 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Contacting SolarWinds

You can contact SolarWinds in a number of ways, including the following:

<table>
<thead>
<tr>
<th>Team</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales</td>
<td><a href="mailto:sales@solarwinds.com">sales@solarwinds.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://www.solarwinds.com">www.solarwinds.com</a></td>
</tr>
<tr>
<td></td>
<td>1.866.530.8100</td>
</tr>
<tr>
<td></td>
<td>+353.21.5002900</td>
</tr>
<tr>
<td>Technical Support</td>
<td><a href="http://www.solarwinds.com/support/">www.solarwinds.com/support/</a></td>
</tr>
<tr>
<td>User Forums</td>
<td><a href="http://www.thwack.com">www.thwack.com</a></td>
</tr>
</tbody>
</table>

Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Specifying</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Window items, including buttons and fields.</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>Book and CD titles, variable names, new terms</td>
</tr>
<tr>
<td><strong>Fixed font</strong></td>
<td>File and directory names, commands and code examples, text typed by you</td>
</tr>
<tr>
<td>Convention</td>
<td>Specifying</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Straight brackets, as in [value]</td>
<td>Optional command parameters</td>
</tr>
<tr>
<td>Curly braces, as in {value}</td>
<td>Required command parameters</td>
</tr>
<tr>
<td>Logical OR, as in value1</td>
<td>value2</td>
</tr>
</tbody>
</table>

**Documentation Library**

The following documents are included in the documentation library:

<table>
<thead>
<tr>
<th>Document</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Guide</td>
<td>Provides detailed setup, configuration, and conceptual information.</td>
</tr>
<tr>
<td>Page Help</td>
<td>Provides help for each resource in the Web Console accessed through the Help button.</td>
</tr>
<tr>
<td>Evaluation Guide</td>
<td>Provides installation, setup, and common scenarios for which SolarWinds Network Configuration Manager provides a simple, yet powerful, solution.</td>
</tr>
</tbody>
</table>
# Table of Contents

**Chapter 1: Introduction** .................................................................................................................. 22
- Why Install SolarWinds Network Configuration Manager ............................................................ 23
- Key Features of SolarWinds Network Configuration Manager ...................................................... 24
- How Does SolarWinds NCM Work? ............................................................................................... 26
- Tips for Performing Common SolarWinds NCM Tasks ................................................................. 27

**Chapter 2: Installing and Upgrading SolarWinds Network Configuration Manager** .............. 28
- Installation Requirements .................................................................................................................. 30
- Scalability ........................................................................................................................................ 36
- Server Sizing .................................................................................................................................... 36
- Installing SolarWinds Network Configuration Manager ............................................................... 37
- Orion Platform Products: Integration Support .................................................................................. 37
- About the Orion Platform Database ................................................................................................ 38
- Installing SolarWinds NCM ............................................................................................................. 38
- Licensing with Internet Access ...................................................................................................... 39
- Licensing without Internet Access .................................................................................................. 40
- Discovering Nodes to Manage ....................................................................................................... 40
- Upgrading NCM Software ............................................................................................................... 42
- Stopping NCM Jobs ......................................................................................................................... 42
  - Stopping the SCP Server Tray ...................................................................................................... 43
  - Launching the NCM Installer ........................................................................................................ 43
- Additional Polling Engine and Web Console ................................................................................... 46
  - Installing an Additional Poller ....................................................................................................... 46
  - Installing an Additional Website ................................................................................................... 47
- Setting Node Communication Defaults ........................................................................................ 50
- Manage Connection Profiles .......................................................................................................... 52
- Using Multiple Connection Profiles .............................................................................................. 53
- Setting Communication Limits ....................................................................................................... 54
- Configuring Event Logging .............................................................................................................. 55
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changing the Vulnerability Announcements folder</td>
<td>84</td>
</tr>
<tr>
<td>Adding direct URLs</td>
<td>84</td>
</tr>
<tr>
<td>Managing End of Support and End of Sales (EOS)</td>
<td>85</td>
</tr>
<tr>
<td>Refreshing EOS Dates</td>
<td>85</td>
</tr>
<tr>
<td>Assigning EOS Dates</td>
<td>85</td>
</tr>
<tr>
<td>Ignoring Devices in EOS Management</td>
<td>86</td>
</tr>
<tr>
<td>Exporting EOS Information</td>
<td>87</td>
</tr>
<tr>
<td>How to Filter EOS Data</td>
<td>87</td>
</tr>
<tr>
<td>Deleting EOS Data</td>
<td>87</td>
</tr>
<tr>
<td>Searching for Network Addresses</td>
<td>89</td>
</tr>
<tr>
<td>Finding IP Addresses</td>
<td>89</td>
</tr>
<tr>
<td>Finding MAC Addresses</td>
<td>89</td>
</tr>
<tr>
<td>Finding Hostnames</td>
<td>89</td>
</tr>
<tr>
<td>Understanding How Addresses are Found</td>
<td>90</td>
</tr>
<tr>
<td>Understanding NCM Macros</td>
<td>92</td>
</tr>
<tr>
<td>Using Custom Macros</td>
<td>94</td>
</tr>
<tr>
<td>Creating a Custom Macro</td>
<td>94</td>
</tr>
<tr>
<td>Editing a Custom Macro</td>
<td>94</td>
</tr>
<tr>
<td>Deleting a Custom Macro</td>
<td>94</td>
</tr>
<tr>
<td>Find Connected Port for a Host (SolarWinds NPM Integration)</td>
<td>95</td>
</tr>
<tr>
<td>Unmanaging and Remanaging Nodes</td>
<td>98</td>
</tr>
<tr>
<td>Unmanaging Nodes</td>
<td>98</td>
</tr>
<tr>
<td>Remanaging Nodes</td>
<td>98</td>
</tr>
<tr>
<td><strong>Chapter 4: Managing Web Accounts</strong></td>
<td>99</td>
</tr>
<tr>
<td>Creating a New Account</td>
<td>100</td>
</tr>
<tr>
<td>Editing an Orion User Account</td>
<td>101</td>
</tr>
<tr>
<td>Setting User Account Access</td>
<td>101</td>
</tr>
<tr>
<td>Creating Account Limitations</td>
<td>104</td>
</tr>
<tr>
<td>Setting User Level Login Credentials</td>
<td>105</td>
</tr>
<tr>
<td>Setting Account Limitations</td>
<td>105</td>
</tr>
</tbody>
</table>
Limiting an Individual User Account ................................................................. 105
Limiting a Group Account .................................................................................. 106
Creating Account Limitations ............................................................................. 107
Using the Account Limitation Builder ................................................................. 107
Creating an Account Limitation ......................................................................... 107
Deleting an Account Limitation .......................................................................... 108
Defining Pattern Limitations .............................................................................. 109
Setting Default Account Menu Bars and Views .................................................. 110
Configuring Audible Web Alerts ......................................................................... 110

Chapter 5: Managing Configuration Files .......................................................... 112

Downloading Configuration Files ......................................................................... 114
Download Configs (Multiple Nodes) ..................................................................... 114
Download Configs (Single Node) ......................................................................... 115
Troubleshooting Config Download ...................................................................... 115
Confining NCM Recognition of the Command Prompt ....................................... 116
Enabling a New Config Type .............................................................................. 116
Enabling the Config and Policy Caches ............................................................... 117
Editing Configuration Files .................................................................................. 117
Upload Edited Configuration File ......................................................................... 118
Executing a Script on a Node ............................................................................... 118
Viewing Script Execution Results ........................................................................ 119
Troubleshooting Script Execution ....................................................................... 119
Config List ............................................................................................................ 119
Decrypting Cisco Type 7 Passwords .................................................................... 120
Defining Comparison Criteria ............................................................................. 120
Creating a New Regular Expression Statement .................................................. 121
Editing a Regular Expression Statement ............................................................ 121
Enabling or Disabling a Regular Expression Pattern .......................................... 121
Deleting a Regular Expression Pattern ................................................................ 121
Comparison Criteria (Exclusion Examples) .......................................................... 121
Comparing Configurations ................................................................. 122
Using the Comparison Overview ...................................................... 122
Importing Configuration Files .......................................................... 123
Understanding Baselines .................................................................... 123
Setting a Baseline .............................................................................. 123
Removing a Config File as a Baseline .................................................. 124
Baselining Your Entire Network .......................................................... 124
Clearing All Baselines ........................................................................ 125
Running a Config Change Report (Once) .............................................. 126
Uploading Configuration Changes ....................................................... 126
Uploading an Entire Configuration ...................................................... 127
Configuring a Config Archive ............................................................. 127
Creating a Config Archive for Local Storage ....................................... 127
Creating a Config Archive for Network Storage .................................. 128
Enabling Real Time Configuration Change Detection .......................... 129
Real Time Configuration Change Requirements .................................. 129
Configuring Real Time Configuration Change Detection ...................... 130
Limiting Real Time Notification Download Operations ....................... 138
Running Syslog and Trap Services as Administrator .......................... 139
Searching for Configuration Files (Web Console) ............................... 139
Deleting Configuration Files from the Database ................................... 140
Automating Configuration File Purges ............................................... 140
Chapter 6: Creating and Modifying Device Templates .......................... 142
Creating a Device Template (XML Editor) .......................................... 143
Editing a Device Template (XML Editor) ............................................ 144
Confirm Device Template Is Working .................................................. 145
Creating a Device Template (Wizard) .................................................. 146
Editing a Device Template (Wizard) .................................................... 148
Gathering the Information You Need ................................................... 149
Device Command Template Best Practices ........................................... 152
Communication Process Diagrams ................................................................. 154
Example: Config Upload and Download (SCP) ............................................... 155
Example CLI Device Command Templates ..................................................... 156
  Cisco IOS Example ..................................................................................... 157
  Nortel BayStack 380 Example ..................................................................... 158
Creating a Menu-Based Command Template ................................................ 159
Command Template Commands ..................................................................... 163
Pre-Command and Command Template Variables ......................................... 166
  Example Pre-Command Device Template Entry .......................................... 168
  Using Command Template Variables to Preclude Pseudoterminal Setup ..... 169
  Using Command Template Variables to Declare a Special Command Prompt 169
  Using Command Template Variables to Switch User Context ....................... 169
  Using Command Template Variables to Respond to Post-Logon Interaction Requests 170
Troubleshooting Device Connections ............................................................. 170

Chapter 7: Working with Command Scripts ..................................................... 172
  Executing Command Scripts ....................................................................... 173
  Using Variables within Scripts ..................................................................... 173
    Example Variable Script ........................................................................... 174
    Defining Script Variables ......................................................................... 174
    Referencing Variables with Variables ...................................................... 174

Chapter 8: Working with Config Change Templates ......................................... 176
  Config Change Template Basics ................................................................... 177
  Preparation and Use of a Template ............................................................. 177
  Parts of a Config Change Template ............................................................ 179
    Parameters ................................................................................................ 179
    Commands ................................................................................................ 179
Understanding Config Change Template Details ............................................. 180
  Example ...................................................................................................... 180
  Parameters ................................................................................................ 180
  Commands ................................................................................................. 181
Adding Tags ................................................................. 203
Removing Tags ............................................................ 203
Exporting a Config Change Template (to thwack) ................. 203
Exporting a Config Change Template (as a file) ...................... 203
Deleting a Config Change Template ..................................... 204
SolarWinds Information Services Data Entities ....................... 204
  NCM.ArpTables .......................................................... 204
  NCM.ARPTables Entity Relationships ................................ 206
  NCM.BridgePorts ....................................................... 207
  NCM.BridgePorts Entity Relationships ................................ 210
  NCM.CatalystCards .................................................... 210
  NCM.CatalystCards Entity Relationships ............................. 214
  NCM.CiscoCards ....................................................... 215
  NCM.CiscoCards Entity Relationships ................................ 217
  NCM.CiscoCdp ............................................................ 217
  NCM.CiscoCdp Entity Relationships ..................................... 220
  NCM.CiscoChassis ..................................................... 220
  NCM.CiscoChassis Entity Relationships ................................. 223
  NCM.CiscoFlash .......................................................... 223
  NCM.CiscoFlash Entity Relationships ................................... 232
  NCM.CiscoFlashFiles .................................................. 232
  NCM.CiscoFlashFiles Entity Relationships ............................... 234
  NCM.CiscoImageMIB .................................................... 234
  NCM.CiscoImageMIB Entity Relationships ............................. 234
  NCM.CiscoMemoryPools .................................................. 235
  NCM.CiscoMemoryPools Entity Relationships ............................ 236
  NCM.EntityLogical ...................................................... 236
  NCM.EntityLogical Entity Relationships ............................... 238
  NCM.EntityPhysical ..................................................... 239
  NCM.EntityPhysical Entity Relationships ............................... 245
Chapter 9: Managing Inventory ............................................... 273
Running a Complete Inventory Scan ....................................... 274
Running an Inventory Scan .................................................... 274
Scheduling an Inventory Scan .................................................. 274
Adjusting Inventory Settings .................................................... 275
Viewing Inventory Status ....................................................... 276
Chapter 10: Managing Inventory Reports ................................. 277
Viewing Reports .................................................................... 278
Creating and Scheduling Reports ............................................. 278
Exporting Reports to PDF and Printing ..................................... 278
Printing Reports ................................................................... 279
Deleting Reports ................................................................... 279
Managing Policy Reports ....................................................... 280
Creating a Policy Report ......................................................... 281
Creating a Policy ................................................................. 281
Creating a Policy Rule ......................................................... 282
Basic String Matching ...................................................... 282
Advanced String Matching ................................................. 283
Rules .................................................................................. 286
Editing a Policy Rule ......................................................... 287
Deleting a Policy Rule ......................................................... 287
Policies ............................................................................. 288
Editing a Policy ................................................................. 288
Deleting a Policy ............................................................... 288
Policy Reports ..................................................................... 288
Editing a Policy Report ..................................................... 288
Generating a Policy Report ................................................ 289
Exporting a Policy Report (to thwack) ............................... 289
Exporting a Policy Report (as a file) ................................. 289
Deleting a Report .............................................................. 290
Scheduling a Policy Report ................................................ 290
Enabling the Config and Policy Caches ............................... 290
        Manually Refresh the Policy Cache ............................. 291

Chapter 12: Managing Jobs ..................................................... 292
Enabling and Disabling a Job ............................................. 293
    Enabling a Job .......................................................... 293
    Disabling a Job .......................................................... 293
Starting and Stopping a Job ................................................. 294
    Starting a Job .......................................................... 294
    Stopping a job .......................................................... 294
Creating or Editing a Job .................................................... 295
Viewing Job Logs ............................................................. 296
Deleting a Job ................................................................. 297

Chapter 13: Approving Device Configuration Changes .......... 298
<table>
<thead>
<tr>
<th>Chapter 14: Understanding the Orion Web Console</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launching and Logging On to Orion Web Console</td>
</tr>
<tr>
<td>Understanding Orion Web Console Resources</td>
</tr>
<tr>
<td>Home</td>
</tr>
<tr>
<td>All Active Alerts Resource</td>
</tr>
<tr>
<td>Config Summary</td>
</tr>
<tr>
<td>Node Details</td>
</tr>
<tr>
<td>Configuration Management</td>
</tr>
<tr>
<td>Config Change Templates</td>
</tr>
<tr>
<td>Reports</td>
</tr>
<tr>
<td>Compliance</td>
</tr>
<tr>
<td>Jobs</td>
</tr>
<tr>
<td>End of Support</td>
</tr>
<tr>
<td>Searching</td>
</tr>
<tr>
<td>Personalizing the Web Console</td>
</tr>
<tr>
<td>Integrating with Engineer's Toolset</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 15: Integrating NCM Actions into Orion Alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Types of NCM Alert Actions</td>
</tr>
<tr>
<td>Using the Default NCM Alert</td>
</tr>
<tr>
<td>Adding Scripted Commands to the Default NCM Alert</td>
</tr>
<tr>
<td>Navigating to the Alert Manager</td>
</tr>
</tbody>
</table>
Available Alert Actions ................................................................. 318
Alert Preconfiguration Tasks .......................................................... 318
Adding an SMTP Server ................................................................. 318
Creating and Configuring Advanced Alerts ...................................... 319
  Creating New Alerts ................................................................. 320
Best Practices and Tips for Alerting .................................................. 320
  Use the Out of the Box Alerts as Templates ................................... 320
Restrict Who Receives Alerts ......................................................... 321
Plan which Devices to Monitor ....................................................... 321
  Establish Dependencies ............................................................ 321
Setting Alert Properties ................................................................. 321
Setting Trigger Conditions ............................................................. 322
Setting Reset Conditions ............................................................... 324
Alert Suppression Example ............................................................ 326
Building Complex Conditions ......................................................... 326
Setting the Time of Day or Schedule ................................................ 327
Setting Trigger Actions & Escalation Levels ...................................... 330
  Trigger Actions ................................................................. 330
  Escalation Levels .............................................................. 331
Setting Reset Actions ................................................................. 332
  Escalating Alerts .............................................................. 333
Adding Alert Actions ................................................................. 333
Available Alert Actions ................................................................. 334
  Sending an Email/Page .......................................................... 334
Playing a Sound ........................................................................... 337
Logging an Advanced Alert to a File ................................................. 338
Logging an Alert to the Windows Event Log ...................................... 339
Logging an Alert to the Event Log .................................................... 340
Sending a Syslog Message .............................................................. 342
Executing an External Program ....................................................... 343
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing a Visual Basic Script</td>
<td>344</td>
</tr>
<tr>
<td>Emailing a Web Page</td>
<td>345</td>
</tr>
<tr>
<td>Using Text to Speech Output</td>
<td>347</td>
</tr>
<tr>
<td>Sending a Windows Net Message</td>
<td>348</td>
</tr>
<tr>
<td>Sending an SNMP Trap</td>
<td>350</td>
</tr>
<tr>
<td>Using Get or Post URL Functions</td>
<td>351</td>
</tr>
<tr>
<td>Dialing Paging or SMS Service</td>
<td>352</td>
</tr>
<tr>
<td>Viewing Alerts from Mobile Devices</td>
<td>353</td>
</tr>
<tr>
<td>Viewing Alerts in the Orion Web Console</td>
<td>353</td>
</tr>
<tr>
<td>Acknowledging Advanced Alerts in the Web Console</td>
<td>354</td>
</tr>
<tr>
<td>Escalated Advanced Alerts</td>
<td>354</td>
</tr>
<tr>
<td>Escalated Alert Example</td>
<td>355</td>
</tr>
<tr>
<td>Viewing Alerts from Mobile Devices</td>
<td>355</td>
</tr>
<tr>
<td>Syslog Alert Variables</td>
<td>356</td>
</tr>
<tr>
<td>Syslog Date/Time Variables</td>
<td>356</td>
</tr>
<tr>
<td>Other Syslog Variables</td>
<td>357</td>
</tr>
<tr>
<td><strong>Chapter 16: Creating and Managing Reports</strong></td>
<td>359</td>
</tr>
<tr>
<td>Predefined Reports</td>
<td>360</td>
</tr>
<tr>
<td>Creating a New Web-Based Report</td>
<td>361</td>
</tr>
<tr>
<td>Viewing Reports in the Orion Web Console</td>
<td>364</td>
</tr>
<tr>
<td>Running a Config Change Report (Once)</td>
<td>365</td>
</tr>
<tr>
<td>Scheduling a Config Change Report (Recurrent)</td>
<td>366</td>
</tr>
<tr>
<td>Creating a Report Schedule While Creating or Editing a Report</td>
<td>367</td>
</tr>
<tr>
<td>Creating, Assigning and Editing Report Schedules in Report Manager</td>
<td>371</td>
</tr>
<tr>
<td>Exporting and Importing Reports</td>
<td>376</td>
</tr>
<tr>
<td>NCM Reports: Brocade Inventory</td>
<td>377</td>
</tr>
<tr>
<td>Current Node Status</td>
<td>378</td>
</tr>
<tr>
<td>Current Volume Status</td>
<td>379</td>
</tr>
<tr>
<td>Daily Node Availability</td>
<td>380</td>
</tr>
<tr>
<td>Events</td>
<td>381</td>
</tr>
</tbody>
</table>
Groups: Current Groups and Groups Members Status .................................................. 382
Groups: Daily Group Availability .............................................................................. 383
Groups: Group Availability (with members) ............................................................. 384
Historical CPU and Memory Reports ..................................................................... 385
Groups: Historical Groups Status ............................................................................. 386
Historical Response Time Reports .......................................................................... 387
Historical VMware ESX Server Reports ................................................................. 388
Historical Volume Usage Reports ............................................................................ 389
Inventory .................................................................................................................. 390
NCM Audit ................................................................................................................ 391
NCM Reports: Cisco Inventory ................................................................................. 392
NCM Reports: Inventory .......................................................................................... 393
NCM Reports: Node Details ..................................................................................... 394
NCM Reports: Polling Status ................................................................................... 396
NCM Reports: Route Tables Inventory ..................................................................... 397
NCM Reports: Security ............................................................................................ 398
NCM Reports: Windows Server Inventory ............................................................... 399
Adding Content to a Web-Based Report Column .................................................... 400
Adding a Custom Chart or Table to a Web-Based Report Column ......................... 402

Chapter 17: Configuring TFTP, Secure Copy /SFTP, SMTP Server ....................... 409
Using the SolarWinds TFTP Server ......................................................................... 410
    Using Secure Copy /SFTP Server ........................................................................ 410
    Using a Third-Party SCP Server ........................................................................ 411
    Configuring the SMTP Server for Email Notifications ...................................... 411
        Email Notification Settings ............................................................................ 412

Chapter 18: Managing EnergyWise Entities .......................................................... 413
What is EnergyWise? ............................................................................................... 414
    Managing and Enabling EnergyWise Nodes ...................................................... 414
    Managing Your PoE Ports ............................................................................... 415

Chapter 19: Common Tasks .................................................................................. 416
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alternation</td>
<td>444</td>
</tr>
<tr>
<td>Quantifiers</td>
<td>444</td>
</tr>
<tr>
<td>Regular Expression Pattern Matching Examples</td>
<td>446</td>
</tr>
<tr>
<td><strong>Appendix C: Using the Database Management Tools</strong></td>
<td>448</td>
</tr>
<tr>
<td>Starting SolarWinds Database Manager</td>
<td>449</td>
</tr>
<tr>
<td>Adding a Server to SolarWinds Database Manager</td>
<td>449</td>
</tr>
<tr>
<td>Viewing Database Details</td>
<td>449</td>
</tr>
<tr>
<td>Viewing Table Details</td>
<td>450</td>
</tr>
<tr>
<td>Moving a Database with SQL Server Management Studio</td>
<td>451</td>
</tr>
<tr>
<td>Creating a Database Backup File with SQL Server Management Studio</td>
<td>451</td>
</tr>
<tr>
<td>Restoring Backup Files to SQL Server 2008 and 2012</td>
<td>453</td>
</tr>
<tr>
<td>Restoring a Database Backup File for SQL Server 2008</td>
<td>453</td>
</tr>
<tr>
<td>Restoring a Database Backup File for SQL Server 2012</td>
<td>454</td>
</tr>
<tr>
<td>Updating SolarWinds NCM to Use the New Database Server</td>
<td>455</td>
</tr>
<tr>
<td><strong>Appendix D: Monitoring SNMP Traps</strong></td>
<td>457</td>
</tr>
<tr>
<td>The SNMP Trap Protocol</td>
<td>458</td>
</tr>
<tr>
<td>Configuring the Trap Viewer</td>
<td>458</td>
</tr>
<tr>
<td>Trap Viewer Settings</td>
<td>458</td>
</tr>
<tr>
<td>Configuring Trap Viewer Filters and Alerts</td>
<td>459</td>
</tr>
<tr>
<td>Available Trap Alert Actions</td>
<td>461</td>
</tr>
<tr>
<td>Working with Traps</td>
<td>463</td>
</tr>
<tr>
<td>Viewing Current Traps</td>
<td>463</td>
</tr>
<tr>
<td>Searching for Traps</td>
<td>463</td>
</tr>
<tr>
<td>Trap Alert Variables</td>
<td>464</td>
</tr>
<tr>
<td>Trap Date/Time Variables</td>
<td>464</td>
</tr>
<tr>
<td>General Trap Variables</td>
<td>465</td>
</tr>
<tr>
<td><strong>Appendix E: Monitoring Syslog Messages</strong></td>
<td>467</td>
</tr>
<tr>
<td>Understanding the Syslog Protocol</td>
<td>468</td>
</tr>
<tr>
<td>Syslog Priorities</td>
<td>468</td>
</tr>
<tr>
<td>Syslog Facilities</td>
<td>468</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

SolarWinds Network Configuration Manager is a comprehensive, intuitive solution designed to streamline and automate network configuration management. SolarWinds Network Configuration Manager increases availability, saves time, improves security, and ensures policy adherence. SolarWinds Network Configuration Manager features automation capabilities that reduce the amount of time network engineers spend on mundane network tasks, allowing them to focus on business-critical network projects.

Why Install SolarWinds Network Configuration Manager
Key Features of SolarWinds Network Configuration Manager
How Does SolarWinds NCM Work?
Why Install SolarWinds Network Configuration Manager

SolarWinds Network Configuration Manager allows you to easily manage configurations on heterogeneous, multi-vendor networks. SolarWinds Network Configuration Manager supports routers, switches, firewalls, load balancers, and wireless access points from numerous vendors, including Cisco, Cisco ASA, Dell, Adtran, Arris, Aruba, Nortel, Nortel Alteon, Nortel BayStack, Extreme, Marconi, Radware, Netscreen, Motorola, HP, Netscalar, Juniper and Foundry. You gain a single point of management. Whether you are faced with managing network configurations for 50 or 5,000 devices, SolarWinds Network Configuration Manager provides you with an intuitive solution that immediately impacts the bottom line. SolarWinds NCM includes the ability to:

- Control access based on user roles
- Schedule device configuration backups
- Implement configuration changes in bulk (IOS and firmware updates)
- Manage configuration changes to multiple devices from different vendors with change management templates
- Generate detailed configuration reports for inventory, change, and policy management
- Receive notification of device configuration changes
- Identify configuration violations through policy management reporting
- Automatically receive results of appropriate SolarWinds NCM actions with the Orion notification of an alerting device (Requires Integration Module)
- View detailed change history and side-by-side comparison of configurations
- Perform detailed device inventory for each managed device
- Track and view configuration changes made by users
- Access your device configurations and configuration changes from either a SolarWinds NCM or Orion Web Console (Requires Integration Module)
- Map the port connections for a specific network switch
Key Features of SolarWinds Network Configuration Manager

Scheduled Configuration Backups

Schedule configuration downloads, configuration uploads, device reboots, command scripts execution, and more. In addition, configuration backups are stored both in a relational database for archival history and as flat files in an intuitive folder structure for easy viewing.

Policy Management

Ensure device compliance with federal regulations, as well as corporate standards. The Policy Reporting Manager comes with several out-of-the-box policy reports, including SOX, HIPAA, CISP, and Cisco Security.

Role-Based Access Control

Integrate your Windows Active Directory or local system user accounts with SolarWinds Network Configuration Manager. You can manage users based on their role and establish individual device login credentials per user. SolarWinds Network Configuration Manager logs all user activity allowing you to keep an archive of changes and activity.

Multi-Vendor Support

Monitor network devices from multiple hardware vendors. As a monitor and manager of routers, switches, firewalls, VPN concentrators, wireless access points and more, SolarWinds Network Configuration Manager is a robust solution that is fully capable of managing your hybrid vendor network.

Bulk Changes

Across many devices you can quickly make changes to community strings, passwords, and black lists. With SolarWinds Network Configuration Manager, you can execute bulk changes either in real time or within a scheduled change window. Uploads, changes, and global command scripting can be scheduled by device type, physical location, by owner, or by any custom property you create.

Configuration Change History

Receive reports on what devices have had configuration changes over any time period you specify. Configuration change reports can also compare current configurations with a baseline configuration alerting you whenever a change is discovered.
Web-Based NCM Settings
Use a web browser to set and adjust SolarWinds NCM Settings.

Web-Based Configuration Viewing, Tracking, and Comparing
Use SolarWinds Network Configuration Manager to remotely view, track and make changes, and compare network device configurations without logging on to the physical SolarWinds NCM server. The Orion Web Console offers these powerful functions to the users you select.

Orion Web Console Integration
SolarWinds NCM adds the following resources to the Device Details view of the Orion Web Console:

- Recent Configurations
- Recent Configuration Changes
- Node Configuration History
- Last 10 Config Changes
- Last X Config Changes
- Last XX Configurations
- Find Connected Port for End Host (Added to the Config Summary view with SolarWindsNPM integration)

Orion Alerts Integration
Use a default SolarWinds NCM alert in the Orion Alert Manager and specify NCM actions to run when this alert triggers. View the results of those actions along with the notification.

Device Configuration Change Templates
Use templates to generate an appropriate sequence of CLI commands for all relevant devices for which you need to make a specific configuration change.

Device Configuration Change Management
Setup a request and approval system for processing the workflow of device configuration changes.
Device End of Life and End of Service Tracking

Setup a request and approval system for processing the workflow of device configuration changes.

How Does SolarWinds NCM Work?

SolarWinds Network Configuration Manager uses a scripting engine to parse individual commands across several different platforms. This scripting engine combined with the SolarWinds Job Engine allows SolarWinds NCM to schedule nightly backups, configuration changes, inventory scans, and more. There are no agents installed on your servers and no remote software to maintain. All configuration changes and user activity is stored in the SolarWinds Orion database and accessible from the Orion Web Console.
Chapter 1: Introduction

Tips for Performing Common SolarWinds NCM Tasks

Click the link under a SolarWinds NCM task for more information:

- Estimating Free Space on the SQL Server Host
  Reliably determine that your installing and upgrading SolarWinds Network Configuration Manager to hold the SolarWinds NCM data and any existing Orion platform product data, while still having enough remaining capacity for your deployment’s usual monitoring and configuration activities.

- Downloading Config Files
  Throttle Managing Configuration Files

- Sequencing NCM Alert Actions
  Types of NCM Alert Actions

- Creating an NCM Custom Property
  Creating a Custom Property

- Setting NCM’s Device Communication Defaults
  Use Setting Node Communication Defaults

- Setting-up a Config Archive
  Troubleshoot Configuring a Config Archive
Chapter 2: Installing and Upgrading SolarWinds Network Configuration Manager

SolarWinds NCM version 7.4 builds on the major rearchitecture that merged all Orion platform and NCM data into a single database.

Check Installation Requirements for information related to the minimum hardware and software needed to successfully run SolarWinds NCM.

You have one option for installing and two options for upgrading the NCM version 7.4 software.

Single Server Standalone (Installation and Upgrade)
This option installs or upgrades NCM on a host by itself, without any other Orion platform products.

Single Server Integrated (Upgrade Only)
This option installs NCM on a host with another Orion platform product, integrating those products so that you can access their features from a single Orion Web Console.

Installing or upgrading NCM involves these processes:

- Installing the NCM software
- Configuring the database, website, and services
- Discovering network devices

Whether you are installing or upgrading NCM, in order to ensure its best performance on your server host, specifically exclude these file paths from anti-virus software scans:

- %USERPROFILE%\AppData\Local\Temp
- %ALLUSERSPROFILE%\Application Data\Solarwinds
- %Program Files (x86)%\SolarWinds\Orion
- %Program Files (x86)%\SolarWinds\Orion\NCM
Chapter 2: Installing and Upgrading SolarWinds Network Configuration Manager

C:\Windows\System32\msmq\storage

SolarWinds NCM 7.4 installation software is in your customer portal.
Installation Requirements

Requirements vary based on:

- The number of nodes
- The frequency of configuration downloads
- The length of time that configurations are maintained in the database

The table provides the general requirements for installing SolarWinds Network Configuration Manager.

<table>
<thead>
<tr>
<th>Software/Hardware</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>• Windows 2003 Server SP2 (32-bit and 64-bit) including R2 SP2, and with IIS installed and running in 32-bit mode</td>
</tr>
<tr>
<td></td>
<td>• Windows 2008 Server Enterprise or Standard (32-bit or 64-bit) including R2, with IIS installed and running in 32-bit mode, and Server 2008 R2 SP1</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 and Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>For evaluation purposes only:</td>
</tr>
<tr>
<td></td>
<td>• Windows 7 and Windows 7 SP1</td>
</tr>
<tr>
<td></td>
<td>• Windows 8 (except Standard edition)</td>
</tr>
<tr>
<td></td>
<td>• Windows 8.1 including Update 1 (except Standard edition)</td>
</tr>
</tbody>
</table>

**Note:** Installation on a Windows Domain Controller is not supported.

<table>
<thead>
<tr>
<th>Operating System Language</th>
<th>• English (US &amp; UK)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• German</td>
</tr>
<tr>
<td></td>
<td>• Japanese</td>
</tr>
</tbody>
</table>
# Chapter 2: Installing and Upgrading SolarWinds Network Configuration Manager

## Software/Hardware Requirements

<table>
<thead>
<tr>
<th>Software/Hardware</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Simplified Chinese.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> NCM does not support using locales outside the group of supported operating system languages.</td>
<td></td>
</tr>
<tr>
<td>SolarWinds NCM Server Hardware</td>
<td><strong>CPU Speed</strong> 3 GHz dual core dual processor</td>
</tr>
<tr>
<td></td>
<td><strong>Memory</strong> 4GB</td>
</tr>
<tr>
<td></td>
<td><strong>Hard Drive Space</strong> 30GB</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This version of NCM holds a searchable config index on local disk that adds 6-10GB additional disk space to the previous requirement.</td>
</tr>
<tr>
<td>Installing Windows Account</td>
<td>Requires administrator permission on the target server.</td>
</tr>
<tr>
<td>File System Access Permissions</td>
<td>Ensure the Network Service account has modify access to the system temp directory (%systemroot%	emp).</td>
</tr>
<tr>
<td>SolarWinds Orion Syslog Server</td>
<td>If you want real-time change detection triggered through devices sending Syslog messages, the executable must have read-write access to the Orion Platform database. For more information, see “Enabling Real-time Configuration Change Detection” and “Monitoring SNMP”.</td>
</tr>
<tr>
<td>Software/Hardware</td>
<td>Requirements</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SolarWinds Orion Trap Service</td>
<td>If you want real time change detection triggered through devices sending SNMP traps, the executable must have read-write access to the Orion Platform database. For more information, see “Enabling Real-time Configuration Change Detection” and “Monitoring SNMP”.</td>
</tr>
<tr>
<td>Microsoft SNMP Trap Service</td>
<td>Must be installed if you want real time change detection triggered through devices sending SNMP traps. For more information, see “Enabling Real-time Configuration Change Detection” and “Monitoring SNMP” in the SolarWinds NCM Administrator Guide.</td>
</tr>
<tr>
<td>Microsoft IIS</td>
<td>Version 6 or later. DNS specifications require hostnames to be composed of alphanumeric characters (A-Z, 0-9), the minus sign (-), and periods (.). Underscore characters (_) are not allowed. For more information, see RFC 952.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> SolarWinds neither recommends nor supports the installation of SolarWinds NCM on the same server or using the same database server as a Research in Motion (RIM) Blackberry server.</td>
</tr>
<tr>
<td>Microsoft ASP .NET 2.0 Ajax Extension</td>
<td>Version 1 or later (if this is not found on the target computer, the setup program downloads and installs the component)</td>
</tr>
<tr>
<td>Microsoft .NET Framework</td>
<td>Version 4.0.3 (if this is not found on the target computer, the setup program downloads and installs it)</td>
</tr>
<tr>
<td>Database</td>
<td><strong>Note:</strong> You must create the SolarWinds Orion database with the SolarWinds Configuration Wizard. Creating the database in another way is not supported. SolarWinds supports using NCM with database servers setup in these languages: English, German, Japanese, and Chinese. Only storing characters in the UTF8 set is supported, however.</td>
</tr>
</tbody>
</table>
## Software/Hardware Requirements

The following database servers are supported as the SolarWinds Network Configuration Manager datastore:

- SQL Server 2014 (also with AlwaysOn Availability Groups)
- SQL Server 2012 with/without SP1 and SP2
  Standard or Enterprise (also with AlwaysOn Availability Groups)
- SQL 2008 R2 without SP, 2008 R2 SP1, 2008 R2 SP2
- SQL 2008 without SP, 2008 SP1, 2008 SP2, 2008 SP3

You can use the following database select statement to check your SQL Server version, service pack or release level, and edition:

```sql
select SERVERPROPERTY ('productversion'),
SERVERPROPERTY ('productlevel'),
SERVERPROPERTY ('edition')
```

The following SQL server collations are supported:

- English with collation setting SQL_Latin1_General_CP1_CI_AS
- English with collation setting SQL_Latin1_General_CP1_CS_AS
- German with collation setting German_PhoneBook_CI_AS
- Japanese with collation setting Japanese_CI_AS
- Simplified Chinese with collation setting Chinese_PRC_CI_AS
### Software/Hardware

<table>
<thead>
<tr>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your database server must support mixed-mode authentication or SQL authentication and have the following protocols enabled:</td>
</tr>
<tr>
<td>- Shared memory</td>
</tr>
<tr>
<td>- TCP/IP</td>
</tr>
<tr>
<td>- Named Pipes</td>
</tr>
<tr>
<td>SQL Server 2008 Express Edition does not enable these protocols.</td>
</tr>
<tr>
<td>The following x86 components must be installed (if the components are not found on the target computer, the setup program downloads and installs the components):</td>
</tr>
<tr>
<td>- SQL Server System Common Language Runtime (CLR) Types</td>
</tr>
<tr>
<td>- Microsoft SQL Server Native Client</td>
</tr>
<tr>
<td>- Microsoft SQL Server Management Objects</td>
</tr>
</tbody>
</table>

### Ports

| The following ports that may be needed for Orion Web Console and depending on how SolarWinds NCM is setup to download and upload configurations. |
| - 20: FTP data transfer |
| - 21: FTP control (setup/teardown) |
| - 22: SSH/SCP default for NCM to transfer configs |
| - 23: TELNET default for NCM to transfer configs |
| - 25: SMTP email default that NCM uses for notifications |
| - 25: SSL/TLS for email alert actions should be enabled on it |
| - 69: TFTP server listens on it |
| - 80: HTTP default for Orion Web Console |
Chapter 2: Installing and Upgrading SolarWinds Network Configuration Manager

<table>
<thead>
<tr>
<th>Software/Hardware</th>
<th>Requirements</th>
</tr>
</thead>
</table>
|                   | ● 161: SNMP statistics collection, NCM's default for polling  
|                   | ● 162: UDP trap messages listened for and received by Trap Server  
|                   | ● 514: UDP Syslog messages arrive for Orion Syslog Service  
|                   | ● 17777: SolarWinds Information Service for Orion Web Console  
|                   | ● 17778: SolarWinds Information Service for Orion Web Console  
|                   | ● 17779: SolarWinds Information Service for Orion Web Console  
|                   | ● 1801: TCP used for MSMQ WCF binding  
|                   | More information: [http://support.microsoft.com/kb/183293](http://support.microsoft.com/kb/183293) |

<table>
<thead>
<tr>
<th>Browser</th>
<th></th>
</tr>
</thead>
</table>
|                   | ● Microsoft Internet Explorer 8, 9, 10, 11 (standard and mobile views)  
|                   | ● Mozilla Firefox 10.0.9, 16.0.2  
|                   | ● Google Chrome v22.0.1229.96, 23.0.1271.64 |

**Notes:**
- The SolarWinds Network Configuration Manager Information Service requires the **Net.Tcp Port Sharing Service** to be enabled and port 17777 open for TCP traffic to the SolarWinds NCM computer. By default, this service is disabled. The setup program sets the service to manual. Resetting the service setting to disabled will adversely affect your installation.
- To take advantage of the numerous integration points in SolarWinds Network Configuration Manager, install the SolarWinds Engineer's Toolset on the same server. You can also take advantage of integration points built into the Web Console by installing the Toolset on computers used to access the Web Console.
Scalability

NCM 7.4 was tested for scalability in a standalone deployment of three servers: one server hosts the main NCM server and the other two servers each host an additional NCM polling engine. The main NCM server manages up to 10,000 NCM nodes, as does each additional NCM polling engine. Therefore, the deployment supports up to 30,000 nodes total.

The standard Orion Web Console deployment has the Orion Platform on the main NCM polling for node status at the default rate. This deployment supports two NCM operations (inventory update and configuration download) performed per day on all 30,000 nodes.

Though the main NCM server and each additional polling engine can manage up to 10,000 nodes, the actual total depends on the system hardware of the server hosts, the types of devices being monitored, and the number of jobs being run concurrently. Should you need to manage more devices, and you decide to add NCM servers, consider consolidating your views of multiple servers with the Orion Enterprise Operations Console. For more information about scaling NCM, please contact your account manager.

Server Sizing

SolarWinds Network Configuration Manager can perform configuration management for any sized network, from small corporate LANs to large enterprise and service provider networks. Most SolarWinds NCM implementations perform well on Pentium-class 3GHz systems with 4GB of RAM using the default simultaneous transfer settings, with no modifications to node monitoring settings.

Should scalability issues arise, adjust the following:

- Number of simultaneous transfers
- Frequency of uploads, downloads, and inventory jobs
- Node polling interval for up/down monitoring

Inventory jobs may run longer than expected in larger environments. To remedy this situation, break large inventory jobs into smaller jobs that do not include as many nodes, and space these jobs over a longer period of time. Adjusting server CPU and memory will enhance user interface performance and job execution speed.
Chapter 2: Installing and Upgrading SolarWinds Network Configuration Manager

Installing SolarWinds Network Configuration Manager

An Orion platform product is one whose features and functions can be accessed and managed through the Orion Web Console. Integrating NCM with another Orion platform product on a single makes all features accessible from the same Orion Web Console.

After installing NCM in a standalone deployment, installing and integrating another Orion platform product with NCM can only be done on the NCM host. The other Orion product would share the Orion platform database established with the NCM installation.

You cannot integrate NCM with an Orion platform product installed on a different host. Conversely, you cannot separate NCM from another Orion platform product once they are integrated, since they share a single database.

Orion Platform Products: Integration Support

If you are integrating NCM with another Orion platform product, the other product must be installed first on the host. SolarWinds NCM version 7.4 integrates with the following Orion platform products and versions:

- SolarWinds Network Performance Manager (NPM) version 11.5.2
- SolarWinds Server and Application Monitor (SAM) versions 6.1.x, 6.2
- EOC: 1.5, 1.6
- SolarWinds IP Address Manager (IPAM) version 4.0, 4.1
- SolarWinds User Device Tracker (UDT) version 3.0, 3.0.1, 3.0.2, 3.0.3
- SolarWinds IPSLA (VNQM) version 4.0.1, 4.1, 4.2
- Toolset: 10.9, 11.0

SolarWinds NCM shares common components with all Orion platform products. Installing and configuring SolarWinds NCM involves shutting down and restarting all Orion services. Choose a time to install when your IT operation can tolerate a short period of downtime for Orion platform products.
About the Orion Platform Database

Microsoft SQL Server 2008 Express Edition is distributed with SolarWinds Network Configuration Manager. SQL Server 2008 Express Edition supports a maximum database size of 10GB, is limited to 1GB of RAM use, and takes advantage of only 1 CPU in a multi-processor server. For more information about SQL Server installation, see the Microsoft website.

We recommend that you create the database on a separate SQL Server host (not the NCM host). To increase performance, we recommend using a remote SQL Server host if you are installing SolarWinds NCM on the same host as SolarWinds NPM.

Installing SolarWinds NCM

1. Log on to the host with a local administrator account.
   
   **Note:** Do not install on a domain controller.

2. Launch the executable from the download location.

3. Select **Send usage statistics to SolarWinds** to send us usage statistics and help improve our products.

4. Accept the License Agreement, and then click **Next**.

5. Accept the default target directory or set another that you prefer.

6. Click **Next** to start copying files.

7. Click **Finish**. The Configuration Wizards starts.

8. Click **Next** to begin configuring the Orion platform database, website, and services.

9. Specify the SQL Server instance you want to use for your database.
Chapter 2: Installing and Upgrading SolarWinds Network Configuration Manager

10. Enter the database authentication method (Windows or SQL Server Authentication), and then click Next.

   **Notes:**
   
   - The SQL Server instance must support SQL authentication or mixed mode.
   - If you are using a local instance of SQL Server Express, use the following syntax to use the default instance: (local)\SQLEXPRESS.
   - If you select SQL Authentication, provide an account with sufficient rights to create new databases on the server instance. For example, specify the SQL administrator (sa) account.

11. Select your existing Orion platform database, and then click Next.
12. Select an existing account with administrator rights on the database, and then click Next.

   **Note:** You must supply a strong password. For more information on strong passwords, see the Microsoft website.

13. Click Next to setup the website with default settings or adjust the settings as needed.
14. Click Yes if a website exists with the same settings.
15. Click Next after reviewing the settings and overview configuration plan.
16. Click Finish when the wizard completes.

**Licensing with Internet Access**

1. Click Enter Licensing Information.
2. Select the I have internet access and an activation key..., enter your Activation Key, and then click Next.
3. If applicable, select I access the internet through a proxy server.
4. Enter registration information, and then click Finish.
5. If licensing fails the software enters evaluation mode for 30 days.
Licensing without Internet Access

1. Click **Enter Licensing Information**.

2. Select **This server does not have internet access**..., click **Next**, and then complete the steps provided.

3. You need a customer ID and password to install the key. For more information, see [Obtaining a Software License Key](#).

Discovering Nodes to Manage

1. Enter a user name and password. The default credentials are *admin* and no password.

2. Click **DISCOVER MY NETWORK** under NCM Nodes to discover nodes for management. Network Sonar Wizard loads.

3. Review and accept the defaults (public/private) for the SNMP read-only and read-write community strings, or click the pencil icon to edit a credential.

4. Click **Next**. These default strings are tried first during node discovery.

5. Click **Add New Credential** under Windows Credentials as needed.

   **Note:** WMI is used to collect CPU, memory, volume, and other data from Windows Servers that do not support SNMP.

6. Define an IP range, subnet, or a list of specific nodes to use in node discovery, and then click **Next**.

7. Review and adjust discovery settings.

8. To ignore nodes that provide no SNMP or WMI information, click **Ignore nodes**....

9. Click **Next**.

10. Click **DISCOVER**. The Discovery Results Wizard opens.

11. Review the list of discovered device types, deselect any that you do not want to import into the database, and then click **Next**.

12. Review the list of discovered volumes, deselect any that you do not want to import into the database, and then click **Next**.

13. Click **Import**.

14. Click **Finish** when the import is done. Discovery Central loads.
Chapter 2: Installing and Upgrading SolarWinds Network Configuration Manager

15. Review the NCM node count in Manage More Nodes under the NCM Nodes option group.

16. Click CONFIGS in the Orion Web Console to access SolarWinds NCM.

Use these topics as needed to finish setting up your deployment:

- Installing an Additional Poller
- Installing an Additional Website
- Removing SolarWinds Network Configuration Manager
- Using SSL Communication with SolarWinds NCM
- Setting Node Communication Defaults
- Using Multiple Connection Profiles
- Setting Communication Limits
- Configuring Event Logging
- Scalability
- Server Sizing
- Licensing SolarWinds Network Configuration Manager
- Obtaining a Software License Key
- Reviewing Your License
- Resetting Your License
- SNMP Communication
Upgrading NCM Software

You have two options for upgrading NCM software to version 7.4.

**Single Server Standalone**

This option installs or upgrades NCM on a host by itself without any other Orion platform products.

**Single Server Integrated**

This option installs NCM on a host with another Orion platform product, integrating those products so that you can access their features from a single Orion Web Console.

**Stopping NCM Jobs**

You cannot upgrade the NCM software while NCM jobs are still running. If the Installer detects running NCM jobs, then you will see this screen, which informs you of the number:

In performing work through a manual or scheduled job, NCM communicates with network devices and with the Orion platform database, modifying data. Allowing either communication to continue can put your network device(s) or database a risk of being stuck in a state that compromises data.

Therefore, you must stop running jobs before the NCM Installer upgrades the software.
To stop running NCM jobs:

1. Open Task Manager (Ctrl + Alt + Del > Task Manager).
2. Click Processes and highlight configMgmtJob.exe.
3. Click End Process.

Stopping the SCP Server Tray

The NCM Installer detects if the SCP Server Tray application is running and must stop it before proceeding with the upgrade.

To end this application:

1. Open Task Manager (Ctrl + Alt + Del > Task Manager).
2. Click Processes, and then highlight ScpServerTray.exe.
3. Click End Process.

Launching the NCM Installer

To upgrade the NCM software:

1. Log on to the host with a local administrator account.
   Note: Do not install on a domain controller.
2. Launch the executable from the download location.
3. Click Next on the Welcome screen.
4. After backing-up your database, type YES and then click Next.
5. Select I accept the terms of the License Agreement, and then click Next.
6. Click Next to start copying files.
7. Click Finish. The Configuration Wizards starts.
8. Click Next.
9. Verify that Database, Website, and Services are selected, and then click Next.
10. Specify the SQL Server instance where your Orion platform database is installed. If you do not have credentials to access the Orion Platform database’s SQL Server host, you must consult a system administrator for that host or for the SQL Server instance to obtain an appropriate set of SQL Server credentials.

11. Enter the database authentication method (Windows or SQL Server Authentication), and then click Next.

**Notes:**

- The SQL Server instance must support SQL authentication or mixed mode.
- If you are using a local instance of SQL Server Express, use the following syntax to use the default instance: (local)\SQLEXPRESS.
- If you select SQL Authentication, provide an account with sufficient rights to create new databases on the instance. For example, specify the SQL administrator (sa) account.

12. Select the appropriate existing Orion Platform database, and then click Next.

13. Select or create an account with administrator rights on the database, and then click Next.

**Note:** You must supply a strong password. For more information about strong passwords, see the Microsoft website.

14. Click Next to setup the website with default settings or adjust the settings as needed.

15. Click Yes if a website exists with the same settings.

16. Click Next after reviewing the settings and overview configuration plan.

17. Click Finish when the wizard completes.

**Use these post-installation topics as needed to finish setting-up your deployment:**

- Installing an Additional Poller
- Installing an Additional Website
- Removing SolarWinds Network Configuration Manager
- Using SSL Communication with SolarWinds NCM
Chapter 2: Installing and Upgrading SolarWinds Network Configuration Manager

Setting Node Communication Defaults
Using Multiple Connection Profiles
Setting Communication Limits
Configuring Event Logging
Installation Requirements
Scalability
Server Sizing
Licensing SolarWinds Network Configuration Manager
Obtaining a Software License Key
Reviewing Your License
Resetting Your License
SNMP Communication
Additional Polling Engine and Web Console

You can add an additional poller or website to your SolarWinds NCM deployment. An additional website adds versatility in accessing SolarWinds NCM information and an additional poller adds scalability to the regular backup of device configs.

Consult these topics as needed:
Installing an Additional Poller
Installing an Additional Website

Installing an Additional Poller

If you are upgrading to SolarWinds NCM 7.4, before you attempt to install an additional poller on another server, you must first Upgrading NCM Software.

To install or upgrade an additional SolarWinds NCM poller:

2. Launch the SolarWinds-Orion_AdditionalPoller.exe file from the download location on the server that will host your additional poller.
3. Click Next on the Welcome screen.
4. Accept the end user agreement, and then click Next.
5. Click Next to accept the default target directory or set another that you prefer.
6. Click Next to start copying files.
7. Click Finish when the files are finished being copied.
8. If prompted to license the additional poller, click Enter Licensing Information.
9. Review the Welcome text, and then click Next.
10. Specify the SQL Server instance where the Orion platform database is located and enter the authentication method (Windows or SQL Server Authentication).
Chapter 2: Installing and Upgrading SolarWinds Network Configuration Manager

11. Click Next.

   Notes:
   
   - The SQL Server instance must support SQL authentication or mixed mode.
   - If you are using a local instance of SQL Server Express, use the following syntax to use the default instance: (local)\SQLEXPRESS.
   - If you select SQL Authentication, provide an account with sufficient rights to create new databases on the server instance. For example, specify the SQL administrator (sa) account.

12. Click Use an existing database, select the Orion platform database in the list, and then click Next.

13. Click Use an existing account, and then select the account credentials from the list.

14. Click Next.

15. Review the services to install, and then click Next.

16. Click Yes to acknowledge that the SNMP Trap Service will be disabled while the Trap Service is installed.

17. Review the Database and Services to be configured, and then click Next.

18. Click Launch Orion Web and Finish.

Installing an Additional Website

If you are upgrading to SolarWinds NCM 7.4, before you attempt to install an additional website on another server, you must first upgrade the main SolarWinds NCM server.

To upgrade the SolarWinds NCM server see Upgrading NCM Software.

To install or upgrade an additional SolarWinds NCM website:


2. Launch the SolarWinds-Orion_WebOnly.exe file from the download location on the server that will host your additional website.

3. Click Next on the Welcome screen.
Installing an Additional Website

4. Accept the end user agreement, and then click Next.
5. Click Next to accept the default target directory or set another that you prefer.
6. Click Next to start copying files.
7. Click Finish when the files are finished being copied.
8. If prompted to license the additional website, click Enter Licensing Information.
9. Review the Welcome text, and then click Next.
10. Specify the SQL Server instance where the Orion Platform database is located and enter the authentication method (Windows or SQL Server Authentication).
11. Click Next.
   
   Notes:

   - The SQL Server instance must support SQL authentication or mixed mode.
   - If you are using a local instance of SQL Server Express, use the following syntax to use the default instance: (local)\SQLEXPRESS.
   - If you select SQL Authentication, provide an account with sufficient rights to create new databases on the server instance. For example, specify the SQL administrator (sa) account.
12. Click Use an existing database, select the Orion Platform database in the list, and then click Next.
13. Click Use an existing account, and then select the account credentials from the list.
14. Click Next.
15. Accept the default for Website Settings, and then click Next.
16. Click Yes to acknowledge that the website already exists and that you want to proceed.
17. Click Yes to acknowledge that the SNMP Trap Service will be disabled while the Trap Service is installed.
18. Review the services to install, and then click Next.
19. Review the Database, Website, and Services to be configured, and then click Next.

20. Click Launch Orion Web and Finish.
Setting Node Communication Defaults

A number of variables can be set globally and applied to all new nodes added to SolarWinds NCM. You can override the defaults when adding nodes, however.

Though NCM supports SNMPv3 with AES-256, the SNMPWalk utility only supports AES-128. If you need to troubleshoot SNMP related to your node, use SNMPWalk to test the SNMPv3 setting for AES-128, and then set to AES-256 after you have resolved the node’s SNMP-related issue.

To set node communication default parameters:

1. From the web console, click Settings > NCM Settings.
2. Click Global Device Defaults.
3. Enter the appropriate values for the following items:

   **Device Login Information**
   Enter User name, Password, Enable Level and Enable Password to set the level of permission at which access to the device is valid for this connection profile.

   **Communication Transfer Protocol**
   Select a protocol for command/script, config request, and config transfer operations.

   **Transfer Ports**
   Set the Telnet and SSH port to whatever ports are allowed given the rules on your network.

   **Reset all devices to use Global Settings**
   Selecting this setting tells NCM to override connection profiles and device settings with the Global Device Defaults.

4. Click Submit.
To override default settings for a particular node:

1. From the web console, under Node & Group Management, click **Manage Nodes**.
2. Use the **Group by** control to organize the node list.
3. Select the relevant node in the list.
4. Click **Edit Properties**.
5. Scroll down to NCM Properties.
6. Edit logon and communication information.
7. Click **Submit**.
Manage Connection Profiles

A connection profile is a global device logon that you apply to one or more NCM-managed devices. Define multiple connection profiles and apply them as needed.

To create or edit a connection profile:

1. From the web console, click **Settings > NCM Settings**.
2. **To create a new connection profile**, click **Create New**.
3. **To edit an existing profile**, select a profile, and then click **Edit**.
4. Enter the appropriate values.

**Device Login Information**

Set the level of permission at which access to the device is valid for this connection profile.

**Communication Transfer Protocol**

Select a protocol for command/script, config request, and config transfer operations.

**Transfer Ports**

Set the Telnet and SSH port to whatever ports are allowed given the rules on your network.

**Use for auto-detect**

Make this profile available to NCM in communicating with nodes for which no profile is assigned.

If you have multiple connection profiles set to **Use for auto-detect**, NCM cycles through them before performing the desired operation on a node without a specific connection profile applied. NCM permanently assigns the first connection profile that works to the node.

**Note**: Though selecting **Use for auto-detect** on your connection profiles helps NCM communicate with devices without assigned profiles, we recommend applying a specific connection profile to each managed node.

5. Click **Submit**.
Chapter 2: Installing and Upgrading SolarWinds Network Configuration Manager

Using Multiple Connection Profiles

A connection profile is a global device logon that you apply to one or more NCM managed devices. Define multiple connection profiles and apply them as needed.

To create or edit a connection profile:

1. From the web console, click Settings > NCM Settings.
2. To create a new connection profile, click Create New.
3. To edit an existing profile, select a profile, and then click Edit.
4. Enter the appropriate values.

   Device Login Information
   
   Set the level of permission at which access to the device is valid for this connection profile.

   Communication Transfer Protocol
   
   Select a protocol for command/script, config request, and config transfer operations.

   Transfer Ports
   
   Set the Telnet and SSH port to whatever ports are allowed given the rules on your network.

   Use for auto-detect
   
   Make this profile available to NCM in communicating with nodes for which no profile is assigned.

   If you have multiple connection profiles set to Use for auto-detect, NCM cycles through them before performing the desired operation on a node without a specific connection profile applied. NCM permanently assigns the first connection profile that works to the node.

   Note: Though selecting Use for auto-detect on your connection profiles helps NCM communicate with devices without assigned profiles, we recommend applying a specific connection profile to each managed node.

5. Click Submit.
Setting Communication Limits

Define timeout values and retry numbers for ICMP, SNMP, Telnet, and SSH communication.

1. From the web console, click Settings > NCM Settings.
3. Enter timeout settings for each protocol.
   • ICMP has a default timeout of 2500 milliseconds.
   • Enter the data portion of the ICMP packet. The default is SolarWinds Network Configuration Manager Version 7.4.
   • SNMP has a default timeout of 1000 milliseconds with 1 retry.
   • Telnet/SSH both have default connection timeouts of 45 seconds and prompt timeouts of 15 seconds.
4. Click Submit.
Chapter 2: Installing and Upgrading SolarWinds Network Configuration Manager

Configuring Event Logging

Log events associated with a specific function of SolarWinds NCM to keep a detailed record of events.

1. From the web console, click Settings > NCM Settings.
2. Click Advanced.
3. Select all log types for which to keep verbose log information. This information aids in troubleshooting.
   
   **Note**: Logs are stored in the Logging folder found in your installation directory. By default this is \Program Data\SolarWinds\Logs\Orion\NCM\Logging.

4. Click Enable Session Tracing to create a log file of each telnet session and troubleshoot communication node by node.
5. Click Submit.

The following areas in SolarWinds NCM provide verbose logging options:

**Scheduled Jobs**

Logs scheduled job events, including time completed and individual item success or failure. For example, the failure to download an individual configuration file included in the job.

**Inventory Monitor**

Logs inventory events, including SNMP timeouts, SNMP community string error messages, and status changes.

**Database Updates**

Logs database events, including backup and connectivity events.

**Real Time Config Change Detection**

Logs real time configuration change detection events, including change events, notification success and failure messages, and device connectivity events.

**Security**

Logs security events, including logon failures, account modifications, and global security setting changes.
Using SSL Communication with SolarWinds NCM

SolarWinds NCM supports the use of Secure Sockets Layer certificates to enable secure communications with the Orion Web Console. Secure SSL communications are conducted over port 443.

An SSL certificate must be installed on your SolarWinds NCM server. For more information, see the SolarWinds Knowledge Base.

To enforce SSL connections to the Orion Web Console:

1. Log on as an administrator to your main SolarWinds NCM server.
2. Click Start > Control Panel > Administrative Tools > Computer Management.
3. Expand Services and Applications > Internet Information Services (IIS) Manager > Web Sites.
4. Right click SolarWinds NetPerfMon, and then click Properties.
5. Click the Web Site tab.
6. Confirm that SSL port is set to 443, and then click Apply.
7. Click Advanced.
8. If the Multiple SSL identities for this Web site field does not list the IP address for the Orion Web Console with SSL port 443, complete the following steps:
   a. Click Add, and then select the IP address of the Orion Web Console.
      Note: As it was set initially in the Configuration Wizard, this option is usually set to (All Unassigned). If the IP address of the Orion Web Console was not initially set to (All Unassigned), select the actual, configured IP address of the Orion Web Console.
   b. Type 443 as the TCP port and click OK.
10. Click Edit in the Secure communications section.
11. Select Require secure channel (SSL), and then click OK.
12. Click Apply.
13. Click OK to exit.
Repairing SolarWinds Network Configuration Manager

Repair a malfunctioning NCM installation with the Programs and Features.

**Warning:** If you install or make changes to the Orion platform website, the Configuration Wizard reboots your IIS server, shutting down all SolarWinds products on the server during the configuration operation. Any websites hosted by the server are stopped and restarted during this process.

**To repair SolarWinds NCM:**

1. Launch SolarWinds Configuration Wizard.
2. Select the components you want to repair or modify, and then click **Next**.
3. Specify the appropriate SQL Server instance and authentication method, and then click **Next**.

**Notes:**

- The SQL Server instance must support SQL authentication or mixed mode.
- If you are using a local instance of SQL Server Express, use the following syntax to use the default instance: (local)\SQLEXPRESS.
- If you select SQL Authentication, provide an account with sufficient rights to create new databases on the server instance. For example, specify the SQL administrator (sa) account.

4. Select the appropriate Orion platform, and then click **Next**.
5. Create a new database account and password or select an existing account on the database server.
   **Note:** You must supply a strong password. For more information about strong passwords, see the [Microsoft website](https://microsoft.com).
6. Click **Next**.
7. Review the services the wizard will install, and then click **Next**.
8. Review the configuration the wizard will change, and then click **Next**.
9. Review the Configuration Summary, and then click **Finish**.
Removing SolarWinds Network Configuration Manager

To remove SolarWinds NCM from a server, you must remove both SolarWinds Orion Network Configuration Manager and SolarWinds Orion NCM-NPM Integration. Failure to remove both components will prevent a future installation on the server.

To remove SolarWinds NCM:

1. Open Add and Remove Programs in the Windows Control Panel.
2. Select SolarWinds Orion Network Configuration Manager, and then click Remove.
3. Select SolarWinds Orion NCM-NPM Integration, and then click Remove.
5. Reboot the server.
Moving SolarWinds Network Configuration Manager

To move SolarWinds Network Configuration Manager to another computer:

1. Log on to the NCM server host with an administrator account.
2. Click SolarWinds > Advanced Features > SQL Database Manager to open the Orion SQL Database Manager.
   
   **Note:** If your SQL Server is not listed, add your server to the list. For details, see Adding a Server to SolarWinds Database Manager.

3. Select your Orion platform database in the left pane of the Database Manager window, and then click Database > Backup Database.
4. Type a description of the database backup and specify a path and file name for the backup file. Save your database backup to a temporary storage area.
   
   **Note:** Ensure the target location has sufficient available disk space.

5. Click OK.
6. Use License Manager in the SolarWinds program group to reset your current license. This makes it available for your new implementation.
7. Log on to the new computer and install SolarWinds Network Configuration Manager. For details, see Installing SolarWinds Network Configuration Manager.
Licensing SolarWinds Network Configuration Manager

SolarWinds Network Configuration Manager can manage almost any network device, including routers, switches, and firewalls. Any of your version 3 or earlier SNMP enabled devices can provide configuration files to SolarWinds Network Configuration Manager. It is licensed by the number of nodes. A node is defined as an entire device, such as a router, switch, server, access point, or modem.

There are seven types of licenses available:

- Up to 50 devices (DL50)
- Up to 100 devices (DL100)
- Up to 200 devices (DL200)
- Up to 500 devices (DL500)
- Up to 1000 devices (DL1000)
- Up to 3000 devices (DL3000)
- Unlimited devices (DLX)

Obtaining a Software License Key

**Note:** Versions of the NCM software that are released during the release candidate period have a limited license. In upgrading your NCM software, even if the software does not change from the release-to-manufacture (RTM) to the general availability (GA) distribution, you must reapply your license upon the software’s official release.

From the appropriate server in your deployment, navigate to the SolarWinds customer portal to obtain your activation key.

- If you are deploying SolarWinds NCM on one server and integrating with Orion platform products on a different server, then you must install the SolarWinds NCM license on the server running the other Orion platform product. For example, if SolarWinds NCM and SolarWindsNPM are integrated but installed on different machines, install the SolarWinds NCM license on the machine that is hosting SolarWinds NPM.
- If you are deploying SolarWinds NCM standalone or on a single integrated server, you must install the SolarWinds NCM license on that server.
Chapter 2: Installing and Upgrading SolarWinds Network Configuration Manager

Licensing with Internet Access

Select I have internet access and an activation key…, enter your Activation Key, and click Next. If applicable, select I access the internet through a proxy server.

Licensing without Internet Access

Select This server does not have internet access…, click Next, and complete the steps provided.

Reviewing Your License

1. From the web console, click Settings.
2. Click NCM Settings.
3. Click Node Licensing.

Resetting Your License

SolarWinds License Manager is a free utility that migrates Orion licenses from one computer to another without contacting SolarWinds.

Note: You must install License Manager on a computer with the correct time. If the time on the computer is off by five minutes from Greenwich Mean Time, you cannot reset a license. Time zone settings do not cause this issue.

Installing License Manager

Install License Manager on the computer from which you are migrating currently licensed products.

1. Start the License Manager Setup in the SolarWinds program folder.
2. Click I Accept to accept the SolarWinds EULA.
3. Click Install.

Deactivating a License on the Current Computer

You must run License Manager on the computer where the currently licensed SolarWinds product is installed.
1. Start the **License Manager** in the SolarWinds program folder.
2. Select the product you want to deactivate on this computer.
3. Click **Deactivate**.
4. Specify your SolarWinds Customer ID and password when prompted, and then click **Deactivate**.

**Activating a License on a New Computer**

The deactivated license is now available for activation on a new computer. Log on to the computer where you want to install your products and begin the installation procedure. The license you deactivated earlier is assigned to the new installation.

**About the SolarWinds Orion Platform Database**

Microsoft SQL Server 2008 Express Edition is distributed with SolarWinds Network Configuration Manager. SQL Server 2008 Express Edition supports a maximum database size of 10GB, is limited to 1GB of RAM use, and takes advantage of only 1 CPU in a multi-processor server. For more information about SQL Server installation, see the [Microsoft website](https://docs.microsoft.com).

We recommend that you create the database on a separate SQL Server host (not the NCM host). To increase performance, we recommend using a remote SQL Server host if you are installing SolarWinds NCM on the same host as SolarWinds NPM.

**Warnings:**

The following characters cannot be included in the database name:

- Asterisk (*)
- Closing square bracket (]
- Colon (:)
- Semicolon (;)
- Single quote (’)
- Double quote (")
- Backward slash (\)
- Forward slash (/)
Chapter 2: Installing and Upgrading SolarWinds Network Configuration Manager

- Less than (<)
- Greater than (>)
- Question mark (?)

The following characters cannot be included in the user name or password of the database account:

- Semicolon (;)
- Single quote (')

**SNMP Communication**

SolarWinds Network Configuration Manager uses SNMP communication to collect inventory information. Properly configure SNMP on all devices from which you want to collect detailed information.
Chapter 3: Managing Nodes

SolarWinds Network Configuration Manager helps you manage, organize, and track changes to your network devices. These devices are known collectively as nodes and include switches, routers, firewalls, and Windows servers. Review the following sections to begin managing nodes:

- Adding Nodes
- Using the Network Sonar Discovery Results Wizard
- Unmanaging and Remanaging Nodes
- Managing End of Support and End of Sales (EOS)
- Refreshing EOS Dates
- Assigning EOS Dates
- Ignoring Devices in EOS Management
- Exporting EOS Information
- Deleting EOS Data
- How to Filter EOS Data
- Understanding NCM Macros
- Using Custom Macros
- Searching for Network Addresses
- Finding IP Addresses
- Finding MAC Addresses
- Finding Hostnames
- Find Connected Port for a Host (SolarWinds NPM Integration)
- Understanding How Addresses are Found
- Viewing Node Interface Details
Chapter 3: Managing Nodes

Adding Nodes

Add nodes using the SolarWinds Network Sonar, add them individually, or import a list of IP addresses or hostnames from a file.

Consult the following topics as needed:

- Adding Nodes with Network Discovery
- Managing NCM Nodes

Adding an Individual Node for Monitoring

1. From the web console, click Settings.
2. Under Node & Group Management, click Manage Nodes.
3. Click Add Node on the Node Management toolbar.
4. Type the hostname or IP Address of the node you want to add.
5. If you only want to use ICMP to monitor node status, response time, or packet loss for the added node, select Status Only (ICMP).
6. If you want to add an External node to monitor a hosted application with Orion platform products (for example, SolarWinds SAM), select External.Node. SolarWinds NCM does not collect or monitor any network performance data from nodes designated as External. The External status is reserved for nodes hosting applications that you want to monitor with SolarWinds Server & Application Monitor.
7. To use SNMP to monitor the added node, confirm that **ICMP (Ping only)** is cleared and complete the following steps:
   
a. Select the SNMP Version for the added node.  

   **Notes:**
   
   - SolarWinds NCM uses SNMPv2c by default. If the device you are adding supports or requires the enhanced security features of SNMPv3, select SNMPv3. (NCM supports SNMPv3 with AES-256.) If SNMPv2c is enabled on a device you want to monitor, by default, SolarWinds NCM uses SNMPv2c to poll for performance information.
   
   - To only poll using SNMPv1, disable SNMPv2c on the device to be polled.
   
b. If the SNMP port on the added node is not the Orion platform product default of 161, type the actual port number. If the added node supports 64-bit counters, select **Allow 64-bit counters** to use them.  

   **Note:** Orion platform products support 64-bit counters, however they can exhibit erratic behavior depending on manufacturer implementation. If you notice peculiar results when using them, disable 64-bit counters for the device in the Node Details view and contact the hardware manufacturer.

8. To use SNMPv2c to monitor the added node, enter valid community strings for the added node.  

   **Note:** The Read/Write Community String is optional, but the public Community String is required.

9. To use SNMPv3 to monitor the added node, enter the following:
   
   - SNMPv3 User name and Context
   - SNMPv3 Authentication Method and Password/Key
   - SNMPv3 Privacy/Encryption Method and Password/Key

10. If you are using SNMP to communicate with your added node, click **Validate SNMP** to confirm your settings.
11. Click **Next**.

12. Select the interfaces, volumes, and interface charts to monitor for the added node, and then click **Next**.

13. To edit the default polling settings for your added node, change the Node Status Polling or Collect Statistics Every values in the Polling area of the Change Properties page.

   **Notes:**
   - The Node Status Polling value is the number of seconds between status checks performed on the added node.
   - The Collect Statistics Every value is the period of time between updates made to displayed statistics for the added node.

14. If you defined custom properties for monitored nodes, enter appropriate values for the added node in the Custom Properties area of the Change Properties page.

   **Notes:**
   - The Custom Properties area is empty if you have not defined any custom properties for monitored nodes. For more information on how to add custom properties, see [Creating Custom Properties](#).
   - SolarWinds NCM ignores custom properties that use words from the list of reserved words. For details, see [Reserved Words](#).

15. Click **Add Node to NCM**.

16. Click **OK, Add Node** when you have completed properties configuration.

17. If you successfully added the node, click **OK**.

---

**Adding Nodes with Network Discovery**

1. From the web console, click **Settings**.

2. Under Getting Started with Orion, click **Discover Network**.

3. **If you want to create a new discovery**, click **Add New Discovery**.

4. **If you have already defined a network discovery**, select one of the following on the Network Sonar Discovery tab:
Adding Nodes with Network Discovery

- If you want to edit an existing discovery before using it, select the discovery, and then click Edit.

- If you want to use an existing discovery to rediscover your network, select the discovery, click Discover Now, and then complete the Network Sonar Results Wizard after discovery completes.

- If you want to import some or all devices found in a defined discovery that you may not have already imported for monitoring, select a currently defined discovery, and then click Import All Results.

- If you want to import any newly enabled devices matching a defined discovery profile, select a currently defined discovery, and then click Import New Results.

- If you want to delete an existing discovery profile, select a currently defined discovery, and then click Delete.

   For more information about network discovery results, see Using the Network Sonar Discovery Results Wizard.

5. If the devices on your network do not require community strings other than the default strings public and private provided by SolarWinds NCM, click Next on the SNMP Credentials view.
6. **If any of your network devices require community strings other than public and private, or if you want to use an SNMPv3 credential**, complete the following steps to add the required SNMP credential:

   **Notes:**
   Repeat the following procedure for each new community string. To speed up discovery, highlight the most commonly used community strings on your network, and then use the arrows to move them to the top of the list. NCM supports SNMPv3 with AES-256.

   a. Click **Add New Credential**, and then select the SNMP Version of your new credential.

   b. **If you are adding an SNMPv1 or SNMPv2c credential**, provide the new SNMP Community String.

   c. **If you are adding an SNMPv3 credential**, enter the following information for the new credential:
      - User Name, Context, and Authentication Method
      - Authentication Password/Key, Privacy/Encryption Method and Password/Key, if required

   d. Click **Add**.

   e. On the SNMP Credentials view, click **Next**.

7. **If you want to add Windows credentials for WMI collections**, click **Add New Credential**:

   a. Choose and name the credential.

   b. Enter the user name with privileges to accomplish WMI polling.

   c. Enter and confirm the user account password.

   d. Click **Add**.

8. **If you want to discover devices located on your network within a specific range of IP addresses**, complete the following procedure:

   **Note:** Only one selection method may be used per defined discovery.
Adding Nodes with Network Discovery

a. Click **IP Ranges** in the Selection Method menu, and then, for each IP range, provide a Start address and an End address.
   
   **Note:** Scheduled discovery profiles should not use IP address ranges that include nodes with dynamically assigned IP addresses (DHCP).

b. *If you want to add another range,* click **Add More** and repeat the previous step.
   
   **Note:** If you have multiple ranges, click **X** to delete an incorrect range.

c. *If you have added all the IP ranges you want to poll,* click **Next.**
9. **If you want to discover devices connected to a specific router or on a specific subnet of your network**, complete the following procedure:

   **Note:** Only one selection method may be used per defined discovery.

   a. Click **Subnets** in the Selection Method menu.

   b. **If you want to discover on a specific subnet**, click **Add a New Subnet**, enter a Subnet Address and Subnet Mask, and then click **Add**.

      **Note:** Repeat this step for each additional subnet you want to poll.

   c. **If you want to discover devices using a seed router**, click **Add a Seed Router**, enter the IP address of the Router, and then click **Add**.

      **Notes:**

      - Repeat this step for each additional seed router you want to use.

      - Network Sonar reads the routing table of the designated router and offers to discover nodes on the Class A network (255.0.0.0 mask) containing the seed router and, if you are discovering devices for an SolarWinds NPM installation, the Class C networks (255.255.255.0 mask) containing all interfaces on the seed router, using the SNMP version chosen previously on the SNMP Credentials page.

      - Networks connected through the seed router are not automatically selected for discovery.

   d. Confirm that all networks on which you want to conduct your network discovery are selected, and then click **Next**.
10. *If you already know the IP addresses or hostnames of the devices you want to discover*, complete the following procedure:

   a. Click **Specific Nodes** in the Selection Method menu.

   b. Type the IPv4 addresses or hostnames of the devices you want to discover for monitoring.

      **Note:** Type only one IPv4 address or hostname per line.

   c. Click **Validate** to confirm that the provided IPv4 addresses and hostnames are assigned to SNMP-enabled devices.

   d. *If you have provided all the IPv4 addresses and hostnames you want to discover*, click **Next**.
11. Configure the options on the Discovery Settings view, as detailed in the following steps. Provide a Name and Description to distinguish the current discovery profile from other profiles you may use to discover other network areas.

**Note:** This Description displays next to the Name in the list of available network discovery configurations on the Network Sonar view.

a. Position the slider or type a value, in milliseconds, to set the SNMP Timeout.

   If you are encountering numerous SNMP timeouts during Network Discovery, increase the value for this setting. The SNMP Timeout should be at least more than double the time it takes a packet to travel the longest route between devices on your network.

b. Position the slider or type a value, in milliseconds, to set the Search Timeout.

   **Note:** The Search Timeout is the amount of time Network Sonar Discovery waits to determine if a given IP address has a network device assigned to it.

c. Position the slider or type a value to set the number of SNMP Retries.

   **Note:** This value is the number of times Network Sonar Discovery will retry a failed SNMP request, defined as any SNMP request that does not receive a response within the SNMP Timeout defined above.

d. Position the slider or type a value to set the Hop Count.

   **Note:** If the Hop Count is greater than zero, Network Sonar Discovery searches for devices connected to any discovered device. Each connection to a discovered device counts as a hop.
Adding Nodes with Network Discovery

e. Position the slider or type a value to set the Discovery Timeout.

  Note: The Discovery Timeout is the amount of time, in minutes, Network Sonar Discovery is allowed to complete a network discovery. If a discovery takes longer than the Discovery Timeout, the discovery is terminated.

12. If you only want to use SNMP to discover devices on your network, select Use SNMP only.

  Note: By default, Network Sonar uses ICMP ping requests to locate devices. Most information about monitored network objects is obtained using SNMP queries.

13. If multiple Orion polling engines are available in your environment, select the Polling Engine you want to use for this discovery.

14. Click Next.

15. If you want the discovery you are currently defining to run on a regular schedule, select either Custom or Daily as the discovery Frequency, as shown in the following steps:

  Notes:

  • Scheduled discovery profiles should not use IP address ranges that include nodes with dynamically assigned IP addresses (DHCP).
  • Default Discovery Scheduling settings execute a single discovery of your network that starts immediately, once you click Discover.
  • Results of scheduled discoveries are maintained on the Scheduled Discovery Results tab of Network Discovery.

  a. If you want to define a custom discovery schedule to perform the currently defined discovery repeatedly in the future, select Custom, and then provide the period of time, in hours, between discoveries.

  b. If you want your scheduled discovery to run once daily, select Daily, and then provide the time at which you want your discovery to run every day, using the format HH:MM AM/PM.
16. *If you do not want to run your network discovery at this time*, select No, don't run now, and then click Save or Schedule, depending on whether you have configured the discovery to run once or on a schedule, respectively.

17. To run Network Sonar discovery immediately, click Discover.

**Note:** Because some devices may serve as both routers and switches, the total number of Nodes Discovered may be less than the sum of reported Routers Discovered plus reported Switches Discovered. For information on importing the results of your discovery, see Using the Network Sonar Discovery Results Wizard.

### Managing NCM Nodes

**Note:** If you remove a node from NCM, all data associated with the node, such as configs, and inventory data, are also removed.

**To add node(s) to NCM:**

1. From the web console, under All Nodes, click Manage Nodes.
2. Select a desired grouping in the left pane or select No Grouping.
3. Click More Actions > Add Nodes to NCM.

**To adjust NCM status of a specific node:**

1. From the web console, under All Nodes, click Manage Nodes.
2. Select a desired grouping in the left pane or select No Grouping.
3. Select the node, and then click Edit Properties.
4. Select the node under Search Nodes, and then click Manage Node.
5. Scroll down to the last section with the property Manage node(s) with NCM.
6. *If you currently do not want the node managed with NCM*, select No.
7. *If you never want the node(s) managed by NCM*, select Never.
8. *If you want to manage the node with NCM*, select Yes. The NCM Properties are listed with their current values.
9. Adjust the values as needed, and then click Submit.
10. Consult the NCM-Licensed column to review node status.
To edit the properties of an NCM node:

1. From the web console, under All Nodes, click Manage Nodes.
2. Select a grouping in the left pane or select No Grouping.
3. Select the node, and then click Edit Properties.
4. Scroll down to the property Manage node(s) with NCM.
5. Select Yes, No, or Never.
6. Adjust other values as needed, and then click Submit.

Adding and Managing NCM Nodes Resource

This resource allows you to add and remove nodes from your NCM environment. Click Enable Import from Discovery to allow the Network Discovery Engine to import newly discovered nodes into NCM.

To find a specific node:

1. From the web console, click CONFIGS > NCM Settings.
2. Under NCM Node Management, click Add or Manage Nodes.
3. To find a specific node, enter an IP address or hostname in the Search window, and then click Search.

To add or edit an NCM node:

1. Use the Group by control to organize the list of nodes.
2. Click the Name(s) of the node(s) you want to license in NCM, and then click Edit Properties.
3. Select the appropriate option for Manage Node(s) with NCM.

Using the Network Sonar Discovery Results Wizard

The Network Sonar Results Wizard directs you through the selection of network devices for monitoring. It opens whenever discovery results are requested: when the Network Sonar Discovery Wizard completes or when either Import All Results or Import New Results is clicked for a selected discovery.

Note: The Results Wizard automatically adds non-server nodes as NCM nodes if there is at least one connection profile setup with use for auto detect enabled.
Chapter 3: Managing Nodes

To select results of a network discovery:

1. From the web console, click **Settings**.
2. Under Getting Started with Orion, click **Discovery Central**.
3. Under Network Discovery, click **Discovery My Network**.
4. Select an existing discovery profile, and then click **Import New Results**.
5. On the Device Types to Import page, select the device types you want to monitor, and then click **Next**.
   
   **Note:** If you are not sure you want to monitor a specific device type, select the device type in question. If later you decide not to monitor a selected device, simply delete the device using Web Node Management.

6. Select the interface types you want to monitor on the Interface Types to Import page, and then click **Next**.
   
   **Note:** If you are not sure you want to monitor a specific interface type, select the interface type in question. If later you decide not to monitor a selected interface, delete it using Web Node Management.

7. On the Volume Types to Import page, select the volume types you want to monitor, and then click **Next**.
   
   **Note:** If you are not sure you want to monitor a specific volume type, select the volume type in question. If later you decide not to monitor any volume of the selected type, delete the volume using Web Node Management.

8. Select valid states for imported interfaces, and then click **Next**.
   
   **Note:** By default, SolarWinds NCM imports interfaces that are discovered in an Operationally Up state. However, because interfaces may cycle on and off intermittently, the Import Settings page allows you to select interfaces found in Operationally Down or Shutdown states as well.

9. **If there are any devices on the Import Preview that you do not ever want to import**, select the device to ignore, and then click **Ignore**. Selected nodes are added to the Discovery Ignore List.

10. Confirm that the network objects you want to monitor are selected on the Import Preview page, and then click **Import**.

11. After the import completes, click **Finish**. Imported devices display in the All Nodes resource.
**Viewing Node Interface Details**

View the following interface details about a node:

- Interface/Port Status
- Interface Traffic
- Interface/Port Configuration
- Time data was last transmitted/received
- Cisco Discovery Protocol (CDP)
- User activity
- Real-time ARP cache

**To view the interface details of a specific node:**

1. Click the Interfaces tab.
2. Select a category from the Interface Details list.
3. Click **Refresh** to view the selected statistics.
4. Select **Auto Refresh** to update statistics every 30 seconds.
5. To change the Auto Refresh time interval:
   a. Click **File > Settings**.
   b. Click **Interfaces** under Node Details.
   c. Adjust the slider to the appropriate interval.
   d. Click **OK**.
Chapter 3: Managing Nodes

Working with Firmware Vulnerability Data

SolarWinds NCM imports into its database the firmware vulnerability warnings provided by National Institute of Standards and Technology (NIST). NCM sources that data into the Firmware Vulnerabilities resources on the Config Summary page.

Use these topics to work with firmware vulnerability data and the NCM nodes it impacts:

Viewing Firmware Vulnerability Reports
Troubleshooting Firmware Vulnerability Reports
Managing Firmware Vulnerability Settings
Vulnerability Summary

Viewing Firmware Vulnerability Reports

The Orion platform includes eight reports on network device firmware vulnerabilities:

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nodes for Each Vulnerability</td>
<td>Lists all vulnerabilities and the corresponding nodes at risk.</td>
</tr>
<tr>
<td>Vulnerabilities for Each Node</td>
<td>Lists nodes with their corresponding vulnerabilities.</td>
</tr>
<tr>
<td>Vulnerabilities for Each Node - Waiver</td>
<td>Lists nodes with their corresponding vulnerabilities with a status of Waiver.</td>
</tr>
<tr>
<td>Vulnerabilities for Each Node - Remediation Planned</td>
<td>Lists nodes with their corresponding vulnerabilities with a status of Remediation Planned.</td>
</tr>
<tr>
<td>Vulnerabilities for Each Node - Potential</td>
<td>Lists nodes with their corresponding vulnerabilities with a status of Potential, meaning that the vulnerability has not yet been verified.</td>
</tr>
<tr>
<td>Vulnerabilities for Each Node - Not</td>
<td>Lists nodes with their corresponding vulnerabilities with a status of Not Applicable, meaning that the vulnerability</td>
</tr>
</tbody>
</table>
These reports list vulnerabilities discovered in the last run of the vulnerability matching logic based on data last downloaded from sources in Vulnerability Data Import Settings (NCM Settings > Advanced > Firmware Vulnerability Settings).

To view a vulnerability report:

1. From the web console, click Reports.
2. Use the Group by control to locate a report.
3. Click the report.

If a Cisco IOS or Cisco Adaptive Security Appliance device does not show up with others of its type in a vulnerability, check for errors in the Vulnerability Log (${All Users Profile}\Application Data\SolarWinds\Logs\Orion\NCM\VulnLib.log).

The difference between the Nodes for Each Vulnerability and Vulnerabilities reports is that CVEs are listed in the Caption and Entry ID columns, and the information is organized by vulnerabilities and nodes, respectively.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicable</td>
<td>does not apply.</td>
</tr>
<tr>
<td>Vulnerabilities for Each Node - Confirmed</td>
<td>Lists nodes with their corresponding vulnerabilities with a status of Confirmed, meaning that the vulnerability has been confirmed but no remediation is planned.</td>
</tr>
<tr>
<td>Vulnerabilities for Each Node - Remediated</td>
<td>Lists nodes with their corresponding vulnerabilities with a status of Remediated, meaning that the vulnerability has been confirmed and then remediated.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caption/Entry ID</td>
<td>The Common Vulnerabilities and Exposures (CVE) identifier for a specific vulnerability being described. CVE numbering authorities often provide identifiers for their own products.</td>
</tr>
</tbody>
</table>
Table:

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS Version</td>
<td>The operating system software version (s) to which the CVE pertains.</td>
</tr>
<tr>
<td>IOS Image</td>
<td>The operating system software image to which the CVE pertains.</td>
</tr>
<tr>
<td>URL</td>
<td>The location of the CVE on the NIST website from which NCM obtained</td>
</tr>
<tr>
<td></td>
<td>vulnerability data.</td>
</tr>
<tr>
<td>CVSS V2 Base Score</td>
<td>The Common Vulnerability Scoring System (CVSS) uses a set of metrics to</td>
</tr>
<tr>
<td></td>
<td>determine the severity of a determined vulnerability. The metrics analyze</td>
</tr>
<tr>
<td></td>
<td>and assign a value to these aspects related to exploiting a vulnerability:</td>
</tr>
<tr>
<td></td>
<td>access required, access complexity, authentication requirement, confidentiality</td>
</tr>
<tr>
<td></td>
<td>protection, integrity or imperviousness of data to change, and availability</td>
</tr>
<tr>
<td></td>
<td>safeguards.</td>
</tr>
<tr>
<td>Severity</td>
<td>A CVSS score determines the severity of a vulnerability as Low (0-3.9),</td>
</tr>
<tr>
<td></td>
<td>Medium (4.0-6.9), or High (7.0-10.0).</td>
</tr>
<tr>
<td>State</td>
<td>State to which this CVE has been set for one or more NCM-managed nodes.</td>
</tr>
<tr>
<td>Last State Change</td>
<td>Date the state of the CVE last changed for one or more NCM-managed nodes.</td>
</tr>
</tbody>
</table>

**Troubleshooting Firmware Vulnerability Reports**

If a Cisco IOS or Cisco Adaptive Security Appliance device does not show up with others of its type in a vulnerability announcement, check for errors in the **Vulnerability Log** (${All Users Profile}\Application Data\SolarWinds\Logs\Orion\NCM\VulnLib.log).
## Vulnerability Summary

This resource provides information on the Common Vulnerabilities and Exposures (CVE) system and enables you to apply a CVE state to one or more managed nodes. Select the desired state, select the nodes to which the CVE applies in this state, and click **Submit**.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVSS V2 Base Score</td>
<td>The Common Vulnerability Scoring System (CVSS) uses a metrics to determine the severity of a determined vulnerability. The metrics analyze and assign a value to these aspects related to exploiting a vulnerability:</td>
</tr>
<tr>
<td></td>
<td>• Access required</td>
</tr>
<tr>
<td></td>
<td>• Access complexity</td>
</tr>
<tr>
<td></td>
<td>• Authentication requirement</td>
</tr>
<tr>
<td></td>
<td>• Confidentiality protection</td>
</tr>
<tr>
<td></td>
<td>• Integrity or imperviousness of data to change</td>
</tr>
<tr>
<td></td>
<td>• Availability safeguards</td>
</tr>
<tr>
<td>Severity</td>
<td>A CVSS score determines the severity of a vulnerability as:</td>
</tr>
<tr>
<td></td>
<td>• Low (0-3.9)</td>
</tr>
<tr>
<td></td>
<td>• Medium (4.0-6.9)</td>
</tr>
<tr>
<td></td>
<td>• High (7.0-10.0)</td>
</tr>
<tr>
<td>URL</td>
<td>The source of the CVE information.</td>
</tr>
<tr>
<td>Published Date</td>
<td>Date the CVE was published.</td>
</tr>
<tr>
<td>Summary</td>
<td>Explanation of how the CVE puts your device(s), network, and data at risk.</td>
</tr>
<tr>
<td>State</td>
<td>The state of the vulnerability with regards to managed nodes:</td>
</tr>
<tr>
<td></td>
<td>• Potential vulnerability</td>
</tr>
<tr>
<td></td>
<td>• Confirmed vulnerability</td>
</tr>
</tbody>
</table>
Chapter 3: Managing Nodes

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Not applicable</td>
<td></td>
</tr>
<tr>
<td>• Remediation planned</td>
<td></td>
</tr>
<tr>
<td>• Remediated, Waiver</td>
<td>Provides an option to apply selected state to some or all nodes.</td>
</tr>
</tbody>
</table>

**Managing Firmware Vulnerability Settings**

Adjust settings and click **Submit** to save changes.

**Vulnerability Search Settings**

1. Select **Enable daily auto run of vulnerability matching logic** if you want such frequency.
2. Click **Run Now** to check the database for vulnerability matches on demand.
3. Click **Delete All** if you do not wish to retain found vulnerabilities.

**Vulnerability Data Import Settings**

1. Set the path to the file containing vulnerability announcements that NCM imports.
2. Click **Validate** to check the assigned path.
3. Set the path to the URLs where vulnerability announcements can be imported into the database.
4. Click **Add New** to set an additional URL where vulnerability announcements can be imported into the database.

**Vulnerability Alerts**

Set the **Vulnerability alert score** threshold. Five is the default.

**Adding Firmware Vulnerability Files**

You can add direct URLs to vulnerability announcements or manually save the XML files to a location on your SolarWinds NCM server.
Saving an XML source to your SolarWinds NCM server

1. Log on to your SolarWinds NCM server.
2. Navigate to the folder used to save your vulnerability announcement XML files. By default, the folder is located at C:\ProgramData\SolarWinds\NCM\Vuln\Xml.
3. Copy a vulnerability announcement XML file to that folder.

Changing the Vulnerability Announcements folder

1. From the web console, click CONFIGS > NCM Settings.
2. Under Advanced, click Firmware Vulnerability Settings.
3. Enter the location of the folder that includes the XML files of vulnerability announcements in Vulnerability Data Import Settings.
4. Click Submit.

Adding direct URLs

1. From the web console, click CONFIGS > NCM Settings.
2. Under Advanced, click Firmware Vulnerability Settings.
3. Click Add New in Vulnerability Data Import Settings.
4. Select Direct urls to xml vulnerability announcements data files to be automatically downloaded and imported into database.
5. Enter the URL to the vulnerability announcements XML file.
6. To test the file, paste the URL into a browser. The server should return XML data.
7. Click Submit.
Managing End of Support and End of Sales (EOS)

The EOS resources help you search vendor-published end of support and sales dates associated with your NCM devices. You can also search for specific nodes and assign EOS dates based on information related to device models.

When you load the EOS resource (CONFIGS > EOS) NCM shows the EOS data currently associated with your NCM devices.

**Note:** SolarWinds neither verifies nor supports EOS/EOL data. Consult your vendor with any data-related issues or questions.

To manage EOS data use the steps in the following sections:

- Refreshing EOS Dates
- Ignoring Devices in EOS Management
- Exporting EOS Information
- Deleting EOS Data
- How to Filter EOS Data

**Refreshing EOS Dates**

NCM maintains a database with EOS data for vendor device models. Based on a schedule, NCM matches EOS data with the machine type of your NCM devices. What you see in the table of the EOS resource is the result of the matching. To make sure you are looking at the latest matches, use Refresh Suggested Dates.

**To refresh suggested EOS dates for your NCM devices:**

1. From the web console, click **CONFIGS > End of Support**.
2. Select the devices for which you want updated data, if available. Use the **Group by** control if necessary.
3. Click **Refresh Suggested Dates**.

**Assigning EOS Dates**

1. From the web console, click **CONFIGS > End of Support**.
2. Select the devices for which you want updated data, if available. Use the **Group by** control if necessary.
3. Click **Assign Dates**.
4. You should see a list of your selected devices on the Assign EOS Data screen under Node Selected. If a device is missing, click Add More Nodes, select the appropriate nodes, and then click OK.

5. Search the table for the model of your selected NCM nodes in the Choose Dates table. If you find it, select that row.

6. Search the table for the model of your selected NCM nodes in the Set EOS Dates table. If you find it, select that row.

The dates listed for a model or series have indications in the Reliability column:

- High indicates that the date(s) are unambiguous and such dates are automatically applied to the relevant devices.
- Medium indicates that the date(s) remains ambiguous due to other incomplete or conflicting information.
- Confirmed indicates that the date(s) were confirmed by an NCM user.

7. If you did not find the model of your selected NCM nodes but want to assign dates anyway, select Option 2 and define your own dates.

8. Add comments as needed.

9. Click Assign.

**Ignoring Devices in EOS Management**

1. From the web console, click CONFIGS > End of Support.

2. Select the devices for which you want updated data, if available.

3. Click Ignore Devices.

4. You should see a list of your selected devices on the Assign EOS Data screen under Node Selected. If a device is missing, click Add More Nodes, select the appropriate nodes, and then click OK.

5. Search the table for the model of your selected NCM nodes in the Choose Dates table. If you find it, select that row.

6. If you did not find the model of your selected NCM nodes, but you want to assign dates anyway, select Option 2 and define your own dates.
Chapter 3: Managing Nodes

7. Add comments as needed.
8. Click **Assign**.

**Exporting EOS Information**

1. From the web console, click **CONFIGS > EOS**.
2. Select the devices for which you want updated data, if available. Use the **Group by** control if necessary.
3. Click **Export**, and then select the format.
4. Select a location.
5. Click **OK**.

**How to Filter EOS Data**

By default, NCM presents data in the End of Support and Sales table for all nodes it manages. NCM collects data either on a daily schedule or when you choose to Refresh Suggested Dates.

You can filter data in the table by column. Each filter you create is applied in the order it is listed above the table. For example, if you first set a filter for Name, NCM filters the Names column before it applies whatever filter comes next in the list of filters.

Setting filters is useful in the following scenarios:

- Displaying which devices reach End of Support or End of Sales at the same time (for example, in the **Next 3 months**)
- Displaying EOS status for devices from the same vendor
- Displaying EOS status on devices in the same subnet

If you want to find the EOS status for a specific device, enter the device name or IP address in the Search window.

**Deleting EOS Data**

1. From the web console, click **CONFIGS > End of Support**.
2. Select the devices for which you want updated data, if available. Use the **Group by** control if necessary.
3. Click **Delete EOS Data**.
4. Click **OK**.
Chapter 3: Managing Nodes

Searching for Network Addresses

SolarWinds Network Configuration Manager can search the entire database (Nodes table, IP Address table, ARP tables, BridgePorts and MAC Forwarding tables, Interfaces) for specific network addresses.

For the best results, add all switches and routers to SolarWinds Network Configuration Manager, and always update your inventory prior to a search (especially when searching for a MAC address).

Consult these topics as needed:
- Finding IP Addresses
- Finding MAC Addresses
- Finding Hostnames
- Understanding How Addresses are Found

Finding IP Addresses

1. From the web console, click CONFIGS.
2. Under Search NCM, type the address pattern you want to find.
   
   For example, 10.199.[2-12].[10-200], would search for nodes 10-100 in the subnets 10.199.3.0 through 10.199.12.0.

3. Click Search.

Finding MAC Addresses

You may need to search all of your configuration files, for example, to see if a MAC address is included in any black lists.

1. From the web console, click CONFIGS.
2. Under Search NCM, type the pattern you want to find.
3. Click Search.

For information on how addresses are found see Understanding How Addresses are Found.

Finding Hostnames

If you network supports DNS, you can search for NCM nodes by hostname.
Understanding How Addresses are Found

1. From the web console, click **CONFIGS**.
2. Under Search NCM, type the pattern you want to find.
3. Click **Search**.

For information on how addresses are found see Understanding How Addresses are Found.

**Understanding How Addresses are Found**

During node inventory, the following tables are populated in the Orion platform database:

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nodes Table</td>
<td>Stores a list of all nodes managed by SolarWinds NCM, along with the declared node properties.</td>
</tr>
<tr>
<td>IP Addresses Table</td>
<td>Stores a list of IP addresses mapped to interface and node IDs.</td>
</tr>
<tr>
<td>Interfaces Table</td>
<td>Stores a list of interfaces, interface indices, interface types, and interface descriptions mapped to node IDs.</td>
</tr>
<tr>
<td>Bridge Ports Table</td>
<td>Stores a list of bridge ports, spanning tree status, spanning</td>
</tr>
</tbody>
</table>
Chapter 3: Managing Nodes

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>tree state, VLAN type, and VLAN ID mapped to node IDs.</td>
</tr>
<tr>
<td>MAC Forwarding Table</td>
<td>Stores a list of MAC addresses, ports, and how the address was mapped to node IDs.</td>
</tr>
<tr>
<td>ARP Tables</td>
<td>Stores a list of data returned from ARP tables and mapped back to node IDs. This information includes interface index, interface ID, MAC address, IP address, and whether the IP address is static or dynamic.</td>
</tr>
</tbody>
</table>

When you search for an IP address, a hostname, or a MAC address, SolarWinds NCM searches these tables for the value and returns all matches.

Where appropriate, returned values include a ranking which reflects how often a MAC address appears in the ARP table for a given port.

**Notes:**

- If you are searching for a MAC address that is part of a VLAN, the results may incorrectly display a rank of 0 for the address.
- If you are only managing switches with SolarWinds NCM, IP addresses will not be returned by the search.
Understanding NCM Macros

NCM macros are used by all NCM web and desktop applications and apply to all editable Node fields.

All NCM macros are enclosed in `{ }`. The macro for system name, for example, is `{SysName}`. You can concatenate any number of macros in each editable node field. For example, the macros `{SysName}` and `{Vendor}` contain the system name and vendor in the field.

SolarWinds NCM can also define macros that point to other macros, and the macro parser can recursively parse the chain of macros applied in the node field.

NCM supports several types of macros:

<table>
<thead>
<tr>
<th>Macro</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nodes Macros</td>
<td>Macros which point to another column in Nodes table.</td>
</tr>
<tr>
<td></td>
<td>For example: <code>{SysName}</code> points to the SysName column in the Nodes table.</td>
</tr>
<tr>
<td></td>
<td>Node macros are unique to each Node.</td>
</tr>
<tr>
<td>Global Macros</td>
<td>Macros defined on the application level and stored in the GlobalSettings table. As their name suggests, the value of these macros is the same for all the nodes. Several global macros, such as <code>{GlobalCommunitySting}</code>, are predefined. You can also create custom global macros.</td>
</tr>
<tr>
<td>Device Template Macros</td>
<td>Macros related to a device vendor and stored in device templates.</td>
</tr>
<tr>
<td></td>
<td>For example: <code>{ConfigType}</code>.</td>
</tr>
</tbody>
</table>
### Macro Description

<table>
<thead>
<tr>
<th>Macro</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu-based Macros</td>
<td>Macros defined to operate with menu-based devices. For example: ${\text{DownArow}}$ simulates sending the Down Arrow key while connected to the device.</td>
</tr>
</tbody>
</table>
Using Custom Macros

A custom macro is a global macro that you create to use in a script, job, or for a specific property that applies across all managed nodes.

Creating a Custom Macro

1. From the web console, click **Settings > NCM Settings**.
2. Under Advanced, click **Manage Macros**.
3. Click **Add New**.
4. Enter a name and value for the new macro. For example: To define a macro to track the provision date and location of devices, use ProvisionAustin1 as the name for devices in Austin, Texas provisioned on a certain date and use the city and date as the value:
   - Macro Name: ProvisionedAustin1
   - Macro Value: Austin 05/10/2015
5. Click **Submit**.

Editing a Custom Macro

1. From the web console, click **Settings > NCM Settings**.
2. Under Advanced, click **Manage Macros**.
3. Select the macro, and then click **Edit**.
4. Modify the value of the macro.
5. Click **Submit**.

Deleting a Custom Macro

1. From the web console, click **Settings > NCM Settings**.
2. Under Advanced, click **Manage Macros**.
3. Select the macro.
4. Click **Delete**.
5. Click **OK**.
Find Connected Port for a Host (SolarWinds NPM Integration)

A SolarWinds NCM integration with SolarWinds NPM allows you to search for currently connected ports on wired or wireless end hosts.

This feature requires that you manage both nodes and interfaces involved in the connection.

The information returned is based on the data available in the Orion database as of the last scheduled discovery of network nodes. It is specified at the top of the table in which search results are presented in this form:

- As of last discovery [MM/DD/YYYY] [HH:MM:SS] [AM/PM]

You can search for connected ports by these node properties:

- IP Address
- DNS Hostname
- MAC Address
- Port Description

To search for connected ports:

1. From the web console, click CONFIGS.
2. Under Find Connected Port for End Host, select the Search By filter, and then enter a value in the Find field.
3. Use the Edit button to adjust the columns of data to include in your search results.
4. Click Find.

Results are presented as rows in a table (one for each connection within the reach of hop of the context node) with the following default columns:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(For Wired Devices)</td>
<td></td>
</tr>
<tr>
<td>Node</td>
<td>Vendor and model of context node</td>
</tr>
</tbody>
</table>
## Find Connected Port for a Host (SolarWinds NPM Integration)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Of the context node</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Of the context node</td>
</tr>
<tr>
<td>Connected Via Interface</td>
<td>On the context node</td>
</tr>
<tr>
<td>To This Interface</td>
<td>On a connection point</td>
</tr>
<tr>
<td>On This Node</td>
<td>Vendor and model of device supporting the connection point</td>
</tr>
<tr>
<td>IP Address</td>
<td>Of a connection point</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Of a connection point</td>
</tr>
<tr>
<td><strong>(For Wireless Devices)</strong></td>
<td></td>
</tr>
<tr>
<td>Mapped Host Name</td>
<td>Vendor and model of context node</td>
</tr>
<tr>
<td>Mapped MAC Address</td>
<td>Of context node</td>
</tr>
<tr>
<td>Mapped Device Type</td>
<td>Of context node</td>
</tr>
<tr>
<td>Source Interface</td>
<td>Of the wireless access point</td>
</tr>
<tr>
<td>Controller Source IP Address</td>
<td>Of the wireless access point</td>
</tr>
<tr>
<td>Controller Description</td>
<td>Of the wireless access point</td>
</tr>
<tr>
<td>Controller Host Name Source SSID</td>
<td>Of the wireless access point</td>
</tr>
<tr>
<td>Source Channel</td>
<td>Of the wireless access point</td>
</tr>
<tr>
<td>Source Interface Alias</td>
<td>Of the wireless access point</td>
</tr>
<tr>
<td>Source Radio Type</td>
<td>Of the wireless access point</td>
</tr>
<tr>
<td>Source Host Name</td>
<td>Of the wireless access point</td>
</tr>
</tbody>
</table>
Chapter 3: Managing Nodes

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Device Type</td>
<td>Of the wireless access point</td>
</tr>
<tr>
<td>Source IP Address</td>
<td>Of the wireless access point</td>
</tr>
</tbody>
</table>
Unmanaging and Remanaging Nodes

SolarWinds NCM does not perform job actions on unmanaged nodes. When performing maintenance on nodes, unmanage the nodes to discontinue processing jobs against them. Maintenance includes upgrading firmware, installing new hardware, or updating security.

**Note:** Configuration data for unmanaged nodes will remain in the Orion platform database.

### Unmanaging Nodes

1. From the web console, under All Nodes, click **Manage Nodes**.
2. Select the nodes you want to unmanage in the nodes list and click **Unmanage**.

### Remanaging Nodes

1. From the web console, under All Nodes, click **Manage Nodes**.
2. Select the nodes you want to remanage in the nodes list and click **Remanage**.
Chapter 4: Managing Web Accounts

Orion Web Console user accounts, permissions, and views are established and maintained with the Manage Accounts option.

Use the following topics to work with Orion accounts:

- Creating a New Account
- Editing an Orion User Account
- Setting User Account Access
- Setting User Level Login Credentials
- Setting Account Limitations
- Creating Account Limitations
- Defining Pattern Limitations
- Setting Default Account Menu Bars and Views
- Configuring Audible Web Alerts

**Note:** To prevent issues with web console accounts, your SQL Server should not be configured with the **no count** connection option enabled. The **no count** option is set in the Default connection options area of the Server Properties > Connections window of SQL Server Management Studio.
Creating a New Account

Any web console administrator may create new Orion Web Console user.

*Note:* For more information about using Windows Pass-through security, Active Directory, and DirectLink accounts for automatic logon to the Orion Web Console, see Configuring Automatic Login.

1. From the web console, click **Settings**.
2. Under User Accounts, click **Manage Accounts**.
3. Click **Add New Account**.
4. Select the type of account you want to add, and then click **Next**.
5. *If you selected Windows individual account,* complete the following steps:
   a. Provide the user name and password for a user that has administrative access to your Active Directory or local domain.
   b. In the Search for Account area, enter the user name of the Active Directory or local domain user for whom you want to create a new web console account, and then click **Search**.
   c. In the Add Users area, select the users for whom you want to create new web console accounts, and then click **Next**.

7. *If you selected Windows group account,* complete the following steps:
   a. Provide the user name and password for a user that has administrative access to your Active Directory or local domain.
   b. In the Search for Account area, enter the Group name of the Active Directory or local domain group for which you want to create a new web console account, and then click **Search**.
   c. In the Add Users area, select the users for whom you want to create new web console accounts, and then click **Next**.

For more information, see Editing an Orion User Account.
**Note:** By default, a new Orion account is created with the `WebUploader` role. To adjust the NCM role for an account, expand Network Configuration Manager Settings and select the appropriate role for the account you are creating.

Select **None** if you do not want this account to access NCM.

8. Click **Submit** to create the account.

**Note:** Accounts are enabled by default, and disabling an account does not delete it. Account definitions and details are stored in the Orion database if the account is enabled later.

### Editing an Orion User Account

The Edit User Account page provides options for configuring web console user accounts. On the Edit User Account page, administrators can disable an account, set an account expiration date, grant administrator and node management rights, set user view limitations, define a default menu bar, and set several other defaults defining how a user account views and uses the Orion Web Console.

You must be an Orion platform administrator to create and manage jobs.

Use these sections as needed to manage accounts:

- [Setting User Account Access](#)
- [Setting Account Limitations](#)
- [Creating Account Limitations](#)
- [Setting Default Account Menu Bars and Views](#)
- [Configuring Audible Web Alerts](#)

### Setting User Account Access

By default, Orion accounts are given the NCM role of `WebUploader`, which enables the account user to make changes to device configurations and submit them for approval.

**Note:** An NCM Administrator can access and change all NCM settings.
Select None if you do not want an account to access any NCM resources. If you select None as the NCM role, and this account might be used for node discovery, you should deselect Enable Import from Discovery (in Settings > NCM Settings > Manage Nodes) to prevent this and similar account users from adding licensed nodes to NCM.

**To edit an Orion user account:**

1. From the web console, click **Settings**.
2. Under User Accounts, click **Manage Accounts**.
3. Select an account, and then click **Edit**.
4. Review the description next to each option and adjust settings.
5. Review the following notes about each option, and then click **Submit**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Enabled</td>
<td>Accounts are enabled by default, and disabling an account does not delete it. Account definitions and details are stored in the Orion database if the account is enabled later.</td>
</tr>
<tr>
<td>Account Expires</td>
<td>By default, accounts are set to Never expire. Dates can be entered in any format, and conform to the local settings on your computer.</td>
</tr>
<tr>
<td>Disable Session Timeout</td>
<td>By default, new user accounts are configured to time out automatically for added security.</td>
</tr>
<tr>
<td>Allow Administrator Rights</td>
<td>Granting administrator rights does not also assign the Admin menu bar to a user. If the user requires access to Admin options, they must be assigned the Admin view. For more information, see Setting Default Account Menu Bars and Views. Administrator rights are not granted by default, but they are required to create, delete, and edit accounts. User accounts without administrator rights cannot access the Admin page.</td>
</tr>
</tbody>
</table>
### Setting User Account Access

<table>
<thead>
<tr>
<th>Option</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Node Management Rights</td>
<td>By default, node management rights are not granted.</td>
</tr>
<tr>
<td>Allow Account to Customize Views</td>
<td>By default, customized view creation is not allowed. Changes made to a view are seen by all other users that have been assigned the same view.</td>
</tr>
<tr>
<td>Alert Sound</td>
<td>Sounds are stored in the default directory located at C:\Inetpub\SolarWinds\NetPerfMon\Sounds. Sounds in .wav format that are added to this directory become available when the Edit User Account page refreshes.</td>
</tr>
<tr>
<td>Default Menu Bars and Views</td>
<td>If you are setting up the menu bars and views for a user account with NCM role <em>None</em>, and your intention is to hide all NCM-related features and functions, select <em>None</em> for all view settings. If you do not set them to <em>None</em>, and you select <em>None</em> as the NCM role for the account, the user will still see a CONFIGS tab and all the NCM views. For details see <a href="#">Setting Default Account Menu Bars and Views</a>.</td>
</tr>
<tr>
<td>Network Configuration Manager Settings &gt; NCM Role</td>
<td>By default, Orion administrator accounts are given the NCM administrator role. You should not assign an Orion admin a role other than NCM Administrator. All other Orion accounts are given the NCM role <em>WebUploader</em>, which enables the account user to make changes to device configurations and submit them for approval.</td>
</tr>
</tbody>
</table>
Chapter 4: Managing Web Accounts

<table>
<thead>
<tr>
<th>Option</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select <strong>None</strong> if you do not want this account to access NCM. If you select <strong>None</strong> as the NCM role, and this account might be used for node discovery, you should deselect <strong>Enable Import from Discovery</strong> (in <strong>Settings &gt; NCM Settings &gt; Manage Nodes</strong>) to prevent this and similar account users from adding licensed nodes to NCM.</td>
</tr>
<tr>
<td></td>
<td>A user with the NCM role <strong>None</strong> will not see any NCM resources in non-NCM views and tabs on the Orion Web Console. For example, such a user sees no Pending Approval List on the Summary view under HOME. Though this user would be able to complete the process of adding NCM resources through the Customize Page, the resources do not display when the target view loads. Though this user may have privileges to add nodes, the user cannot add nodes to NCM (the <strong>Add Node to NCM</strong> option does not appear), and NCM properties are hidden when the user edits a node.</td>
</tr>
<tr>
<td></td>
<td>If an account user with NCM role <strong>None</strong> sets up an NCM Alert Action, Orion Web Console displays an error in Alert Details.</td>
</tr>
</tbody>
</table>

**Creating Account Limitations**

SolarWinds NCM provides predefined account limitations that use built-in properties to limit user access. For greater flexibility, however, you can use the Account Limitation Builder to create your own account limitations based on predefined or custom properties.

The Account Limitation Builder application allows you to create and customize account limitations for the Orion Web Console. These limitations ensure that users can only view the network objects that are pertinent to their job duties.

Examples of uses of account limitation in the Orion Web Console include:

- Limit customer views to specific network nodes
- Limit views by department or functional area
Setting User Level Login Credentials

- Limit views by device type or device role
- Limit views based on the geographic location of devices

Consult these topics as needed:
Setting Account Limitations
For more information about custom properties, see Creating a Custom Property.

Note: NCM ignores custom properties that use words from the list of reserved words. For details, see Reserved Words.

Setting User Level Login Credentials

These credentials enable you to access network devices with NCM user credentials instead of credentials defined on each network device.

1. From the web console, click **Settings > NCM Settings**.
2. Under Security, click **Manage User Level Login Credentials**.
3. Enter a valid NCM user name and password.
4. Select an Enable Level if you want to limit the account to a specific level of access on relevant network devices.
5. If you select an Enable Level, enter the password for it.
6. Click **Submit**.

Setting Account Limitations

To restrict user access to designated network areas, or to withhold certain types of information from designated users:

1. From the web console, click **Settings**.
2. Under User Accounts, click **Manage Accounts**.

Limiting an Individual User Account

1. On the Individual Accounts tab, select the account to limit.
2. Click **Edit**.
3. Click **Add Limitation** under Account Limitations.
Chapter 4: Managing Web Accounts

4. Select the type of limitation to apply, and then click **Continue**.

   **Notes:**
   
   - Because SolarWinds NCM initially caches account limitations, it may take up to a minute for account limitations to take effect.
   - Account limitations defined using the Account Limitation Builder display as options on the Select Limitation page. Account limitations can be defined and set using almost any custom properties. For more information, see [Creating Account Limitations](#).

5. Define the limitation as directed on the Configure Limitation page that follows. For more information about defining pattern-type limitations, refer to [Defining Pattern Limitations](#).

### Limiting a Group Account

**Note:** Limitations applied to a selected group account only apply to the group account and not, by extension, to the accounts of members of the group.

1. On the Groups tab, select the group account you want to limit.
2. Click **Edit**.
3. Under Account Limitations, click **Add Limitation**.
4. Select the type of limitation to apply, and then click **Continue**.

   **Notes:**
   
   - Because SolarWinds NCM initially caches account limitations, it may take up to a minute for account limitations to take effect.
   - Account limitations defined using the Account Limitation Builder display as options on the Select Limitation page. Account limitations can be defined and set using almost any custom properties. For more information, see [Creating Account Limitations](#).

5. Define the limitation as directed on the Configure Limitation page that follows. For more information about defining pattern-type limitations, refer to [Defining Pattern Limitations](#).
Creating Account Limitations

SolarWinds NCM provides predefined account limitations that use built-in properties to limit user access. For greater flexibility, however, you can use the Account Limitation Builder to create your own account limitations based on predefined or custom properties.

The Account Limitation Builder application allows you to create and customize account limitations for the Orion Web Console. These limitations ensure that users can only view the network objects that are pertinent to their job duties.

Examples of uses of account limitation in the Orion Web Console include:

- Limit customer views to specific network nodes
- Limit views by department or functional area
- Limit views by device type or device role
- Limit views based on the geographic location of devices

Consult these topics as needed:

Setting Account Limitations

For more information about custom properties, see Creating a Custom Property.

Note: NCM ignores custom properties that use words from the list of reserved words. For details, see Reserved Words.

Using the Account Limitation Builder

Before you can use the Account Limitation Builder, you must have first created the custom property that you want to use to limit the Orion Web Console view. For details, see Trap Date/Time Variables. After you have defined custom properties and populated them with data, you may use the Account Limitations Builder as directed in the following procedure.

NCM ignores custom properties that use words from the list of reserved words. For details, see Reserved Words.

Creating an Account Limitation

1. Start the Account Limitation Builder in the SolarWinds > Grouping and Access Control program folder.
2. Click Start on the splash screen.
3. Click **Edit > Add Limitation**.
4. Select a Custom Property.
   
   **Notes:**
   
   - If Custom Property is empty, define a custom property. For more information, see [ Trap Date/Time Variables](#).
   - The remaining boxes are populated automatically, based on your selection.

5. Choose a Selection Method.
   
   **Note:** This is the selection format that appears when you choose values for the account limitation through the web Account Manager. For more information, see [Installing and Upgrading SolarWinds Network Configuration Manager](#).

6. To include your own description of the account limitation, type your description over the default text in the **Description** field.

7. Click **OK**.

   The newly defined account limitation is added to the top of the table view. You may now use it in the Orion Web Console Account Manager. For more information, see [Installing and Upgrading SolarWinds Network Configuration Manager](#).

**Deleting an Account Limitation**

1. Start the **Account Limitation Builder** in the SolarWinds > Grouping and Access Control program folder.
2. Click **Start** on the splash screen.
3. Click the row of the limitation to delete.
   
   **Note:** Press **Shift+Click** to highlight consecutive rows or **Ctrl+Click** to highlight non-consecutive rows.
4. Click **Edit > Delete Selected Limitations**.

   **Note:** Deleting a limitation makes it unavailable for future use in the Orion Web Console. All accounts that have been assigned that limitation remain limited.

**Defining Pattern Limitations**

Pattern limitations may be defined using **OR**, **AND**, **EXCEPT**, and **NOT** operators with _ and * as wild card characters. The following examples show how to use available operators and wild card characters:

**Note:** Patterns are not case sensitive.

- **foo** matches only objects named "foo".
- **foo_** matches all objects with names consisting of the string "foo" followed by only one additional character, like **foot** or **food**, but not **seafood** or **football**.
- ***foo_** matches all objects with names ending with the string "foo", like **bigfoot** or **seafood**, but not **food**.
- **foo*** matches all objects with names starting with the string "foo", like **football** or **food**, but not **seafood**.
- ***foo*** matches all objects with names containing the string "foo", like **seafood** or **Bigfoot**.
- ***foo* OR *soc*** matches all objects containing either the string "foo" or the string "soc", including **football**, **socks**, **soccer**, and **food**.
- ***foo* AND *ball*** matches all objects containing both the string "foo" and the string "ball", including **football** but excluding **food**.
- ***foo* NOT *ball*** matches all objects containing the string "foo" that do not also contain the string "ball", including **food** but excluding **football**.
- ***foo* EXCEPT *ball*** matches all objects containing the string "foo" that do not also contain the string "ball", including **food** but excluding **football**.

You can also group operators using parentheses, as in the following example:

(*foo* EXCEPT *b*) AND (*all* OR *sea*) matches **seafood** and **footfall**, but not **football** or **Bigfoot**.
Chapter 4: Managing Web Accounts

Setting Default Account Menu Bars and Views

1. From the web console, click **Settings**.
2. Under User Accounts, click **Manage Accounts**.
3. Select an account, and then click **Edit**.
4. Scroll down to Default Menu Bar and Views.
5. Set the default menu bar displayed when you click the tab corresponding to an installed module in the Orion Web Console.
   
   **Note:** If you are editing a user account that must have administrator privileges, select **Admin**.

6. Click **Submit**.

Configuring Audible Web Alerts

When browsing the Orion Web Console, audible alerts can be sounded whenever new alerts are generated. When enabled, you will receive an audible alert the first time, after login, that an alert is displayed on the page. This alert may come from either an alert resource or the Alerts view. You do not receive audible alerts if the Alerts view or the alert resource you are viewing is empty.

Following the initial alert sound, you will receive an audible alert every time an alert is encountered that was triggered later than the latest alert that has already been viewed.

For example, a user logs in and sees a group of alerts with trigger times ranging from 9:01AM to 9:25AM, and the user receives an audible alert. If the user browses to a new page or allows the current page to auto-refresh, a new alert sounds if and only if an alert triggered later than 9:25AM is then displayed.

**To enable audible web alerts:**

1. From the web console, click **Settings**.
2. Under User Accounts, click **Manage Accounts**.
3. Select an account, and then click **Edit**.
4. Select the sound file you want to play when new alerts arrive from the Alert Sound list.

Notes:

- Sounds are stored in the default directory located at C:\Inetpub\SolarWinds\NetPerfMon\Sounds.
- Sounds in .wav format that are added to this directory become available when the Edit User Account page refreshes.

5. Click Submit.
Chapter 5: Managing Configuration Files

Configuration files can be downloaded, edited, compared, and uploaded using SolarWinds Network Configuration Manager.

1. From the web console, click **Settings > NCM Settings**.
2. Under Configs, click **Configs**.
3. Under Config Transfer, adjust **Config Min Length**. This setting limits the number of lines required for a config file to be recognized as valid for download. The default is 11 lines.

Use **Simultaneous Downloads/Uploads** value to throttle the load that a big job could put on the network.

- Downloading Configuration Files
- Download Configs (Single Node)
- Download Configs (Multiple Nodes)
- Enabling a New Config Type
- Editing Configuration Files
- Executing a Script on a Node
- Decrypting Cisco Type 7 Passwords
- Comparison Criteria (Exclusion Examples)
- Importing Configuration Files
- Understanding Baselines
- Removing a Config File as a Baseline
- Baselining Your Entire Network
- Clearing All Baselines
Chapter 5: Managing Configuration Files

Creating New Config Change Report Exclusions
Uploading Configuration Changes
Uploading an Entire Configuration
Configuring a Config Archive
Enabling Real Time Configuration Change Detection
Searching for Configuration Files (Web Console)
Deleting Configuration Files from the Database
Automating Configuration File Purges
Downloading Configuration Files

Download configuration files to view the current configuration of your device, compare current and previous configurations, or archive configuration files for backup. SolarWinds Network Configuration Manager can transfer files using direct and indirect transfers.

Select a topic:
- Download Configs (Single Node)
- Download Configs (Multiple Nodes)

**Download Configs (Multiple Nodes)**

1. From the web console, click **CONFIGS > Jobs**.
2. Click **Create New Job**.
3. Name the job, and then select **Download Configs from Devices** from **Job Type**.
   
   **Note:** By default, NCM does not download a config with fewer than 11 lines. Adjust the **Config Min Length** setting if necessary. For more information, see Managing Configuration Files.
4. Select the **Schedule Type**.
   - **If you are creating a Basic schedule**, select the frequency of the job: once, daily, weekly, or monthly.
   - **If you are creating an Advanced schedule**, use the five fields to create an appropriate cron expression.
5. Add a comment if desired, and then click **Next**.
6. Select the nodes to target with this job, and then click **Next**.
7. Select an email notification option, and then click **Next**.
8. Select the configuration types you want to download.
9. Set your notifications preference, and then click **Next**.
10. Review the settings for the job, and then click **Finish**.

**Note:** In a multi-node download operation, the **Simultaneous Downloads/Uploads** setting can be used as a throttle. By default it runs 10 sessions simultaneously.
Chapter 5: Managing Configuration Files

Download Configs (Single Node)

1. From the web console, click CONFIGS > Config Summary.
   
   Note: Use an account that has the WebDownloader, WebUploader, Engineer, or Administrator role.

2. Click a node in the list.

3. Click Configs on the left.

4. Under Download Config, select the config type and click Download.
   
   Note: By default, NCM does not download a config with fewer than 11 lines. Adjust the Config Min Length setting if necessary. For more information, see Managing Configuration Files.

5. Click Downloaded config.

6. If you receive a connectivity error, click Fix Connection in Device Template.

7. Follow the prompts of the Device Template wizard:

   a. Select what you want the script to do, and then click Next.
   b. Verify settings under Connection Profile and Device Template.
   c. Click Test.
   d. If the test fails, troubleshoot login credentials with an SSH client, then modify Login Credentials under Connection Profile.
   e. When the credentials are working properly, click Next.
   f. Click Perform Download Test, and then click Next.
   g. Click Finish.

Downloaded configuration files are stored on your server in an archive. The location is specified in NCM Settings > Configs > Config Archive Folder Locations.

Troubleshooting Config Download

If a config includes the command prompt character, NCM stops downloading.
We provide a new device template command, *UseExactPromptMatch*, to instruct NCM to act on the command prompt only if it appears on a separate line. For details on using the command, see [Confining NCM Recognition of the Command Prompt](#).

**Confining NCM Recognition of the Command Prompt**

By default, NCM ceases downloading a config file that contains the device command prompt in the body of the config. Use the *UseExactPromptMatch* command to prevent NCM from recognizing the command prompt unless it appears on a separate line:

1. From the web console, click **CONFIGS > NCM Settings**.
2. Under Advanced, click **Device Templates**.
3. Select a device template.
4. Click **Edit > Using XML Editor**.
5. Add this line to the Template XML:
   ```xml
   <Command Name="UseExactPromptMatch" Value="true"/>
   ```
6. Click **Save**.

**Enabling a New Config Type**

You can create a custom type of configuration to download from relevant devices. To do this you must enable NCM to recognize the new type and modify the templates for devices from which you intend to download the new type of configuration.

All functions that operate on standard config types in NCM operate as well with custom config types, with the following exceptions:

- The Overall Baseline vs. Running Config Conflicts chart is limited to the specified standard config types.
- The Overall Running vs. Startup Config Conflicts chart is limited to the specified standard config types.

To enable a new config type for your device:

1. From the web console, click **Settings > NCM Settings**.
2. Under Configs, click **Configs**.
3. Under Config Types, enter a name for the new config type.
4. Click **Add New**.
5. Click **Submit**.
6. Follow [Communication Process Diagrams](#) to modify your relevant device template with an appropriate statement.

**Note**: NCM uses the `show` command to download configurations.

### Enabling the Config and Policy Caches

**Note**: If enabled, the config and policy caches are updated daily at 11:55 PM.

1. From the web console, click **Settings > NCM Settings**.
2. Under Advanced, click **Advanced Settings**.
3. Under Cache Settings, select **Enable Config and Policy Caches**.
4. Click **Submit**.

### Editing Configuration Files

To update access lists, modify community strings, or make other configuration changes, edit the configuration files you downloaded with SolarWinds Network Configuration Manager.

1. From the web console, click **CONFIGS > Config Summary**.
   
   **Note**: Use an account that has the `WebDownloader`, `WebUploader`, `Engineer`, or `Administrator` role.
2. Click a node in the node list on the left.
3. Click **Configs** on the left.
4. Under Config List, select a config, and then click **Edit Config**.
5. Edit the Config Title if necessary.
6. Select **Edit Config Text**, and then make changes.
7. Add comments if necessary.
8. Click **Submit**.
   
   **Note:** The revision is saved in the Config List with the indication that it is an Edited config of its type.

---

**Upload Edited Configuration File**

2. Click **Upload**.
   
   For more information, see [Uploading Configuration Changes](#).

---

**Executing a Script on a Node**

This resource is available to users with the **WebUploader**, **Engineer**, or **Administrator** role. For more information, see [Creating and Editing an NCM Account](#)

The script you execute must be saved as a text file that can be uploaded from the client computer.

1. From the web console, click **CONFIGS > Configuration Management**.
   
   **Note:** If you do not have administrator privileges you may not be able to see some nodes. Your account must at least have the **WebDownloader** role to download configs, and the **WebUploader** role to execute a script against nodes.

2. Select one or more nodes.
3. Click **Execute Script**.
4. Select a script to execute or click **Load Script from File**, and then locate it in the file system.

   **Note:** You can specify a delay (in seconds) inside a script. A delay is the time NCM will wait before sending the next command. The following is a sample script that includes a delay:

   {Command 1}
   ${Delay:20}
   {Command 2}

   This feature is useful, for example, when uploading a flash image. Some time is required for the formatting of the flash to complete before then performing the image upload.

5. Select script options at the bottom if necessary.

6. Click **Execute**.

   If execution fails, see **Troubleshooting Script Execution**.

**Viewing Script Execution Results**

1. Click **CONFIGS > Configuration Management**.

2. Click **Transfer Status**.

3. In the **Action** column, locate the most recent entry labeled **Execute Script**.

4. Click **Show Script Results** in the **Status/Details** column.

**Troubleshooting Script Execution**

If a script fails to execute, review the log located in

```C:\ProgramData\SolarWinds\NCM\Logging\NCMBusinessLayerPlugin.log```

Alternatively, execute the script by creating a job. For details, see **Creating or Editing a Job**.

**Config List**

Under Node Details, the Config List provides a list of the last X number of configurations downloaded from this device. Click a configuration to load its Details page, which includes the following:
Decrypting Cisco Type 7 Passwords

When viewing a configuration file, all encrypted Cisco Type 7 passwords in the file can be decrypted. This is helpful when trying to recover lost passwords.

To decrypt Cisco Type 7 passwords:

1. Open the SolarWinds Network Configuration Manager application.
2. Click on the configuration file in the left pane.
3. Click **Configs > Edit Configs**.
4. Click **Actions**.
5. Click **Decrypt Type 7 Passwords**.

Notes:

- All passwords that have been decrypted appear in green text.
- Decrypting Type 7 Passwords alters the text of the configuration file. If the configuration file is saved after decrypting the passwords, the passwords are saved without encryption.

Defining Comparison Criteria

Defining comparison criteria enables you to filter out of comparison results lines that you do not need SolarWinds NCM to evaluate. This saves processing time and makes the review of compared files easier.

You use regular expression patterns to create the filters that SolarWinds NCM uses to ignore statements of the config files that you ask it to comparatively evaluate.

The regular expressions you create and enable are used throughout SolarWinds NCM to compare config files, as in performing scheduled jobs.

Use the following procedures to create, edit, enable/disable, or delete a regular expression pattern.
Creating a New Regular Expression Statement

1. From the web console, click Settings > NCM Settings.
2. Under Configs, click Comparison Criteria.
3. Click Add New.
4. Give the pattern a title and write the regular expression.
5. Select Enable NCM to ignore this pattern when comparing config files to activate this pattern, or leave it disabled for future editing.
6. Click OK.

Editing a Regular Expression Statement

1. From the web console, click Settings > NCM Settings.
2. Under Configs, click Comparison Criteria.
3. Select a regular expression, and then click Edit.
4. Change the title or the regular expression. See Regular Expression Pattern Matching Examples for details on regular expression statements supported in creating comparison criteria.
5. Select Enable NCM to ignore this pattern when comparing config files to activate this pattern or clear it to disable.
6. Click OK.

Enabling or Disabling a Regular Expression Pattern

Select one or more items and click Enable or Disable.

Deleting a Regular Expression Pattern

Select one or more items and click Delete.

Comparison Criteria (Exclusion Examples)

Defining comparison criteria enables you to filter out of comparison results lines that you do not need SolarWinds NCM to evaluate. This saves processing time and makes the review of compared files easier.
Comparing Configurations

SolarWinds Network Configuration Manager can compare configuration files. Configuration files can be compared between two nodes, or an older configuration can be compared with the current configuration.

When comparing, you can select comparison criteria for excluding lines that contain a specific string pattern.

1. From the web console, click **CONFIGS > Configuration Management**.
2. *If you want to compare configs from two different nodes*, select both nodes.
3. *If you want to compare two configs from the same node*, select the single node.
4. Click **Compare node(s) configs**.
5. Select the configs you want to compare.
6. Review the configs for changes (yellow highlights), added lines (green highlights), and missing lines (red highlights).
7. Click **Edit Config** for either config if you need to make changes.
8. Click **Set/Clear Baseline** on either config to make it the baseline. NCM uses the baseline to alert you to future config changes.
9. If a config is obsolete and should be removed, click **Delete Config**.
10. Click **Export to PDF** in the top right if you want a PDF of the config comparison.
11. Click **Close**.

**Note:** You can create and enable exclusion filters. See [Defining Comparison Criteria](#) for details.

Using the Comparison Overview

A comparison overview is displayed to the left of the side-by-side comparison. This overview scales to fit the size of the window allowing for an overview of the entire comparison. Click anywhere on the comparison overview to jump to the associated sections of the configuration files.
Chapter 5: Managing Configuration Files

Importing Configuration Files

You can import configuration files you have already downloaded from your devices into SolarWinds Network Configuration Manager. Configuration files can be imported using the following file formats:

- SolarWinds Network Configuration Manager Archive (.Config)
- SolarWinds Cisco Config Downloader (.CiscoConfig)
- Text File (.txt)
- Configuration File (.cfg)
- Any file in ASCII text

To import a configuration file:

1. From the web console, click **CONFIGS > Configuration Management.**
2. Click a node.
3. Under Nodes Details, click **Configs.**
4. Under Config List, click **Import Config.**
5. Click **Choose File,** and then browse to the config file.
6. Click **Submit.**

Understanding Baselines

A baseline is a configuration file that is known to be good for a particular application. It is important to establish a baseline when making node configuration changes.

Setting a Baseline

To mark a downloaded config as the baseline against which to compare future downloads:

1. From the web console, click **CONFIGS > Configuration Management.**
2. Click the node(s) in the node list.
3. Under Node Details, click **Configs.**
4. Under Config List, select the config, and then click **Set/Clear Baseline.**

Notes:
Removing a Config File as a Baseline

- If you do not have administrator privileges you may not be able to see some nodes. Your account must have the WebUploader role to upload configs.
- Resetting a baseline does not regenerate cache data, so there may be a delay before the chart displays the most current data. Downloading a config resets cache data, however.
- When downloading new configuration files, select **Compare to Last Baseline Config** in the Download Config window to automatically compare the new configuration file to the baseline. If no baseline is found, the configuration is compared against the previously downloaded configuration file.

**Removing a Config File as a Baseline**

1. From the web console, click **CONFIGS > Configuration Management**.
2. Click the node(s) in the node list.
   
   **Note:** If you do not have administrator privileges you may not be able to see some nodes. Your account must have the WebUploader role to upload configs.
3. Under Node Details, click **Configs**.
4. Under Config List, select the current baseline.
5. Click **Set/Clear Baseline**.

**Baselining Your Entire Network**

A full inventory scan can take anywhere from a few minutes to several hours to complete. The time period varies based on the number of nodes and the type of statistics you want to collect. For more information on how to establish what statistics are collected, see **Adjusting Inventory Settings**.

1. From the web console, click **CONFIGS > Jobs**.
2. Click **Create New Job**.
3. Name the job and select **Baseline Entire Network** from **Job Type**.
4. Select the **Schedule Type**:
   - *If you are creating a Basic schedule*, select the frequency of the job: once, daily, weekly, or monthly.
   - *If you are creating an Advanced schedule*, use the five fields to create an appropriate cron expression.

5. Add a comment if desired, and then click **Next**.

6. Click **Next**.

7. Select an email notification option, and then click **Next**.

8. Select one of the following options:
   - *Set the Network Baseline to the last Config downloaded from each Node*
   - *Set the Network Baseline to a specific date*

9. Click **Next**

10. Review the settings for the job, and then click **Finish**.

### Clearing All Baselines

1. From the web console, click **CONFIGS > Jobs**.
2. Click **Create New Job**.
3. Name the job, and then select **Baseline Entire Network** from **Job Type**.
4. Select the **Schedule Type**:
   - *If you are creating a Basic schedule*, select the frequency of the job: once, daily, weekly, or monthly.
   - *If you are creating an Advanced schedule*, use the five fields to create an appropriate cron expression.

5. Add a comment if desired, and then click **Next**.

6. Click **Next**.

7. Select an email notification option, and then click **Next**.

8. Select **Clear All Baselines**, and then click **Next**.

9. Review the settings for the job, and then click **Finish**.
Running a Config Change Report (Once)

1. From the web console, click CONFIGS > Jobs.
2. Click Create New Job.
3. Name the job, and then select Generate a Config Change Report from Job Type.
   Note: Do not use special characters in the job name.
4. Select Basic as the Schedule Type.
5. Select Once, and then enter a day and time that is at least 15 minutes from the current NCM server time.
6. Add a comment if desired, and then click Next.
7. Select the nodes to target with this job, and then click Next.
8. Select an email notification option, and then click Next.
9. Select the type of config change report to generate, and then click Next.
10. Select Only send devices that had changes if desired, and then click Next.
11. Review the settings for the job, and then click Finish.

Notes:

- To create a config change report to run recurrently, see Scheduling a Config Change Report (Recurrent)
- When processing an active job, NCM uses credential settings of the user who last edited the job. For example, if the user has user-level logon credentials, NCM uses the connection profile associated with the device.

Uploading Configuration Changes

In the case of a multi-node upload/download operation, the Simultaneous Downloads/Uploads setting can be used as a throttle. By default it is set to run 10 Sessions simultaneously.
For IPv6, you can rediscover devices that were previously discovered with the engine using IPv4, and you can do inventories for devices already discovered with IPv4 or rediscovered with IPv6. Otherwise, new IPv6 addresses can be added to SolarWinds NCM, though IPv6 addresses cannot be communicated with through SNMP. You can execute scripts, upload, and download configuration files on IPv6 addresses, and Telnet and SSH communication is supported.

Note: You can upload changes to a custom config type only to a single device, but through an indirect transfer protocol (Telnet\TFTP). As a result, the Write Config to NVRAM After Upload option is disabled.

Uploading an Entire Configuration

1. From the web console, click CONFIGS > Configuration Management.
2. Select one or more nodes.
3. Click Upload.
4. Select a config, and then edit it if necessary.
5. Click Advanced at the bottom.
6. Select one or more advanced options, and then click Upload.

Configuring a Config Archive

SolarWinds Network Configuration Manager can copy every configuration file downloaded to an archive location for backup.

Creating a Config Archive for Local Storage

1. From the web console, click Settings > NCM Settings.
   Note: If you do not have NCM Administrator privileges you may not be able to see some nodes and settings.
2. Under Configs, click Configs.
3. Select Save a copy of each Config to the Config-Archive directory when it is downloaded.
4. To save space on your storage target, if you need only the immediately past version in addition to the current config, select When configs are edited, only retain the last version.
5. Type the path of the local directory to store the NCM Config Archive.  
   Note: By default, NCM sets the directory for your Config Archive as 
   %PROGRAMDATA%\SolarWinds\NCM\Config-Archive\. As 
   preparation for a growing archive, SolarWinds recommends moving the 
   Config Archive to a different location.

6. Type the template you want to use when naming the configuration files. For 
   more information, see Configuration Archive Variables.

7. Click Submit.

Creating a Config Archive for Network Storage

1. From the web console, click Settings > NCM Settings > Advanced 
   Settings.
   Note: If you do not have NCM Administrator privileges you may not be able 
   to see some nodes and settings.

2. Select Use Custom Credentials to give NCM write access, provide 
   credentials, and then click Validate Credentials.

   If credentials fail to validate, check that the NCM-related account 
   has Windows permissions for the network storage.

3. Click Settings > NCM Settings.

4. Under Configs, click Configs.

5. Select Save a copy of each Config to the Config-Archive directory 
   when it is downloaded.

6. To save space on your storage target, if you need only the immediately past 
   version in addition to the current config, select When configs are edited, 
   only retain the last version.

7. Type the path of the network storage for the NCM Config Archive.

8. Type the template you want to use when naming the configuration files. For 
   more information, see Configuration Archive Variables.

9. Click Submit.
Enabling Real Time Configuration Change Detection

The Real Time Configuration Change Detection feature provides notification through email whenever a change to any of your device configurations occurs. Unlike the Config Change Report, changes are detected only on the same configuration type. For example, if you download a startup configuration, make changes to it, and upload it as a running configuration, the change will be detected against the previous running configuration. A comparison is not made between running and startup configuration types.

- Real Time Configuration Change Requirements
- Configuring Real Time Configuration Change Detection
- Limiting Real Time Notification Download Operations
- Running Syslog and Trap Services as Administrator

Real Time Configuration Change Requirements

- A Windows user account with administrative rights.
- Network devices configured to send Syslog or SNMP Trap messages when configurations change.
- The SolarWinds Syslog Service account must have read-write access to the Orion platform database. For example, if your SQL Server resides on the same server as SolarWinds NCM, consider using a local administrator account for the SolarWinds Syslog Service.
- The SolarWinds Trap Service account must have read-write access to the Orion platform database. For example, if your SQL Server resides on the same server as SolarWinds NCM, consider using a local administrator account for the SolarWinds Trap Service.
- The SolarWinds Syslog and Trap Services must be configured to run as administrator so that their scheduled jobs are processed correctly. For detailed steps, see Running Syslog and Trap Services as Administrator.
- Ensure the SNMP Trap Service is running. If the SNMP Trap Service is not listed as a running service in the service control manager (services.msc), you can enable Simple Network Management Protocol in the Management and Monitoring Tools through Add/Remove Windows Components in the Add/Remove Programs application.
Configuring Real Time Configuration Change Detection

Notes:

- The SolarWinds Syslog and Trap Services must be configured to run as administrator so that their scheduled jobs are processed correctly. For detailed steps, see Running Syslog and Trap Services as Administrator.

- Cisco devices send trap messages when a user enters config mode, but not when the user exits. As a result, if you make changes to the config on your device, you will receive a trap about those changes only when you enter config mode the next time. That is usually not until another change to the config needs to be done. Due to this behavior, SolarWinds recommend that you use the syslog option for setting up real time change detection.

- SolarWinds Kiwi Server Syslog Server setup instructions appear in Step 8 if you are using that product for syslog server notifications.

To enable real-time configuration change detection:

1. From the web console, click Settings > NCM Settings.
2. Click Configure Real Time Change Detection.
   
   **Note:** You must complete all six steps for Real Time Change Detection to operate correctly.

3. On the Real Time Change Detection setup page, complete the prerequisite (Step 1) by manually configuring your devices to send syslog or trap messages when configuration changes are detected.

   For more information, see the vendor documentation for each network device.

   **Note:** Remove device configurations by running a given command with no in front of it. For example, no set logging server ip_address removes that target from the remote logging stream.

   - a. Click CONFIGS > Configuration Management.
   - b. Select the node(s), and then click Execute Script.
c. Paste in the commands from the following example(s), changing the IP address to match your device:

**Syslog (IOS)**

config terminal
logging 10.199.3.43
logging trap 6
end

**Syslog (CatOS)**

set logging server 192.168.0.30
set logging server facility local4
set logging server severity 4
set logging server enable

**Traps (IOS)**

snmp-server host 10.110.68.33 public config
snmp-server enable traps config

**Traps (CatOS)**

set snmp trap 10.110.68.33 public config
set snmp trap enable config

d. Click **Execute**.
ed. Click **Transfer Status**.
f. In the **Action** column, locate the most recent entry labeled Execute Script.
g. Click **Show Script Results** in the **Status/Details** column.

**Note:** Steps 5 through 8 pertain to the NCM Process section (Step 2) on the Real Time Change Detection setup page.

4. **If your Cisco devices send change notifications using Syslog messages**, follow these steps.

   a. Start the **Syslog Viewer** from the SolarWinds > Syslog and SNMP Traps program folder.

   b. Click **View > Alerts/Filter Rules**.
c. Select **NCM Rule: Cisco IOS - Change Notifications**.

d. Click **OK**.

5. **If your devices are not Cisco devices and send change notifications using Syslog messages**, follow these steps:

a. Start the **Syslog Viewer** from the SolarWinds > Syslog and SNMP Traps program folder.

b. Click **View > Alerts/Filter Rules**.

c. Click **Add New Rule**.

d. Provide the appropriate information under General and DNS Hostname.

e. Click **Message**.

f. In the **Message Type Pattern** field, type the pattern to find.

   **Note**: The message pattern will vary by device type. For example, when a change is made to a Cisco router, a syslog message containing `SYS-5-CONFIG_I: is sent. For more information about what messages are sent, see the documentation provided by the vendor of your device.

g. Click **Alert Actions**, and then click **Add New Action**.

h. Select **Execute an external program**, and then click **OK**.
Chapter 5: Managing Configuration Files

i. Type the following in the **Program to execute** field:

```
Path\Orion\SolarWinds.NCM.RTNForwarder.exe ${IP}, RealtimeNotification,${DateTime},${Message}
```

Where:

*Path*

The location of the Orion folder. For example, `C:\Program Files\SolarWinds`. If the path contains spaces, enclose the path section of the statement in quotation marks ("Path to executable").

*${IP}*

The IP address of the triggering device.

*RealtimeNotification*

This text is displayed as the user name value. Currently, there is no means to parse the message text for the user name. The text is required to include the Message variable.

*${DateTime}*

The current date and time. This is equivalent to the Windows Control Panel defined Short Date and Short Time format.

*${Message}*

The Syslog message in the real time detection notification. If your Syslog message contains the user making the change, the user name is included through the use of this variable.

**Note:** You must include the commas and, if including Message, you must include placeholder text in the second comma delimited location and the DateTime variable.

j. Click **OK**.

k. Ensure the new rule is selected in the Alerts/Filter Rules tab of the Syslog Server Settings window, and then click **OK**.

6. **If your devices send change notifications using SolarWinds Kiwi Syslog Server,** follow these steps:
a. Start the **Kiwi Syslog Server Console** in the SolarWinds Syslog Server Console program folder.

b. Click **File > Setup**.

c. Click **Filter**, and then right-click **New Filter** to rename it.

d. Select **Field > Message text** and **Filter Type > Simple**, and then type the message to include with a syslog notification.

e. Right-click **Actions**, and then rename **New Action**.

f. In the the **Program file name** field, type

   
   Path\Orion\SolarWinds.NCM.RTNForwarder.exe

   
   Where:

   **Path**

   The location of the Orion folder. For example, C:\Program Files \SolarWinds. If the path contains spaces, enclose the path section of the statement in quotation marks ("Path to executable").

   
   g. Add the string %MsgIPAddr,RTN,%MsgText to Command line options

   
   h. Click **Apply/OK**.

   
   i. Ensure the appropriate filter and action are selected in Rules lists, and then click **OK**.

7. **If your device sends change notifications using SNMP Trap messages**, follow these steps:

   a. Start the **Trap Viewer** in the SolarWinds > Syslog and SNMP Traps program folder.

      **Note:** SolarWinds does not include a predefined rule with filters for trap messages since we strongly recommend using the syslog option instead. However, if you want to use trap messages for Real Time Change Detection, continue with these steps.

   b. Click **View > Alerts/Filter Rules**.

   c. Click **Add Rule**.
d. Provide the appropriate information on the General and DNS Hostname tabs.

e. Click **Conditions**, and then click **Add a condition**.

f. Click **SNMPv2-MIB:snmpTrapOID**, and then browse to the MIB that contains the trap message.

For example, browse to CISCO-CONFIG-MAN-MIB:ccmHistoryEventConfigDestination (1.3.6.1.4.1.9.9.43.1.1.6.1.5).

g. Click the asterisk, and then type the message pattern to match.

For example, when a change is made to the running config the HistoryEventMedium is 3. Changes to the startup config are designated by the integer 4.

h. If you need to match on more than one condition, click **Browse (…)** next to your last condition, and then click the appropriate conjunction: *(and or or)*.

Repeat Steps f through g for as many conditions as you need to match. For example, along with the change history event value, consider matching the command source CISCO-CONFIG_MAN_MIB:ccmHistoryEventCommandSource (1.3.6.1.4.1.9.9.43.1.1.6.1.3) and select 1 (command line) or 2 (snmp) as the value. For more information about what messages are sent from your devices, see the documentation provided by the vendor of your device.

i. Click **Alert Actions**.

j. Click **Add Action**.
k. Select **Execute an external program**, and then click **OK**.

l. Type the following in the Program to execute field:
   
   "Path\Orion\SolarWinds.NCM.RTNforwarder.exe"${IP}.

   Where:

   **Path**
   
   The location of the Orion folder. For example, "C:\Program
   Files\SolarWinds". If the path contains spaces, enclose the path
   section of the statement in quotation marks ("Path to
   executable").

   **${IP}**
   
   The IP address of the triggering device.

m. Click **OK**.

n. Ensure the new rule is selected in the Alerts/Filter Rules tab of the
Trap Server Settings window, and then click **OK**.

8. **If your device sends change notifications to a system other than
SolarWinds Network Configuration Manager**, follow these steps:

   a. Start your third-party Syslog or SNMP Trap receiver.

   b. Setup an alert that executes an external program.

   c. Type the following in the Program to execute field:

   "Path\Orion\SolarWinds.NCM.RTNforwarder.exe"${IP}.

   Where:

   **Path**
   
   The location of the Orion folder. For example, “C:\Program
   Files\SolarWinds”. If the path contains spaces, enclose the path
   section of the statement in quotation marks ("Path to
   executable").

   **${IP}**
   
   The IP address of the triggering device.
Chapter 5: Managing Configuration Files

d. Save the alert, and then ensure it is enabled.

9. Enter the Windows account credentials and device login information if prompted.

10. Set download, baseline config, and email notification options.

11. Click **Config Changes** under NCM Process on the Real Time Change Detection setup page.

12. Each syslog or trap that triggers RTCD immediately results in the download of the latest running config on the relevant device(s).

   a. Define the device access account to create and run RTCD-related download jobs.

   b. Select **Enable these account credentials** to access all NCM-managed devices if you want to allow them to access all network devices managed in NCM.

      **Note:** If the control is unavailable (grayed-out), then Device Login and User Account Credentials is set to Global – Device Level on the Security resource (**Settings > NCM Settings > Security**). Click **Security** to change that setting if necessary.

   c. Select **Include syslog/trap message in NCM email notification** if desired.

   d. Click **Submit**.

13. Click **Config Downloads and Notification Settings** on the Real Time Change Detection setup page to specify config download details.

   a. Select the file **In Previously Downloaded Config File** that you want to monitor.

   b. Select the config file type in **Baseline Config File** against which you want to compare differences with the file downloaded as part of the RTCD operation.

   c. Select the relevant **Email Notification Options**

   d. Enter the **Sender Name**, **Subject**, and **To** address information to be used in sending out RTCD email notifications. **Reply Address** is optional.

   e. Click **Submit**.
14. Click Config NCM SMTP Server on the Real Time Change Detection setup page to specify config download details.
   a. Enter the mail server’s FQDN or IP address.
   b. Enter the relevant port number on which the mail server handles messages.
   c. Enter an access authentication option (either Password or None).
   d. Enter a valid user name by which the mail server will identify your RTN recipient.
   e. If you are requiring password authentication, type and confirm the password for the user name.
   f. Click **Submit**.

   The email server settings you enter here will be used to send notifications regarding RTCD, config change approvals, and running jobs.

   For information on config change approvals, see [Approving Device Configuration Changes](#).

15. Click **Enable** to turn on Real Time Change Detection.
16. Click **Submit**.

**Limiting Real Time Notification Download Operations**

The config downloads may overwhelm resources on your NCM server, in response to syslog and trap information flowing in from your network devices.

1. From the web console, click **Settings > NCM Settings**.
2. Under Configs, click **Configs**.
3. Adjust the number of Simultaneous Download/Uploads. The default number of concurrent sessions is 10.
4. Click **Submit**.
Running Syslog and Trap Services as Administrator

Although the SolarWinds Syslog Service and Trap Service are installed and launched with administrator access, you must manually grant them administrator access to run correctly.

1. Navigate to the SolarWinds installation folder. The default is `C:\Program Files\SolarWinds\Orion\`
2. Right-click `SyslogService.exe` and click **Run as**.
3. Click **The following user** and then select **Administrator**.
4. Click **OK**.
5. Right-click `SWTrapService.exe` and click **Run as**.
6. Click **The following user** and then select **Administrator**.
7. Click **OK**.

Searching for Configuration Files (Web Console)

Complete the following procedure to search for specific strings of text within the configuration files stored in the Orion platform database. If you want to complete detailed searches using Regular Expression pattern matching or if you want to ensure your configurations follow appropriate configuration standards, use the SolarWinds NCM. For more information, see [Managing Policy Reports](#).

**Note**: Search may not find a config newly added to the database for up to 10 minutes.

1. From the web console, click **CONFIGS**.
2. Under Search NCM, click **Advanced Search**.
3. Enter a string pattern. For information on using Regular Expressions, see [Using Regular Expressions](#).
4. Select a search target from the list: All, Nodes, Configs from All Nodes, or Configs from Selected Nodes.
5. Select a search method.
6. Click **Search**.
7. To search within the returned results, select **Search in results**, type a new string pattern, and then click **Search** again.
Deleting Configuration Files from the Database

**Note:** If you may need information you currently want to delete, back up your database. For more information, see Creating a Database Backup File with SQL Server Management Studio.

1. From the web console, click **CONFIGS > Configuration Management**.
2. Use the **Group by** filters to find the node, and then click it.
3. Under the node list in the center, click + to expand the list of configs under the targeted node.
4. Under the **Suggested action** column, click **Delete** beside the relevant config.

### Automating Configuration File Purges

If you do not need to keep historical configuration files and want to improve database performance, you can automate the removal of unnecessary configuration files. If your database is not stored on a high performance SQL Server, or is running on a locally installed instance of SQL Server Express, ensure you regularly purge unused config history. For more information, see Reviewing Your License.

1. From the web console, click **CONFIGS > Jobs**.
2. Click **Create New Job**.
3. Name the job, and then select **Purge Old Configs from Database** from **Job Type**.
4. Select the **Schedule Type**.
   - *If you are creating a Basic schedule*, select the frequency of the job: once, daily, weekly, or monthly.
   - *If you are creating an Advanced schedule*, use the five fields to create the appropriate cron expression.
5. Add a comment if desired, and then click **Next**.
6. Select the nodes to target with this job, and then click **Next**.
7. Select a Save option.
9. Select an email notification option, and then click **Next**.
Chapter 5: Managing Configuration Files

11. Select a Purge Configs option, and then click **Next**.
12. Review the settings for the job, and then click **Finish**.
Chapter 6: Creating and Modifying Device Templates

It may be necessary to create a new device template or modify a supplied template to add support for your device. Before creating or modifying device templates, review the following sections.

Preparation
- Gathering the Information You Need
- Device Command Template Best Practices
- Communication Process Diagrams

Creating and Modifying
- Creating a Device Template (Wizard)
- Creating a Device Template (XML Editor)
- Editing a Device Template (Wizard)

Examples
- Example CLI Device Command Templates
- Nortel BayStack 380 Example
- Creating a Menu-Based Command Template
- Command Template Commands
- Pre-Command and Command Template Variables
- Example Pre-Command Device Template Entry
- Using Command Template Variables to Preclude Pseudoterminal Setup
- Using Command Template Variables to Declare a Special Command Prompt
- Using Command Template Variables to Switch User Context
- Using Command Template Variables to Respond to Post-Logon Interaction Requests
Creating a Device Template (XML Editor)

1. From the web console, click **CONFIGS > NCM Settings**.
2. Under Advanced, click **Device Templates**.
3. Click **Add New > Using XML Editor**.
4. Add information to the template, and then modify the XML according to your device.
5. Click **Save**.

For more information, see the following:
- Gathering the Information You Need
- Device Command Template Best Practices
- Communication Process Diagrams
- Example CLI Device Command Templates
- Pre-Command and Command Template Variables
- Using Command Template Variables to Respond to Post-Logon Interaction Requests
- Using Command Template Variables to Declare a Special Command Prompt
- Using Command Template Variables to Preclude Pseudoterminal Setup
- Using Command Template Variables to Switch User Context
Editing a Device Template (XML Editor)

1. From the web console, click **CONFIGS > NCM Settings**.
2. Under Advanced, click **Device Templates**.
3. Select a device template, click **Copy**, name the copy, and then click **Save**.
   **Note**: Since you may have applied the existing template to nodes, it is best to copy and rename the template before making changes.
4. Select the copied template, and then click **Edit > Using XML Editor**.
5. **If you want to modify an existing command**, make changes as needed.
   For example, a device shows version information when you type `show sys info`. The current device command template includes:
   ```xml
   <Command Name="Version" Value="show version"/>
   ```
   The value needs to be changed to `show sys info`.
   The updated command is:
   ```xml
   <Command Name="Version" Value="show sys info"/>
   ```
   **Note**: You can set up cascading templates by creating a series that targets slightly different OIDs. For example:
   - 1.3.6.1.4.1.9 = Cisco (All)
   - 1.3.6.1.4.1.9.1.23 = Cisco 2507
   You can specify a specific device with a more exact OID, and SolarWinds NCM will try to find the closest match. If SolarWinds NCM is talking to a device with a system OID of 1.3.6.1.4.1.9.1.25, it uses the **Cisco (All)** template, but if the system OID is 1.3.6.1.4.1.9.1.23, it uses the **Cisco 2507** template.
6. Click **Save**.
7. Select the template again, and then click **Assign to Nodes**.
8. Select nodes, and then click **Submit**.
Chapter 6: Creating and Modifying Device Templates

Confirm Device Template Is Working

1. Click **CONFIGS**.
2. Under NCM Node List, click a node to which you assigned the device template.
3. On the node details page, click **Configs** on the left.
4. Under Download Config, select a config type.
5. Click **Download**.
6. If the downloads succeeds, the device template is working as expected.

Topics related to editing device templates:

- Editing a Device Template (Wizard)
- Gathering the Information You Need
- Device Command Template Best Practices
- Communication Process Diagrams
- Example CLI Device Command Templates
- Pre-Command and Command Template Variables
- Using Command Template Variables to Respond to Post-Logon Interaction Requests
- Using Command Template Variables to Declare a Special Command Prompt
- Using Command Template Variables to Preclude Pseudoterminal Setup
- Using Command Template Variables to Switch User Context
- Confining NCM Recognition of the Command Prompt
Creating a Device Template (Wizard)

1. From the web console, click **CONFIGS > NCM Settings**.
2. Under Advanced, click **Device Templates**.
3. Click **Add New > Using Interactive Wizard**.
4. Use the **Level** and **Group by** controls to organize the node list.
5. Select a node, and then click **Next**.
   - **Note**: NCM pulls the OID value from the properties of the node you select.
6. Choose the scope of operation for this device template, and then click **Next**.
7. Verify and adjust Connection Profile and Device Template settings.
8. Click **Test**.
9. Click **Next**.
10. Verify and adjust Download Command and Config Types settings.
11. Set the config type to use in the download test, and then click **Perform Download Test**.
12. Click **Next**.
13. Enter and adjust the Device Template and Assign Device Template settings.
14. Click **Finish**.

**For more information, see the following:**

- Creating a Device Template (XML Editor)
- Gathering the Information You Need
- Device Command Template Best Practices
- Communication Process Diagrams
- Example CLI Device Command Templates
- Pre-Command and Command Template Variables
- Using Command Template Variables to Respond to Post-Logon Interaction Requests
- Using Command Template Variables to Declare a Special Command Prompt
Chapter 6: Creating and Modifying Device Templates

Using Command Template Variables to Preclude Pseudoterminal Setup
Using Command Template Variables to Switch User Context
Editing a Device Template (Wizard)

1. From the web console, click **CONFIGS > NCM Settings**.
2. Under Advanced, click **Device Templates**.
3. Select a device template, click **Copy**, name the copy, and then click **Save**.
   **Note:** Since you may have applied the existing template to nodes, it is best to copy and rename the template before making changes.
4. Select the copied template, and then click **Edit > Using Interactive Wizard**.
5. Use the **Level** and **Group by** controls to organize the node list.
6. Select a node, and then click **Next**.
   **Note:** NCM pulls the OID value from the properties of the node you select.
7. Choose the scope of operation for this device template, and then click **Next**.
8. Verify and adjust Connection Profile and Device Template settings.
9. Click **Test**.
10. Click **Next**.
11. Verify and adjust Download Command and Config Types settings.
12. Set the config type to use in the download test, and then click **Perform Download Test**.
13. Click **Next**.
14. Enter and adjust the Device Template and Assign Device Template settings.
15. Click **Finish**.
Gathering the Information You Need

Before attempting to modify or create a new template, answer all of the following questions about your device:

<table>
<thead>
<tr>
<th>Question</th>
<th>Note</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>What are the Machine Type and System OID values displayed in the Device Details tab of the node properties?</td>
<td>Use this information to save the device template with a unique name that SolarWinds NCM recognizes, ensuring its use when connecting to the device.</td>
<td></td>
</tr>
<tr>
<td>What command is used to disable pagination?</td>
<td>This command is the value used in the template <code>RESET</code> command.</td>
<td><code>terminal pager 0</code></td>
</tr>
<tr>
<td>What command is used to reboot the device?</td>
<td>This command is the value used in the template <code>Reboot</code> command.</td>
<td><code>reload noconfirm</code></td>
</tr>
<tr>
<td>What command is used to configure the terminal?</td>
<td>This command is the value used in the template <code>config terminal</code></td>
<td></td>
</tr>
<tr>
<td>Question</td>
<td>Note</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>enter configuration mode?</td>
<td>EnterConfigMode command.</td>
<td></td>
</tr>
<tr>
<td>What command is used to exit configuration mode?</td>
<td>This command is the value used in the template ExitConfigMode command.</td>
<td>quit</td>
</tr>
<tr>
<td>What command is used to specify the startup configuration?</td>
<td>This command is the value used in the template Startup command.</td>
<td>startup</td>
</tr>
<tr>
<td>What command is used to specify the running configuration?</td>
<td>This command is the value used in the template Running command.</td>
<td>running</td>
</tr>
<tr>
<td>What command sequence is used to directly download</td>
<td>This command sequence is the value used in the template DownloadConfig command*.</td>
<td>show ${ConfigType}</td>
</tr>
</tbody>
</table>
### Chapter 6: Creating and Modifying Device Templates

<table>
<thead>
<tr>
<th>Question</th>
<th>Note</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>the configuration using Telnet or SSH?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What command sequence is used to upload the configuration using Telnet or SSH?</td>
<td>This command sequence is the value used in the template UploadConfig command*.</td>
<td><code>${EnterConfigMode}${CRLF}${ConfigText}${CRLF}${ExitConfigMode}</code></td>
</tr>
<tr>
<td>What command sequence is used to download the configuration using SNMP, that is, indirect transfer?</td>
<td>This command sequence is used in the template DownloadConfigIndirect command*.</td>
<td><code>copy ${TransferProtocol}:/${StorageAddress}/${StorageFilename}/${ConfigType}${CRLF}${CRLF}</code></td>
</tr>
<tr>
<td>What command sequence is used to erase the configuration</td>
<td>This command sequence is used in the template EraseConfig command.</td>
<td>write erase ${CRLF}Yes</td>
</tr>
</tbody>
</table>
### Device Command Template Best Practices

<table>
<thead>
<tr>
<th>Question</th>
<th>Note</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>What command sequence is used to commit a configuration to memory?</td>
<td>This command sequence is used in the template SaveConfig command.</td>
<td>write memory</td>
</tr>
<tr>
<td>What command sequence is used to show the version information?</td>
<td>This command sequence is used in the template Version command.</td>
<td>show version</td>
</tr>
</tbody>
</table>

*For more information about variables that can be used in command scripts and device command templates, see [Pre-Command and Command Template Variables](#).*

### Device Command Template Best Practices

Consult the following best practices before modifying device command templates.

- Review several device templates and familiarize yourself with the appropriate command syntax before creating a new template.
- Write down a list of all the commands you need to include in the new device template, including whether or not you have to press Enter after you type the command to ensure the device recognizes the command.
Telnet to your device to find the pre-commands you need. A pre-command can be used for any device which requires input before prompting for credentials. A pre-command is used before logging in. For example, when you connect to a router and before you are asked for a password, you must press Enter to wake up the connection. Add the following line to the template: `<Command Name="PreCommand" Value="$\{CRLF\}"/>

Create a new device template by modifying an existing device template.

Before modifying a device template, make a copy of the original.

If you have a device that indicates enable mode with any character other than a number sign (#), add the following line to the template: `<Command Name="EnableIdentifier" Value="*"/>

where * is the character used to indicate the enable privilege level.

Ensure that you do not have two command templates with the same System OID.

If the value for the Command Device Template field within the Node Details view is set to Auto Determine, SolarWinds NCM chooses the command template with the System OID value that is closest to the system OID of the device. For example, if the System OID for the device is 1.3.6.1.9.25.5.4, then SolarWinds NCM starts the search for a template that includes 1.3.6.1.9.25.5.4 as the System OID. If no template is found, SolarWinds NCM looks for a template with 1.3.6.1.9.25.5, and then 1.3.6.1.9.25, and so on. To be safe, use the full System OID when building templates.

To declare the ready prompt for your device, use the VirtualPrompt command to designate the prompt: `<Command Name="VirtualPrompt" Value="unc-dsf%"/>

where unc-dsf% is the prompt used by the device to designate it is ready for commands to be sent. You can use the Virtual Prompt to avoid an issue with special characters in banners. For example, to avoid SolarWinds NCM recognizing the number sign (#) as an enable prompt. Ensure you use the MenuBased command when using the VirtualPrompt command: `<Command Name="MenuBased" Value="false"/> or `<Command Name="MenuBased" Value="true"/>

Devices, such as VPN concentrators, may require a null value for the Reset command to function properly. If you receive an Out of Range error, change the value of the Reset command from 0 to blank ( ). For example, `<Command Name="RESET" Value=""/>


Note: Not all commands are supported on all devices.

Communication Process Diagrams
Example: Config Upload and Download (SCP)

File Name
Cisco IOS-1.3.6.1.4.1.9.ConfigMgmt-Commands
Example CLI Device Command Templates

Two examples of device command templates for CLI devices are provided below:
Chapter 6: Creating and Modifying Device Templates

Cisco IOS Example
Nortel BayStack 380 Example
For a list of commands and their descriptions, Command Template Commands.

Cisco IOS Example

File Name
Cisco IOS-1.3.6.1.4.1.9.ConfigMgmt-Commands

Contents
<!--SolarWinds Network Management Tools-->  
<!--Copyright 2008 SolarWinds.Net All rights reserved-->  
<Configuration-Management Device="Cisco Devices" SystemOID="1.3.6.1.4.1.9">  
  <Commands>  
  <Command Name="RESET" Value="terminal width 0${CRLF}terminal length 0"/>  
  <Command Name="Reboot" Value="reload${CRLF}y${CRLF}y"/>  
  <Command Name="EnterConfigMode" Value="config terminal"/>  
  <Command Name="ExitConfigMode" Value="end"/>  
  <Command Name="Startup" Value="startup"/>  
  <Command Name="Running" Value="running"/>  
  <Command Name="DownloadConfig" Value="Show ${ConfigType}"/>  
  <Command Name="UploadConfig" Value="${EnterConfigMode}${CRLF}${ConfigText}${CRLF}${ExitConfigMode}"/>  
  <Command Name="DownloadConfigIndirect" Value="copy ${ConfigType} ${TransferProtocol}:/${StorageAddress}/${StorageFilename} ${CRLF}${CRLF}"/>  
  <Command Name="UploadConfigIndirect" Value="copy ${TransferProtocol}:/${StorageAddress}/${StorageFilename} ${ConfigType}${CRLF}"/>  
  <Command Name="EraseConfig" Value="write erase${CRLF}Y"/>  
</Commands>
<Command Name="SaveConfig" Value="write memory"/>
<Command Name="Version" Value="show version"/>
</Commands>
</Configuration-Management>

Nortel BayStack 380 Example

File Name
Nortel Baystack380-1.3.6.1.4.1.45.3.45.ConfigMgmt-Commands

Contents
<!--SolarWinds Network Management Tools-->  
<!--Copyright 2008 SolarWinds.Net All rights reserved-->  
<Configuration-Management Device="Nortel BayStack 380 Devices" SystemOID="1.3.6.1.4.1.45.3.45">
<Commands>
  <Command Name="RESET" Value="terminal length 0"/>
  <Command Name="Reboot" Value="reload${CRLF}Yes"/>
  <Command Name="EnterConfigMode" Value="config terminal"/>
  <Command Name="ExitConfigMode" Value="end"/>
  <Command Name="Startup" Value="configuration"/>
  <Command Name="Running" Value="running-config"/>
  <Command Name="DownloadConfig" Value="show ${ConfigType}"/>
  <Command Name="UploadConfig" Value="${EnterConfigMode}${CRLF}${ConfigText}${CRLF}${ExitConfigMode}"/>
  <Command Name="DownloadConfigIndirect" Value="copy ${ConfigType} ${TransferProtocol}:/${StorageAddress}/${StorageFilename}${CRLF}"/>
  <Command Name="UploadConfigIndirect" Value="copy ${TransferProtocol}:/${StorageAddress}/${StorageFilename} ${ConfigType}${CRLF}"/>
  <Command Name="Version" Value="show sys info"/>
  <Command Name="PreCommand" Value="${CTRL+Y}"/>
</Commands>
Creating a Menu-Based Command Template

SolarWinds Network Configuration Manager supports the upload and download of configs on menu-based devices that do not have command line interfaces. SolarWinds NCM does not support execution of command scripts on exclusively menu-based devices, however.

All Telnet commands for menu-based devices should be described in the device command template XML file (*.ConfigMgmt-Commands). For more information about file contents, see Command Template Commands.

On some menu-based devices, such as Cisco SF300 LAN switches, menu item numbers can be used instead of arrow moves. For example, instead of assigning:

Value="${ENTER}\n${DownArrow}\n${DownArrow}\n${DownArrow}\n${DownArrow}\n${DownArrow}\n${DownArrow}\n${DownArrow}\n${DownArrow}\n${DownArrow}\n"

You could instead assign:

Value= "1${ENTER}7${ENTER}" \\

Login user name and password have to be sent as pre-command values instead of from the NCM Node Details configuration.

To do this:

1. Clear the user name and password fields for the node in Login Information.
2. Set Enable to <No Enable Login>.
3. Use the following pre-commands:

   <Command Name="PreCommand" Value="username${DownArrow}"/>
   <Command Name="PreCommand" Value="password${ENTER}"/>

The following example provides the values declared for menu-driven indirect transfer:

<Commands>
   <Command Name="RESET" Value="/">
   <Command Name="Reboot" Value="/">
   <Command Name="EnterConfigMode" Value="/">
</Commands>
Creating a Menu-Based Command Template

To create a menu-based device command template:

1. Manually Telnet to your device to discover the pre-commands you must send before the device presents the login screen. Pre-commands are used for any device which requires input before prompting for credentials. For example, when you connect to a router and before you are asked for password, you must press Enter to wake up the connection. Add the following line to the template:

   <Command Name="PreCommand" Value="${CRLF}"/>
2. SolarWinds Network Configuration Manager also sends a *Version* command during the validate login action. To set this command value, complete the following:

   a. To determine this command, find the option in the menu which shows device version information. For example, if the System Information menu shows device version information and to access this menu item you press the down arrow key (↓) twice and then press `Enter`, type the following line into the device command template:

   ```
<Command Name="Version" Value="${DownArrow}${DownArrow}${CRLF}"
   ```

   b. Find the string that is received when the command is complete. For example, if the command is complete when the device responds with System Characteristic, then you must add the following attribute to the command:

   ```
   RegEx="System Characteristic"
   ```

   c. Add a delay between keystrokes by adding the following attribute:

   ```
   Delay="300"
   ```

   d. The complete command line for the Version command is now:

   ```
<Command Name="Version" Value="${DownArrow}${DownArrow}${CRLF}" RegEx="System Characteristic" Delay="300" />
```
3. Access the configuration file menu, and then download a configuration manually. During this operation, note the keys you press to complete this process. For example, on a Nortel Baystack 552048T you would press the following keys to download a configuration:

   a. Down arrow (↓) nine times – Highlights Configuration file menu item
   b. Enter – Opens Configuration file menu
   c. Enter – Opens file Download/Upload menu
   d. ConfigName + Enter – Sets the name of configuration file
   e. Down arrow (↓) + TFTP IP Address + Enter – Sets the TFTP server address
   f. Down arrow (↓) + Space + Enter – Starts the downloading process

4. Translate all these command into SolarWinds NCM variables. In this example, the following commands are used:

   ```
   ${Downarrow}${Downarrow}${Downarrow}${Downarrow}
   ${Downarrow}
   ${Downarrow}${Downarrow}${Downarrow}${Downarrow}
   ${CRLF}
   ${CRLF}
   ${StorageFilename}${CRLF}
   ${DownArrow}${StorageAddress}${CRLF}
   ${DownArrow} ${CRLF}
   
   Note: For a list of commands and their descriptions, see Command Template Commands.
   ```

5. Find the string that is received when the command is complete. For example, the command is complete when the device responds with written. In this case, you must add the following attribute to the command:

   RegEx="written".

6. Add a delay between keystrokes by adding the following attribute:

   Delay="300".

7. The complete download command is as follows:
<Command Name="DownloadConfigIndirect"
Value="${Downarrow}${Downarrow}${Downarrow}${Downarrow}
${Downarrow}${Downarrow}${Downarrow}${CRLF}${CRLF}
${StorageFilename}${CRLF}${DownArrow}
${StorageAddress}${CRLF}${DownArrow} ${CRLF}"
Delay="300" RegEx="written"/>

**Command Template Commands**

The following commands are used to modify and declare the behavior of device templates in SolarWinds NCM. These commands modify the interaction between SolarWinds NCM and your network devices. Ensure you fully understand what modifications will do before modifying a device in production using these commands.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomPasswordPrompt</td>
<td>Allows you to specify the password prompt issued by a device in case NCM is having trouble recognizing the device's prompt (for example, due to unsupported characters).</td>
</tr>
<tr>
<td>DownloadConfig</td>
<td>Series of commands used to download a configuration from a device</td>
</tr>
<tr>
<td>DownloadConfigIndirect</td>
<td>Series of commands used to download a configuration indirectly from a device using TFTP.</td>
</tr>
<tr>
<td>DownloadConfigIndirectSCP</td>
<td>Series of commands used to download a configuration indirectly from a device using SCP</td>
</tr>
<tr>
<td>EnableCommand</td>
<td>Allows you to declare a custom enable command for those devices that do not useEnable as the command.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EnableIdentifier</td>
<td>Only used when a device does not return the # symbol at the end of a prompt to indicate enable mode. Declare the value displayed while in enable mode for a device.</td>
</tr>
<tr>
<td>EnterCLI</td>
<td>Specifies the commands to send upon receiving the VirtualPrompt command to enter the CLI mode of the menu driven command. Use pre-command variables to declare the command values. For more information, see Pre-Command and Command Template Variables.</td>
</tr>
<tr>
<td>EnterConfigMode</td>
<td>Series of commands used to enter the configuration mode of a device</td>
</tr>
<tr>
<td>ExitConfigMode</td>
<td>Series of commands used to exit the configuration mode of a device</td>
</tr>
<tr>
<td>IPAddress</td>
<td>The IP address of the server where SolarWinds Network Configuration Manager is installed</td>
</tr>
<tr>
<td>MenuBased</td>
<td>Specifies whether the device is menu- or CLI-based. If a device is menu-based and you can switch it to CLI from the menu, use the VirtualPrompt and EnterCLI commands to do so. Valid values are true or false.</td>
</tr>
<tr>
<td>MenuDrivenConfigStart</td>
<td>Allows you to declare a value after which the transmitted data is considered the config, requested from the menu-driven device. For example, in the Cisco VPN Concentrator device template, the declared value is #######. The information sent after the ten hash signs is saved as the requested configuration file.</td>
</tr>
</tbody>
</table>
### Chapter 6: Creating and Modifying Device Templates

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>More</td>
<td>Specifies the More prompt in the rare instance that this prompt is not recognized automatically. Do not specify this command unless you are experiencing issues with paging.</td>
</tr>
<tr>
<td>Precommand</td>
<td>Specifies the device requires a pre-command. For more information, see <a href="#">Pre-Command and Command Template Variables</a>.</td>
</tr>
<tr>
<td>Reboot</td>
<td>Series of commands used to reboot the device</td>
</tr>
<tr>
<td>RebootAt</td>
<td>Series of commands used to reboot a device at a specified time. Use the variables listed in the <a href="#">Configuration Archive Variables</a> section to assign the date and time.</td>
</tr>
<tr>
<td>RESET</td>
<td>Series of commands used to set the length and pagination of the session</td>
</tr>
<tr>
<td>Running</td>
<td>Value used to specify a running configuration type</td>
</tr>
<tr>
<td>SaveConfig</td>
<td>Series of commands used to write the configuration to the devices memory</td>
</tr>
<tr>
<td>Startup</td>
<td>Value used to specify a startup configuration type.</td>
</tr>
<tr>
<td>UploadConfig</td>
<td>Series of commands used to upload a configuration to a device</td>
</tr>
<tr>
<td>UploadConfigIndirect</td>
<td>Series of commands used to upload a configuration indirectly to a device using TFTP.</td>
</tr>
<tr>
<td>UploadConfigIndirectSCP</td>
<td>Series of commands used to upload a configuration indirectly to a device using SCP.</td>
</tr>
</tbody>
</table>
### Pre-Command and Command Template Variables

Pre-command variables are used in command scripts and device command templates. The Pre-command variables mimic keyboard strokes that are normally entered in the command interface. For more information on creating command scripts, see [Working with Command Scripts](#).

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${ConfigType}</td>
<td>Value used to insert the type of configuration</td>
</tr>
<tr>
<td>${CR}</td>
<td>Carriage return</td>
</tr>
<tr>
<td>${CRLF} or $[ENTER]</td>
<td>Carriage return - linefeed combination</td>
</tr>
<tr>
<td>${CTRL+@}</td>
<td>CTRL + @</td>
</tr>
<tr>
<td>${CTRL+A}</td>
<td>CTRL + A</td>
</tr>
</tbody>
</table>
### Chapter 6: Creating and Modifying Device Templates

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${CTRL+B}</td>
<td>CTRL + B</td>
</tr>
<tr>
<td>${CTRL+C}</td>
<td>CTRL + C</td>
</tr>
<tr>
<td>${CTRL+D}</td>
<td>CTRL + D</td>
</tr>
<tr>
<td>${CTRL+E}</td>
<td>CTRL + E</td>
</tr>
<tr>
<td>${CTRL+F}</td>
<td>CTRL + F</td>
</tr>
<tr>
<td>${CTRL+G}</td>
<td>CTRL + G</td>
</tr>
<tr>
<td>${CTRL+H}</td>
<td>CTRL + H</td>
</tr>
<tr>
<td>${CTRL+I}</td>
<td>CTRL + I</td>
</tr>
<tr>
<td>${CTRL+J}</td>
<td>CTRL + J</td>
</tr>
<tr>
<td>${CTRL+K}</td>
<td>CTRL + K</td>
</tr>
<tr>
<td>${CTRL+L}</td>
<td>CTRL + L</td>
</tr>
<tr>
<td>${CTRL+M}</td>
<td>CTRL + M</td>
</tr>
<tr>
<td>${CTRL+N}</td>
<td>CTRL + N</td>
</tr>
<tr>
<td>${CTRL+O}</td>
<td>CTRL + O</td>
</tr>
<tr>
<td>${CTRL+P}</td>
<td>CTRL + P</td>
</tr>
<tr>
<td>${CTRL+Q}</td>
<td>CTRL + Q</td>
</tr>
<tr>
<td>${CTRL+R}</td>
<td>CTRL + R</td>
</tr>
<tr>
<td>${CTRL+S}</td>
<td>CTRL + S</td>
</tr>
<tr>
<td>${CTRL+T}</td>
<td>CTRL + T</td>
</tr>
<tr>
<td>${CTRL+U}</td>
<td>CTRL + U</td>
</tr>
<tr>
<td>${CTRL+V}</td>
<td>CTRL + V</td>
</tr>
</tbody>
</table>
### Example Pre-Command Device Template Entry

The following line from a device command template specifies the pre-command, the delay, and the text that triggers the pre-command. Delay and trigger text (RegEx) are optional variables.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${CTRL+W}</code></td>
<td>CTRL + W</td>
</tr>
<tr>
<td><code>${CTRL+X}</code></td>
<td>CTRL + X</td>
</tr>
<tr>
<td><code>${CTRL+Y}</code></td>
<td>CTRL + Y</td>
</tr>
<tr>
<td><code>${CTRL+Z}</code></td>
<td>CTRL + Z</td>
</tr>
<tr>
<td><code>${CTRL+[]}</code></td>
<td>CTRL + [ (equivalent to ESC key press)</td>
</tr>
<tr>
<td><code>${CTRL+\}</code></td>
<td>CTRL + \</td>
</tr>
<tr>
<td><code>${CTRL+]}</code></td>
<td>CTRL + ]</td>
</tr>
<tr>
<td><code>${CTRL+CTRL}</code></td>
<td>CTRL + CTRL</td>
</tr>
<tr>
<td><code>${CTRL+_]}</code></td>
<td>CTRL + _</td>
</tr>
<tr>
<td><code>${UPARROW}</code></td>
<td>Up Arrow</td>
</tr>
<tr>
<td><code>${DOWNARROW}</code></td>
<td>Down Arrow</td>
</tr>
<tr>
<td><code>${RIGHTARROW}</code></td>
<td>Right Arrow</td>
</tr>
<tr>
<td><code>${LEFTARROW}</code></td>
<td>Left Arrow</td>
</tr>
<tr>
<td><code>${StorageAddress}</code></td>
<td>Value used to insert the TFTP server IP address or hostname</td>
</tr>
<tr>
<td><code>${StorageFilename}</code></td>
<td>Value used to insert the name generated by SolarWinds NCM for the downloaded configuration file</td>
</tr>
<tr>
<td><code>${TransferProtocol}</code></td>
<td>Value used to insert the transfer protocol used during indirect transfer</td>
</tr>
</tbody>
</table>
Chapter 6: Creating and Modifying Device Templates

<Command Name="Precommand" Value="${CTRL+Y}" Delay="3" RegEx="password:"/>

Notes:

- Device command templates are located in the DeviceTypes folder of your installation folder.
- The default location is: \Program Files\SolarWinds\Configuration Management\DeviceTypes\.

Using Command Template Variables to Preclude Pseudoterminal Setup

If your device does not support pseudoterminal device pairs, you can prevent Telnet from attempting to negotiate pseudoterminal setup by using the following command variable:

<Command Name="allocatePty" Value="false"/>

Specifies that the command script will be run with pseudoterminal mode disabled.

Using Command Template Variables to Declare a Special Command Prompt

If the command prompt is not > or #, or you need to specify more than one character to designate the command prompt, as in the case of banners using the # symbol, declare the command prompt using the following command variables:

<Command Name="MenuBased" Value="false"/>

Specifies that the template logic should run in CLI mode

<Command Name="VirtualPrompt" Value="CustomPrompt%"/>

Specifies the exact value of the command prompt designating the device is ready to receive commands.

Using Command Template Variables to Switch User Context

If you log on to a device and must switch user context to execute a command, resulting in a different command prompt, use the following command variables to switch context and recognize the new command prompt:

<Command Name="MenuBased" Value="false"/>
Specifies that the template logic should run in CLI mode

<Command Name="Reset"
Value="appropriateSwitchContextCommands"
RegEx="newPrompt"/>

Specifies the reset command to switch user context and the new command prompt to expect. Use pre-command variables to designate the switch context commands and specify the entire new prompt in the RegEx value.

Using Command Template Variables to Respond to Post-Logon Interaction Requests

If you log on to a device and perform an action and are then prompted for interaction (for example, you receive a *Press Any Key* prompt), use the following command variables in the command template to not time out:

<Command Name="PreCommand" Value="${CTRL+Y}"/>

Sent when the device does not respond for three seconds.

<Command Name="PreCommand" Value="${CTRL+Y}" Delay="3"/>

Sent when the device does not respond for more than three seconds.

<Command Name="PreCommand" Value="${CTRL+Y}" Delay="3"
RegEx="Press Any Key"/>

Sent when the device does not respond for more than three seconds and the last received data was *Press Any Key*.

Troubleshooting Device Connections

When you experience problems connecting to a device, you may need to perform a session trace to troubleshoot the issue. A session trace shows all communication sent to and from the network device to which you are connecting. The session trace log contains error messages and commands sent that generated the error.

1. From the web console, click **Settings > NCM Settings**.
2. Under Advanced, click **Advanced Settings**.
3. Select **Enable Session Tracing**.
4. Perform the steps to recreate the issue you are troubleshooting.
5. Open the session trace file.
6. Apply the necessary changes to the device command template to resolve the issue. For more information, see Creating and Modifying Device Templates.
Chapter 7: Working with Command Scripts

Several tasks can be automated with command scripts, for example:

- Downloading configuration files
- Uploading configuration files
- Uploading IOS images
- Updating logon banners
- Updating access control lists (ACLs)

With the appropriate use of variables, a single script can be executed on several different devices, without concern for syntax differences.

Note: Scripts are delivered one line at a time to the target devices.

For more information:

Executing Command Scripts
Using Variables within Scripts
Chapter 7: Working with Command Scripts

Executive Command Scripts

1. From the web console, click **CONFIGS > Configuration Management**.
2. Click the Script Management tab.
3. Click **Add new script**.
4. Add the script information.
5. Click **Save**.
6. Click the Config Management tab.
7. Select one or more nodes.
8. Click **Execute Script**.
9. Select a script or click **Load Script from File**.
   
   **Note:** You can specify a delay (in seconds) inside a script. A delay is the time NCM will wait before sending the next command. The following is a sample script that includes a delay:

   ```
   {Command 1}
   ${Delay:20}
   {Command 2}
   ```

   This feature is useful, for example, when uploading a flash image. Some time is required for the formatting of the flash to complete before then performing the image upload.

10. Select script options at the bottom if necessary.
11. Click **Execute**.

Using Variables within Scripts

Variables are a powerful feature of the SolarWinds NCM scripting engine. Variables always begin with a dollar sign and curly brace (${}) and end with a curly brace (}).

Script variables substitute the appropriate commands based on the device type. For example, the variable ${EnterConfigMode} parses as *config terminal* when communicating with Cisco IOS devices, but parses as *configure* when communicating with an HP Procurve Switch.
For more information: Command Template Commands.

Example Variable Script

The following script contains commands with variables to remove the public read-only community string:

${EnterConfigMode}no snmp-server community public RO${ExitConfigMode}${SaveConfig}${Reboot}

Parsed for Cisco IOS devices:

config terminal
no snmp-server community public RO
end
write
memory
reload
${CRLF}y${CRLF}y

Parsed for a Dell PowerConnect Switch:

config
no snmp-server community public RO
end
copy
running-config
startup-config
${CRLF}${CRLF}reload
${CRLF}Yes

Note: The ${CRLF} variable equals a carriage return line feed for all devices.

Defining Script Variables

Script variables are defined in device command templates. Templates are located in the \Configuration Management\DeviceTypes folder. Each .ConfigMgmt-Commands file contains a System OID that is used to uniquely identify a device. A list of command names, and the corresponding commands to be sent to the device when the command name is called, are also included in the templates. These command names are the variables used when creating a script.

Consider the following line taken from the Cisco IOS device command template:

<Command Name="EnterConfigMode" Value="config terminal"/>

When a script is run on a Cisco IOS device, the variable ${EnterConfigMode} parses as config terminal. New command names can be added and existing command names can be modified within these files.

Referencing Variables with Variables

The script engine also allows you to reference variables with variables. For example, you can define a complex variable in the device template:
Chapter 7: Working with Command Scripts

ShowInt = running | include interface

Then define another variable that includes the first:
Reveal = show ${ShowInt}

When you call ${Reveal}, it equals show running | include interface.

For more information about variables that can be used in command scripts and device command templates, see Command Template Commands.
Chapter 8: Working with Config Change Templates

SolarWinds Network Configuration Manager allows you to create, use, and manage config change templates that streamline making recurrent and complex configuration changes.

Generate and execute accurate sets of CLI commands with a single config change template. Perform a specific task on different machine types in your network.

For more information:
- Config Change Template Basics
- Understanding Config Change Template Details
- Additional Examples of Working with Configuration Change Templates
- Executing a Config Change Template
- Creating a Config Change Template
- Editing a Config Change Template
- Importing a Config Change Template
- Tagging a Config Change Template
- Exporting a Config Change Template (to thwack)
- Exporting a Config Change Template (as a file)
- Deleting a Config Change Template
- SolarWinds Information Services Data Entities
Chapter 8: Working with Config Change Templates

**Config Change Template Basics**

A change config template enables you to accomplish a specific device configuration task for a set of NCM-managed nodes. *Template* describes the runtime wizard through which the user selects the NCM nodes or interfaces targeted for the change. The script behind the wizard articulates the logic of the configuration change itself.

An example of configuration change workflow is an IT manager who creates the script for a template, and other team members who use the template’s wizard to perform the specific configuration changes on a set of NCM-managed nodes.

The framework for creating config change templates depends on the SolarWinds Information Service (SWIS). SWIS is an API that is installed with NCM and that interacts with inventory data in the Orion platform database. Any device that has not been inventoried in NCM cannot be targeted with a config change template. Each object in a device inventory is a SWIS entity that can be referenced in specific ways within scripts.

Examples of routine changes you can expedite with config change templates include:

- Changing VLAN membership by device port
- Configuring device interfaces based on description
- Enabling IPSLA for VOIP implementations
- Managing NetFlow collection at the source devices

For more information:

- Preparation and Use of a Template
- Parts of a Config Change Template

**Preparation and Use of a Template**

Every change config template does its work based on NCM device inventory objects. Those objects are the database entities that the SolarWinds Information System accesses in managing NCM’s communication with its database. As a result, performing an NCM device inventory and updating device inventories are the prerequisites for creating and running a config change template.
See the section SolarWinds SolarWinds Information Services Data Entities for all the NCM device entities and their properties that you can use in your work with config change templates.

Two types of NCM users work with config change templates:

- **Template Creator**: This user creates the script for a config change template. The user must know the basics of writing a script that uses commands, variables, and logical structures.
  
  When executed, a config change template displays a wizard that uses input values to generate CLI commands that accomplish a specific config change on targeted NCM devices. Based on input, the template’s run-time wizard generates a different set of commands for each type of device that you specify as a target for config changes.

  **Note**: You must have the NCM role of Administrator or Engineer to create or edit a change config template.

- **Template User**: This user enters values based on a template's run-time wizard input prompts, reviews the CLI commands that the template outputs for each type of targeted device, and tells NCM to execute the commands against targeted NCM devices. The user makes specific config changes if necessary.

  **Note**: You must have the NCM role of Administrator, Engineer, or WebUploader to use a change config template.

**For more information:**

- Parts of a Config Change Template
- Config Change Template Basics
- Understanding Config Change Template Details
- Additional Examples of Working with Configuration Change Templates
- Executing a Config Change Template
- Creating a Config Change Template
- Editing a Config Change Template
- Importing a Config Change Template
- Tagging a Config Change Template
Chapter 8: Working with Config Change Templates

Exporting a Config Change Template (to thwack)
Exporting a Config Change Template (as a file)
Deleting a Config Change Template

Parts of a Config Change Template

Every config change template includes two parts: parameters and commands.

Parameters

Parameters tell a user about the template’s purpose through its descriptions. Parameters prompt the user for the values, such as the specific node(s) on which to make the template’s specific config change.

Commands

Commands declare the input type for a variable through arguments. Commands include arguments and logical operations needed to produce a set of CLI commands and execute those commands against each NCM node targeted for a specific config change.

A template creator develops a script for a template by defining the parameters that tell a user about the template and associating a description or label with a variable in the template’s user interface.

For more information:

Preparation and Use of a Template
Config Change Template Basics
Understanding Config Change Template Details
Additional Examples of Working with Configuration Change Templates
Executing a Config Change Template
Creating a Config Change Template
Editing a Config Change Template
Importing a Config Change Template
Tagging a Config Change Template
Exporting a Config Change Template (to thwack)
Exporting a Config Change Template (as a file)
Deleting a Config Change Template

Understanding Config Change Template Details

A config change template named *Change VLAN Membership on ports Cisco IOS* installs with SolarWinds NCM. Its purpose is to change VLAN membership on Cisco (IOS) device ports.

The following sections explain the specific components of a config change template by demonstrating how to use the *Change VLAN Membership on ports Cisco IOS* template to make VLAN membership config changes on hypothetical Cisco device interfaces.

Viewed as parsable code, a config change template consists of two parts: parameters and commands. For more information, see Parts of a Config Change Template.

Example

This section assumes that you know how to make VLAN membership changes to device interfaces from the Cisco IOS command line. This section also assumes that you are familiar with using variables, data arrays, foreach loops, if/else conditional statements, and logical operators in creating system administration scripts.

The following sections show the reference template broken up into parameter, command, and output sections.

Parameters

These are the parameters for the *Change VLAN Membership on ports Cisco IOS* template. Notice that the parameters already have values associated with them, which are either a string or a variable.

```c
/*
   .CHANGE_TEMPLATE_DESCRIPTION
       This change template configures VLAN membership on Cisco IOS devices. The template was verified on Cisco 2950 Catalyst Switch running IOS software version 12.1(12c).
   .CHANGE_TEMPLATE_TAGS
       Cisco, IOS, VLAN Membership
```
Chapter 8: Working with Config Change Templates

.PLATFORM_DESCRIPTION
  Cisco IOS

.PARAMETER_LABEL @ContextNode
  NCM_Node
.PARAMETER_DESCRIPTION @ContextNode
  The node the template will operate on. All templates require this by default. The target node is selected during the first part of the wizard so it will not be available for selection when defining values of variables.

.PARAMETER_LABEL @TargetPorts
  Select Port(s)
.PARAMETER_DESCRIPTION @TargetPorts
  Select the port(s) for which you would like to change VLAN membership.

.PARAMETER_LABEL @VlansToRemove
  VLAN(s) to remove
.PARAMETER_DESCRIPTION @VlansToRemove
  Select the VLAN(s) you would like to remove. Selecting VLANs irrelevant to interfaces simply will result in no actions taken for those interfaces.

.PARAMETER_LABEL @VlanToAssign
  VLAN to assign
.PARAMETER_DESCRIPTION @VlanToAssign
  Select the VLAN you would like to assign.

/*

Commands

There is one instance of the script command and multiple instances of the CLI{ } command, and all variables have declarations.

script ConfigureVLANmembershipCiscoIOS (   NCM.Nodes @ContextNode,   NCM.Interfaces[] @TargetPorts,   NCM.VLANs[] @VlansToRemove,
NCM.VLANs @VlanToAssign 
{
    // Enter configuration mode
    CLI
    {
        configure terminal
    }

    // Loop through selected ports
    foreach (@portItem in @TargetPorts)
    {
        CLI
        {
            interface @portItem.InterfaceDescription
        }

        // Loop through list of vlans to remove
        foreach (@vlanRemove in @VlansToRemove)
        {
            CLI
            {
                no switchport access vlan @vlanRemove.VLANID
            }
        }

        CLI
        {
            switchport access vlan @VlanToAssign.VLANID
        }

        CLI
        {
            exit
        }
    }

    // Exit configuration mode
    CLI
    {

Chapter 8: Working with Config Change Templates

```
exit
}
}
```

**Output Commands**

These are the commands that NCM executes after logging on to the NCM device (s) selected as the target for this config change template. We are changing VLAN membership on one interface of two different Cisco switches.

NCM Node bgp-2651-03configure terminalinterface
FastEthernet0/0/no switchport access vlan 1004
switchport access vlan 1002
exitend
NCM Node cur-3725Configure terminalinterface
FastEthernet0/1/no switchport access vlan 1004
switchport access vlan 1002
exitend

**Setting Up Parameters**

The parameters of a script define and label the variables for which a user of the template must provide appropriate values when the template is executed.

The script of every config change template includes at least five parameters. Only one, **PARAMETER_LABEL**, can recur in a single template and each instance requires user input to determine the value of a specific variable.

**Required Parameters**

**CHANGE_TEMPLATE_DESCRIPTION**

This parameter appears at the top of the script and briefly explains the purpose of the template. It does not have any associated variable(s) and is not exposed in the run-time wizard.

**CHANGE_TEMPLATE_TAGS**

This parameter holds the tags that NCM uses to provide grouping options in the Config Change Template resource. It does not have any associated variable(s) and is not exposed in the run-time wizard.
PLATFORM DESCRIPTION

This parameter defines the type of NCM device for which the template is designed.

PARAMETER_LABEL @<variable_name>

Each instance of this parameter in a config change template is associated with a specific variable. The template's run-time wizard requires the user to provide the value for each parameter variable.

By providing the input parameters for executing a template, PARAMETER_LABEL delimits the data that a template can use. Think of PARAMETER_LABEL as simultaneously making a variable available for user input and providing the metadata so that the user knows what the variable is holding a place for.

For example, PARAMETER_LABEL is used in every template with @ContextNode. The user sets the value by selecting the NCM node(s) that will be targeted for config change. An instance of the parameter appears in a script as follows:

.PARAMETER_LABEL @ContextNode NCM Node

In this case, NCM Node is the actual label that appears under the field where the NCM nodes are selected in the template's run-time wizard.

A config change template may have as many instances of PARAMETER_LABEL as needed to support the user input needed for the template.

PARAMETER_DESCRIPTION

This parameter holds the explanatory text for an input field and always appears after PARAMETER_LABEL.

For example, the PARAMETER_DESCRIPTION for the input field labeled NCM Node might be something like:

"The NCM nodes the template will operate on. Target nodes are selected during the first part of the wizard and cannot be changed when defining values of variables."

Optional Parameters

PARAMETER_DISPLAY_TYPE

This parameter creates a list of options. The format for using this parameter is as follows. The pipe character (|) divides the items in the list.
Chapter 8: Working with Config Change Templates

PARAMETER_DISPLAY_TYPE @VariableName
Listbox:1=String1|2=String2|3=String3

Basic Commands

There are two commands in a config change template: script and CLI.

Script Command

The script{} command declares the input type of every variable that the template uses. The script command declares the input type for every variable introduced in setting up the template parameters. The form of the script command is:

```
script script_name (  
    data_type @variable  
    data_type @variable  
    data_type @variable  
)  
```

The data_type can be swis.entity (for example, NCM.Nodes), int (integer), or string.

Cisco Example

```
script ConfigureVLANmembershipCiscoIOS (  
    NCM.Nodes @ContextNode,  
    NCM.Interfaces[] @TargetPorts,  
    NCM.VLANs[] @VlansToRemove,  
    NCM.VLANs[] @VlanToAssign  
)
```

Four variables are introduced in the parameter section of the template with an instance of PARAMETER_LABEL given a specific SolarWinds Information Service entity data type:

- **@ContextNode** is determined with data from the NCM.Nodes entity in the database.
- **@TargetPorts** is determined with data from the NCM.Interfaces entity.
- **@VlansToRemove** and **@VlanToAssign** are determined with data from the NCM.VLANs entity.
Note: Any variable that references an NCM object that NCM knows through device inventory must take a SolarWinds Information Service entity as its data type. In this case, the four variables work with data that NCM captured and stored in the database through the device inventory process. If you attempt to assign a string instead of a SWIS entity in such cases, NCM will fail to correctly parse your script.

CLI command

CLI{ } defines a specific CLI command that NCM issues on a target device when the config change template is executed by a user.Script command. Its purpose is to create a command line statement that NCM can execute directly on the command line of NCM nodes targeted for the template’s config change(s).

The config change template creator creates a CLI command by including its arguments wrapped by curly brackets { }. At run time, NCM parses any variables contained within CLI { }. Often a CLI command is as simple as the command you would type directly on the command line of an NCM device.

Cisco Example

To enter config mode on Cisco IOS devices, type configure terminal. In your config change template script, add the command as follows:

```java
CLI
{
  configure terminal
}
```

NCM parses the argument of the CLI { } command by passing through the string itself (configure terminal) as a command to execute against each targeted NCM node at template run time:

Cisco Example with Variables

```java
script ConfigureVLANmembershipCiscoIOS ( 
  NCM.Nodes @ContextNode, 
  NCM.Interfaces[] @TargetPorts, 
  NCM.VLANs[] @VlansToRemove, 
  NCM.VLANs[] @VlanToAssign 
) 
{
  CLI
}
```
Chapter 8: Working with Config Change Templates

```
{
    vlan database vlan @vlaniddescription @vlandesc exit
}
```

This example shows a CLI statement with variables to specify VLAN properties while using the `vlan database` command line editor. For purposes of demonstration, we assume that:

- `@vlanid = 1`
- `@vlandesc = Local-Office`

At run time, NCM parses the `CLI{ }` command as:
```
vlan database vlan 1 description Local-Office exit
```

If this were all that is included in the *Change VLAN membership on ports Cisco IOS* template, then the config change result would be to set the description of `vlan 1` to `Local-Office` on all NCM nodes selected as targets.

This config change template, however, actually changes the VLANs associated with targeted NCM node ports. For that we need to introduce advanced `CLI{ }` command logic.

**Advanced Commands**

The scripting framework for change config templates allows you to create `CLI{ }` command arguments that include `foreach` loops, `if/else` conditional operations, and functions for manipulating string patterns.

**Foreach Loops**

A `foreach` statement iterates through an array of items based on a SolarWinds Information Service (SWIS) entity data type. Foreach statements use the following pattern:
```
foreach (@ItemVaraible in @EntityArrayVariable)
```

A primary purpose of a `foreach` loop is to allow the template user to select multiple NCM objects for config change. The loop instructs NCM to perform the same config change on all items in scope as determined by the SWIS entity in the database and delimited at run time by the template user’s selections in the template wizard.
Cisco Example

```cisco
foreach (@portItem in @TargetPorts) {
    CLI{
        interface @portItem.InterfaceDescription
    }
}
```

The `foreach` statement creates a set that contains two related variables: `@portItem` and `@TargetPorts`. The `@TargetPorts` variable holds an array of objects with the data type of an SWIS entity called `NCM.Interfaces[]`. The array will be a set of interfaces on NCM nodes.

The `@TargetPorts` variable is associated with the `PARAMETER_LABEL Select port(s)` and the template user selects one or more ports at run time. The template user determines the set of interfaces to fill the array `NCM.Interfaces[]`, and the template will perform VLAN membership config changes on each interface in that array.

`@portItem` is a dynamic variable that the loop uses during its iterating to hold the value of the current interface from the array represented by `@TargetPorts`.

The foreach loop format is fixed and NCM expects it to include the dynamic variable.

The user interacts with this template wizard screen:

![Config Change Templates](image)

**Execute Change VLAN membership on ports Cisco IOS**

**Select Nodes > Define Variables > Preview**

**Define variables in config change template**

The variables below exist in this config change template and need to be defined each time you run it.

- **Select Port(s)**: 0 Entities Selected
  Select the port(s) for which you would like to change VLAN membership.

- **VLAN to remove**: 0 Entities Selected
  Select the VLAN(s) you would like to remove. Selecting VLAN(s) irrelevant to interfaces simply will result in no action taken for those interfaces.

- **VLAN to assign**: 0 Entities Selected
  Select the VLAN you would like to assign.
Chapter 8: Working with Config Change Templates

Click Select Interface List to load a tree that displays available interfaces and NCM nodes previously selected in the wizard:

![Select Interface List](image)

Conditional Statements

Conditional logic in a config change template script uses an if/else pattern to define two branches of possible action, enclosing specific conditions within parentheses. Within each branch of the conditional pattern are CLI{ } commands to execute if that branch meets the specific conditions.

Here is the basic structure:

```plaintext
if (condition is true)
CLI
{
  execute commands
}
else
CLI
{
  Execute other commands
}
```
**Note:** The else section is optional. If you omit it, and the if condition is false, NCM excludes the relevant CLI commands from the template output.

**Operators**

Use any of these operators to specify a parenthetical condition:

<table>
<thead>
<tr>
<th>Operator</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>==</td>
<td>Is Equal To</td>
</tr>
<tr>
<td>&gt;</td>
<td>Is Greater Than</td>
</tr>
<tr>
<td>&gt;=</td>
<td>Is Greater Than or Equal To</td>
</tr>
<tr>
<td>&lt;</td>
<td>Is Less Than</td>
</tr>
<tr>
<td>&lt;=</td>
<td>Is Less Than or Equal To</td>
</tr>
<tr>
<td>!=</td>
<td>Is Not Equal To</td>
</tr>
<tr>
<td>Contains</td>
<td>'string'</td>
</tr>
<tr>
<td>containsExact</td>
<td>'case sensitive string'</td>
</tr>
<tr>
<td>startsWith</td>
<td>'string'</td>
</tr>
<tr>
<td>startsWithExact</td>
<td>'case sensitive string'</td>
</tr>
<tr>
<td>endsWith</td>
<td>'string'</td>
</tr>
<tr>
<td>endsWithExact</td>
<td>'case sensitive string'</td>
</tr>
</tbody>
</table>

**Note:** Use single quotes around string values.

**Cisco Example**

Add conditional logic in the foreach loop to prevent errors that may occur if the user accidentally selects an inappropriate interface (for example, the loopback address).

```csharp
foreach @portItem in @TargetPorts)
{
    if (@PortItem.InterfaceDescription != ‘Loop0’)
    {
```
Chapter 8: Working with Config Change Templates

CLI
{
    interface @portItem.InterfaceDescription
}

If the template encounters the loopback interface, it does nothing and passes on to the next interface. This code prevents damage from template user error.

**Manipulating Strings**

Five functions for manipulating strings constitute a final scripting resource that you can use most readily for managing ACL config changes for network firewalls, in which a config change template needs to iterate through a predictably variable set of IP addresses, for example.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Declaration</th>
<th>Variable Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Substring</td>
<td>Specify a starting point within a string and the length from the starting point that you want to capture for manipulation.</td>
<td>string Substring (string str, int startIndex, int length)</td>
<td>• str is the full string from which the substring comes • startIndex marks the position where the substring begins • length is the number of characters that the substring includes</td>
</tr>
<tr>
<td>Function</td>
<td>Description</td>
<td>Declaration</td>
<td>Variable Definitions</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>StrLength</td>
<td>Return the length of a string.</td>
<td>In StrLength (string str)</td>
<td>• <em>str</em> is the user-input string whose length is used as the integer value</td>
</tr>
<tr>
<td>IndexOf</td>
<td>Find the number of characters in a string.</td>
<td>int IndexOf (string str, string search)</td>
<td>• <em>str</em> is a string to search on</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <em>search</em> is a user-input string NCM uses to find the numerical value of the string being searched</td>
</tr>
<tr>
<td>SetOctet</td>
<td>Replace an octet within an IP address.</td>
<td>string SetOctet (string ipAddress, int octetPosition, string octet)</td>
<td>• <em>ipAddr</em> is the IP address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <em>octetPostion</em> marks the position where the target octet begins</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <em>octet</em> is the new value of the target octet</td>
</tr>
<tr>
<td>GetOctet</td>
<td>Retrieve an octet from a user-specified IP address and octet position.</td>
<td>string GetOctet (string ipAddress, int octetPosition)</td>
<td>• <em>ipAddress</em> is a user-input IP address</td>
</tr>
</tbody>
</table>
Chapter 8: Working with Config Change Templates

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Declaration</th>
<th>Variable Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>• octetPosition is the user-input value for the place where the function finds the beginning of the octet to get</td>
</tr>
</tbody>
</table>

Example 1: Manipulating a String

```script
text IPshuffle(string @str, string @search )
{
    int @length = strlen(@str)
    int @startIndex = indexof(@str,@search)
    int @substringLength = @length - @startIndex
    @res = substring(@strA, @startIndex, @substringLength)

    CLI
    {
        @res
    }
}
```

The user enters ABCDEF for the @str variable and CD for the @search variable in the template’s wizard. Based on those values, the script does the following:

1. Uses ABCDEF in the `strlen` function to give a value of 6 to a variable called @length.
2. Uses CD as the substring of ABCDEF to set a value 2 for the variable called @startIndex.
3. Subtracts 2 (@startIndex) from 6 (@length) to determine the value of @substringLength as 4.
4. Takes the original string ABCDEF and calculates a result (@res) using @startIndex to count in two positions and @substringlength to count four positions from the start index.

5. Outputs CDEF as the result.

Example 2: Changing an Access Control List

This example creates a block of Access Control List (ACL) instructions that predictably vary the value of a specific octet within an IP address. The instructions conform to the pattern 10.10.@id.10, where the value of @id is determined by user input.

The user enters 10.10.10.10 as the value of @ipaddress in the config change template’s run-time wizard. The user enters 1, 22, and 222 for the @indexes variable declared in the script command.

```plaintext
PARAMETER_LABEL @ipaddress
IP address
PARAMETER_DESCRIPTION @ipaddress
Enter an IP address

PARAMETER_LABEL @indexes
Octets
PARAMETER_DESCRIPTION @indexes
Enter a pattern of octet replacements. Separate numbers with a comma.
*
```

```plaintext
script ACLChanges(string @ipaddress, int[] @indexes)
{
    string @ipnew

    foreach(@id in @indexes)
    {
        @ipnew = setoctet(@ipaddress,3,@id)
        CLI
        { Allow @ipnew out
        Allow @ipnew UDP 2055 OUT
        }
```

```
The script uses the `SetOctet` function to determine the value of an `@ipnew` variable. `SetOctet` is defined to take the user-input IP address and create a new IP address by iteratively replacing the third octet with user-input values. For each new IP address, the script produces a command to create outgoing UDP transmission access through port 2055:

- Allow 10.10.1.10 out
- Allow 10.10.2.20 out
- Allow 10.10.22.10 out
- Allow 10.10.222.10 out

**Example 3: Managing an Access Control List for Multiple Routers**

In this example, a config change template generates a block of ACL instructions for a router in a store. We create an ACL block of instructions for this device that varies based on a portion of the device’s IP address.

If the store has four routers, 10.1.1.1, 10.1.4.1, 10.1.6.1, and 10.1.10.1, the template script generates an ACL block that appears this way on the selected router (10.1.1.1):

- Allow 10.1.2.0/24 out
- Allow 10.1.2.4 UDP 2055 OUT
- Allow 10.1.4.0/24 out
- Allow 10.1.4.4 UDP 2055 OUT
- Allow 10.1.6.0/24 out
- Allow 10.1.6.4 UDP 2055 OUT
- Allow 10.1.10.0/24 out
- Allow 10.1.10.4 UDP 2055 OUT

Here is the script that produces the output:

```bash
class OpenACLs(NCM.Nodes @ContextNode, string[] @IpRouters)
{
    foreach (@ipRouter in @IpRouters) {
        // Logic for processing ipRouter
    }
}
```
Example 3: Managing an Access Control List for Multiple Routers

```c
string @octet = getoctet(@IpRouter, 3)
string @ipnew = setoctet(@ContextNode, 3, @octet)
CLI
{
    Allow @ipnew out
    Allow @ipnew UDP 2055 OUT
}
```

This script does the following:

- Uses a foreach loop to go through a user-input series of router IP addresses.
- Uses the GetOctet function to focus the third octet of the current router IP address.
- Uses the SetOctet function to create a new IP address as a value for @ipnew.
- Creates a CLI { } command that will execute Allow operations for each of the selected routers.

The result is a set of Allow commands that open access in the ACL so that the router 10.1.1.1 can send OUT traffic via UDP on port 2055 to 10.1.4.1, 10.1.6.1, and 10.1.10.1.

Here are the parameters for this config change template. The template user selects the router on which to make ACL changes and inputs the target router IP address through this template:

```
.PARAMETER_LABEL @ACLRouter
    Router for ACL Change
.PARAMETER_DESCRIPTION @ACLRouters
    Select a Router
.PARAMETER_LABEL @ipRouters
    Target Routers
.PARAMETER_DESCRIPTION @ipRouters
    Add Routers to Target with ACL Allowances
```
Additional Examples of Working with Configuration Change Templates

For more information:

Enable NetFlow on CiscoASA  
Understanding Config Change Template Details.

Enable NetFlow on CiscoASA

A config change template named *Enable NetFlow on CiscoASA* installs with SolarWinds NCM. It configures a CiscoASA for NetFlow export.

Here are the commands that this template executes on the command line of the targeted devices selected in the template's run-time setup wizard. For this example, we are including values as if the user entered them in the wizard interface.

```
configure terminal
flow-export destination inside 10.10.18.157 2055
flow-export template timeout-rate 1
flow-export delay flow-create 60
logging flow-export syslogs disable
access-list netflow-export extended permit ip any
class-map netflow-export-class
match access-list netflow-export
policy-map netflow-policy
class netflow-export-class
flow-export event-type all destination 10.10.18.157
service-policy netflow-policy global
flow-export enable
exit
end
```

You could execute this set of CLI commands on your target device and the result would be config changes in the status of NetFlow data processing by the device.

The config change template that produces this output of CLI commands is:

```
/*
.CHANGE_TEMPLATE_DESCRIPTION
   This change template configures your Cisco ASA for
```
Enable NetFlow on CiscoASA

NetFlow export. This was verified on an ASA 5505 running ASA software version 8.2(1)12.

.CHANGE_TEMPLATE_TAGS
Cisco, ASA, NetFlow

.PLATFORM_DESCRIPTION
Cisco ASA

.PARAMETER_LABEL @ContextNode
NCM Node

.PARAMETER_DESCRIPTION @ContextNode
The node the template will operate on. All templates require this by default. The target node is selected during the first part of the wizard so it will not be available for selection when defining values of variables.

.PARAMETER_LABEL @NetFlowCollectorIPAddress
NetFlow Collector IP Address

.PARAMETER_DESCRIPTION @NetFlowCollectorIPAddress
Enter the IP address of the server running the NetFlow traffic analysis solution (e.g. SolarWinds NetFlow Traffic Analyzer—NTA).

.PARAMETER_LABEL @NetFlowExportPort
NetFlow Export Port

.PARAMETER_DESCRIPTION @NetFlowExportPort
Enter the NetFlow export port (default for SolarWinds NTA is 2055).

/*

script EnableNetflowOnCiscoASA ( 
    NCM.Nodes @ContextNode, 
    string @NetFlowCollectorIPAddress, 
    int @NetFlowExportPort 
) 
{
    // Enter configuration mode and generate NetFlow commands
    CLI
    {

```
configure terminal
flow-export destination inside @NetFlowCollectorIPAddress
flow-export template timeout-rate 1
flow-export delay flow-create 60
logging flow-export-syslogs disable
access-list netflow-export extended permit ip any any
class-map netflow-export-class
match access-list netflow-export
policy-map netflow-policy
class netflow-export-class
flow-export event-type all destination @NetFlowCollectorIPAddress
service-policy netflow-policy global
flow-export enable
exit
}
}

Parameters

The parameters defined at the beginning of this script create an interface in which the user types the IP address and port of the NetFlow receiver.

.PARAMETER_LABEL @NetFlowCollectorIPAddress
NetFlow Collector IP Address
.PARAMETER_DESCRIPTION @NetFlowCollectorIPAddress
Enter the IP address of the server running the NetFlow traffic analysis solution (e.g. SolarWinds NetFlow Traffic Analyzer--NTA).

.PARAMETER_LABEL @NetFlowExportPort
NetFlow Export Port
.PARAMETER_DESCRIPTION @NetFlowExportPort
Enter the NetFlow export port (default for SolarWinds NTA is 2055).
The first line defines the parameter or variable name (in this case, @NetFlowCollectorIPAddress) for which the user enters a value in the wizard interface text box at run time. The second line defines the label (in this case, NetFlow Collector IP Address) that appears in the wizard interface to prompt the user to enter the appropriate IP address. The third and fourth lines define the description that appears below the wizard interface text box.

The parameters for NetFlow Export Port (in lines 5-12) function exactly the same way as the first four. The parameter variables, labels, and descriptions guide the config change template's run-time execution by receiving specific user input.

**Command Declarations (script)**

The script declarations include all the variables for which the template prompts the user to provide input. In this case, three variables and their data types are declared:

```plaintext
script EnableNetflowOnCiscoASA (  
    NCM.Nodes @ContextNode,  
    string @NetFlowCollectorIPAddress,  
    int @NetFlowExportPort  
)  
{
...
}
```

NCM.Nodes is applied to the @ContextNode variable. NCM.Nodes refers to the Nodes entity in the SolarWinds Information Service (SWIS). In the interface wizard, the user enters a string value for the NetFlow Collector IP Address and an integer value for the NetFlow Export Port on the device.

For a complete list of entities and properties, see [SolarWinds Information Services Data Entities](#).

**CLI Commands**

The majority of config change template code outputs original CLI commands with only a few parsed variables. Any time a variable is referenced, a value is used in its place. For example, since the user typed 10.10.18.157 as the IP address and 2055 as the collector port number, NetFlowCollectorIPAddress is replaced with 10.10.18.157 and @NetFlowExportPort is replaced with 2055 when the script runs.

`flow-export destination inside @NetFlowCollectorIPAddress @NetFlowExportPort`
Chapter 8: Working with Config Change Templates

The previous line of code generates the following output:

flow-export destination inside 10.10.18.157 2055

Executing a Config Change Template

1. From the web console, click **CONFIGS > Config Change Templates**.
2. Select a template in list.
3. **If you want to edit the template**, click **Advanced Modify**.
4. Click **Define Variables & Run**.
5. Select the target nodes. Use the **Group by** control if necessary.
6. Click **Next**.
7. Enter the appropriate values in the input fields.
   - Input fields for a change configuration template are defined and managed through the Edit Config Template resource. For example, in a template that enables NetFlow data exporting for a set of Cisco devices, you may be asked to enter the IP address of the relevant NetFlow collector and the port on which your target device exports flow data.
8. Click **Next**.
9. **If you want to see the CLI commands for a device**, click **Show commands in new window**.
10. Click **Execute**.

Creating a Config Change Template

1. From the web console, click **CONFIGS > Config Change Templates**.
2. Click **Create New Config Change Template**.
3. Name the template, enter a description, and then add tags.
4. Create your Config Change Template.
   - As needed, consult [Config Change Template Basics](#), [Advanced Commands](#), and [Understanding Config Change Template Details](#).
5. Click **Validate** to check syntax.
6. Click **Submit** to save the template or **Execute** to save and run it.
   
   If you choose the execute the template, NCM validates the syntax of the template. If validation succeeds, NCM saves a copy of the template and loads the relevant interface for user input.
   
   If validation fails, NCM displays an error that guides you to make changes.

### Importing a Config Change Template

1. From the web console, click **CONFIGS > Config Change Templates**.
2. Click **Import**.
3. Click **Choose File** to find the file on your computer. Config change template files have the extension `.ncm-template`.
4. Click **Submit**.
5. Change the name, edit the description, and then add tags, if necessary.
6. Modify the logic of your Config Change Template.
   
   As needed, consult [Config Change Template Basics](#), [Advanced Commands](#), and [Understanding Config Change Template Details](#).
7. Click **Validate** to check syntax.
8. Click **Submit**.

### Editing a Config Change Template

1. From the web console, click **CONFIGS > Config Change Templates**.
2. Select a template in the list.
3. Click **Advanced Modify**.
   
   As needed, consult [Config Change Template Basics](#), [Advanced Commands](#), and [Understanding Config Change Template Details](#).
4. Change the name, edit the description, and then add tags, if necessary.
5. Modify the logic of your Config Change Template.
6. Click **Validate** to check syntax.
7. Click **Submit**.
Chapter 8: Working with Config Change Templates

Tagging a Config Change Template

Adding Tags

1. From the web console, click CONFIGS > Config Change Templates.
2. Select a template in the list.
3. Click Tags.
4. Add tags.
   - *If you want to add an existing tag*, select a tag in the list.
   - *If you want to add a new tag*, click Add new tag(s), and then type your tags separated by commas.
5. Click Submit.

Removing Tags

1. From the web console, click CONFIGS > Config Change Templates.
2. Select a template in the list.
3. Click Tags.
4. Click Remote tag(s).
5. Select one or more tags.
6. Click Submit.

Exporting a Config Change Template (to thwack)

1. From the web console, click CONFIGS > Config Change Templates.
2. Select a template in list.
3. Click Export to thwack.
4. If prompted, enter your user name and password, and then click Log In.

Exporting a Config Change Template (as a file)

1. From the web console, click CONFIGS > Config Change Templates.
2. Select a template in the list.
3. Click **Export as File**. Verify that a pop-up blocker does not prevent the file from being downloaded.

4. Download the file to a local folder.

5. **If you are finished**, click **Return to Config Change Templates**.

6. **If you want to upload the template to thwack.com**, click **Share Now**.

7. Under the Actions area, click **Content Exchange Upload**.

8. Click **Select a File** and browse to it on your local computer.

9. Click **Save**.

10. Enter a title and description.

11. Select or enter tags.

12. Click **Publish**.

**Deleting a Config Change Template**

1. From the web console, click **CONFIGS > Config Change Templates**.

2. Select a template in the list.

3. Click **Delete**.

**SolarWinds Information Services Data Entities**

The following tables document all the SWIS entities and properties that you can use in developing config change templates.

**NCM.ArpTables**

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InterfaceIndex</td>
<td>System.Int32</td>
<td>The interface on which this entry’s equivalence is effective. The interface identified by a particular value of this index is the same interface as identified by the same value of RFC 1573’s ifIndex.</td>
</tr>
</tbody>
</table>
## Chapter 8: Working with Config Change Templates

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InterfaceID</td>
<td>System.String</td>
<td>A unique GUID ID from ncm.Interfaces table.</td>
</tr>
<tr>
<td>MAC</td>
<td>System.String</td>
<td>The media dependent `physical' address.</td>
</tr>
<tr>
<td>IPAddress</td>
<td>System.String</td>
<td>The IP address corresponding to the media dependent physical address.</td>
</tr>
<tr>
<td>IPSort</td>
<td>System.Double</td>
<td>A list of IP addresses sorted with octet markers (dots) omitted.</td>
</tr>
<tr>
<td>Source</td>
<td>System.String</td>
<td>The type of IP address associated with an ARP operation and media dependent address.</td>
</tr>
</tbody>
</table>

Possible Values:
- Other (1)
- Invalid (2)
- Dynamic (3)
- Static (4)
Setting this object to the value invalid (2) has the effect of invalidating the corresponding entry in the ipNetToMediaTable. That is, it effectively disassociates the interface identified with said entry from the mapping identified with said entry. It is an implementation specific matter as to whether the agent removes an Invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant ipNetToMediaType object.

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDNSLookup</td>
<td>System.String</td>
<td>Result of DNS lookup on IPAddress.</td>
</tr>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of interfaces for which ARP data is reported.)</td>
</tr>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM first discovered the device during inventory.</td>
</tr>
</tbody>
</table>

**NCM.ARPTables Entity Relationships**

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsArpTables (System.Hosting)</td>
</tr>
</tbody>
</table>
# NCM.BridgePorts

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InterfaceIndex</td>
<td>System.Int32</td>
<td>The value of the instance of the ifIndex object, defined in MIB-II, for the interface corresponding to this port.</td>
</tr>
<tr>
<td>Port</td>
<td>System.Int32</td>
<td>The port number of the port for which this entry contains bridge management information.</td>
</tr>
<tr>
<td>SpanningTreeEnabled</td>
<td>System.String</td>
<td>The enabled/disabled status of the port. Possible Values: Enabled (1) Disabled (2)</td>
</tr>
<tr>
<td>SpanningTreeState</td>
<td>System.String</td>
<td>The port's current state as defined by application of the Spanning Tree Protocol. This state controls what action a port takes on reception of a frame. If the bridge has detected a port that is malfunctioning it will place that port into the broken (6) state. For ports which are disabled (see dot1dStpPortEnable), this object will have a value of disabled (1).</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VlanType</td>
<td>System.String</td>
<td>The type of VLAN membership assigned to this port. A port with static VLAN membership is assigned to a single VLAN directly. A port with dynamic membership is assigned a single VLAN based on content of packets received on the port and through VQP queries to VMPS. A port with multiple VLAN membership may be assigned to one or more VLANs directly. A static or dynamic port membership is specified by the value of vmVlan. A multiVlan port membership is specified by the value of vmVlans. Possible Values: Static(1) Dynamic(2) MultiVlan(3)</td>
</tr>
<tr>
<td>VLANID</td>
<td>System.Int32</td>
<td>The VLAN id of the VLAN the port is assigned to when vmVlanType is set to static or dynamic. This object is not instantiated if not applicable. The value may be 0 if the port is not assigned to a VLAN.</td>
</tr>
</tbody>
</table>
### Chapter 8: Working with Config Change Templates

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
</table>
| PortStatus    | System.String| An indication of the current VLAN status of the port. A status of inactive(1) indicates that a dynamic port does not yet have a VLAN assigned, or a port is assigned to a VLAN that is currently not active. A status of active(2) indicates that the currently assigned VLAN is active. A status of shutdown(3) indicates that the port has been disabled as a result of VQP shutdown response.  
Possible Values: inactive(1) active(2) shutdown(3) |
| NodeID        | System.String| A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of interfaces for which bridge port data is reported.) |
| LastDiscovery | System.DateTime| A SWIS-generated date and time marker for when NCM last discovered the device during inventory.                                           |
| FirstDiscovery| System.DateTime| A SWIS-generated date and time marker for when NCM first discovered the device during inventory.                                         |
### NCM.BridgePorts Entity Relationships

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsBridgePorts (System.Hosting)</td>
</tr>
</tbody>
</table>

### NCM.CatalystCards

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CardIndex</td>
<td>System.Int32</td>
<td>A unique value for each module within the chassis.</td>
</tr>
<tr>
<td>CardType</td>
<td>System.Int32</td>
<td>The type of module.</td>
</tr>
</tbody>
</table>

**Possible Values:**
- (notdefined(0), version1(1), version2(2), version3(3), version4(4), version5(5), version6(6), version7(7), version8(8), version9(9), version10(10), vi2(11), vi4(12), vi30(13), s1b(14), sa2(15), as16(16), new8as(17), Isa(18), fxs2(19), fxo2(20), em2(21), fxs4(22), fxo4(23), em4(24), sab(25), e1vi(26), am12(27), am6(28), ndec(29), newsa2(30), aux(31), console(32), sic-wan(33), sic-1fe(34), sic-1sa(35), sic-3as(36), sic-1e1(37), sic-1t1(38), sic-1bu(39), sic-2bu(40), sic-1bs(41), sic-2bs(42), sic-1am(43), sic-2am(44), sic-1em(45), sic-2em(46), sic-1fxs(47), sic-2fxs(48), sic-1fxo(49), sic-2fxo(50), fcm6(51), sa8(52),...}
## Chapter 8: Working with Config Change Templates

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
</table>
| t11(53), t12(54), t14(55), t1vi(56), fcm4(57), fcm2(58), rtb21ce3(59), ame6(60), ame12(61), wsx5162(62), e11-f(65), e12-f(66), e14-f(67), t11-f(68), t12-f(69), t14-f(70), e11-f-17(71), t11-f-17(72), rtb21ct3(73), atmads1(74), atmads2(75), atm155m(76), ase8(77), ase16(78), sae4(79), sae2(80), wsx5012a(81), wsx5167(82), wsx5239(83), wsx5168(84), wsx5305(85), wsx5550(87), wsf5541(88), atmshds1(90), atmshds2(91), atmshds4(92), atm25m(93), atme3(94), atm3(95), xdsl-fec(96), xdsl-adsl(97), xdsl-gshdsl(98), xdsl-bri(99), xdsl-scc(100), ge1(101), pos155m(102), cpos(103), fe1op(104), sae8(105), atm155m-mm(106), atm155m-sm(107), atm155m-sml(108), fe1op-sfx(109), fe1op-mfx(110), cpos-t1(111), ge1-op(112), ge2-op(113), ge2(114), fix-1wan(115), fix-1sae(116), cavium(117), sic-1Eth(118), atm1ADSLI(119), atm2ADSLI(120), fix-e11(121), fix-t11(122), e18-75(123), e18-120(124), t18(125), sic-1vifxs(126), sic-1vifxo(127), sic-2vifxs(128), sic-2vifxo(129), xdsl-fec-new(130), xdsl-sa(131), bs4(132), ima-8e175(133), ima-8e1120(134), ima-4e175(135), ima-4e1120(136), ima-8t1(137), ima-4t1(138), sic-1t1f(139), sic-1e1f(140), fe4(149), }
<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>t1vi2</td>
<td></td>
<td>(227)</td>
</tr>
<tr>
<td>osm</td>
<td></td>
<td>(229)</td>
</tr>
<tr>
<td>sd707</td>
<td></td>
<td>(230)</td>
</tr>
<tr>
<td>dm-epri</td>
<td></td>
<td>(231)</td>
</tr>
<tr>
<td>dm-tpri</td>
<td></td>
<td>(232)</td>
</tr>
<tr>
<td>erpu-h</td>
<td></td>
<td>(233)</td>
</tr>
<tr>
<td>wsf6kmsfc2</td>
<td></td>
<td>(234)</td>
</tr>
<tr>
<td>wsx6324mmmt</td>
<td></td>
<td>(235)</td>
</tr>
<tr>
<td>wsx6348rj45</td>
<td></td>
<td>(236)</td>
</tr>
<tr>
<td>wsx6ksup22ge</td>
<td></td>
<td>(237)</td>
</tr>
<tr>
<td>wsx6324sm</td>
<td></td>
<td>(238)</td>
</tr>
<tr>
<td>wsx6516gbic</td>
<td></td>
<td>(239)</td>
</tr>
<tr>
<td>osm4geWanGbic</td>
<td></td>
<td>(240)</td>
</tr>
<tr>
<td>osm1oc48PosSS</td>
<td></td>
<td>(241)</td>
</tr>
<tr>
<td>osm1oc48PosSI</td>
<td></td>
<td>(242)</td>
</tr>
<tr>
<td>osm1oc48PosSL</td>
<td></td>
<td>(243)</td>
</tr>
<tr>
<td>wsx6381ids</td>
<td></td>
<td>(244)</td>
</tr>
<tr>
<td>wsc6500sfm</td>
<td></td>
<td>(245)</td>
</tr>
<tr>
<td>osm16oc3PosMM</td>
<td></td>
<td>(246)</td>
</tr>
<tr>
<td>osm16oc3PosSI</td>
<td></td>
<td>(247)</td>
</tr>
<tr>
<td>osm16oc3PosSL</td>
<td></td>
<td>(248)</td>
</tr>
<tr>
<td>osm2oc12PosMM</td>
<td></td>
<td>(249)</td>
</tr>
<tr>
<td>osm2oc12PosSL</td>
<td></td>
<td>(250)</td>
</tr>
<tr>
<td>osm2oc12PosSL</td>
<td></td>
<td>(251)</td>
</tr>
<tr>
<td>wsx650210ge</td>
<td></td>
<td>(252)</td>
</tr>
<tr>
<td>osm8oc3PosMM</td>
<td></td>
<td>(253)</td>
</tr>
<tr>
<td>osm8oc3PosSI</td>
<td></td>
<td>(254)</td>
</tr>
<tr>
<td>osm8oc3PosSL</td>
<td></td>
<td>(255)</td>
</tr>
<tr>
<td>wsx6548rj45</td>
<td></td>
<td>(258)</td>
</tr>
<tr>
<td>wsx6524mmmt</td>
<td></td>
<td>(259)</td>
</tr>
<tr>
<td>wsx6066SlbApc</td>
<td></td>
<td>(260)</td>
</tr>
<tr>
<td>wsx6516getx</td>
<td></td>
<td>(261)</td>
</tr>
<tr>
<td>osm2oc48OneDptSS</td>
<td></td>
<td>(265)</td>
</tr>
<tr>
<td>osm2oc48OneDptSI</td>
<td></td>
<td>(266)</td>
</tr>
<tr>
<td>osm2oc48OneDptSL</td>
<td></td>
<td>(267)</td>
</tr>
<tr>
<td>osm2oc48OneDptSSDual</td>
<td></td>
<td>(268)</td>
</tr>
<tr>
<td>osm2oc48OneDptSIDual</td>
<td></td>
<td>(269)</td>
</tr>
<tr>
<td>osm2oc48OneDptSLDual</td>
<td></td>
<td>(270)</td>
</tr>
<tr>
<td>wsx6816gbic</td>
<td></td>
<td>(271)</td>
</tr>
<tr>
<td>osm4choc12T3MM</td>
<td></td>
<td>(272)</td>
</tr>
<tr>
<td>osm4choc12T3SI</td>
<td></td>
<td>(273)</td>
</tr>
<tr>
<td>osm8choc12T3MM</td>
<td></td>
<td>(274)</td>
</tr>
<tr>
<td>osm8choc12T3SI</td>
<td></td>
<td>(275)</td>
</tr>
<tr>
<td>osm1choc48T3SS</td>
<td></td>
<td>(276)</td>
</tr>
<tr>
<td>osm2choc48T3SS</td>
<td></td>
<td>(277)</td>
</tr>
<tr>
<td>wsx6500sfm2</td>
<td></td>
<td>(278)</td>
</tr>
<tr>
<td>osm1choc48T3SI</td>
<td></td>
<td>(279)</td>
</tr>
<tr>
<td>osm2choc48T3SI</td>
<td></td>
<td>(280)</td>
</tr>
<tr>
<td>wsx6348rj21</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 8: Working with Config Change Templates

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CardName</td>
<td>System.String</td>
<td>A descriptive string used by the network administrator to name the module.</td>
</tr>
<tr>
<td>ModuleModel</td>
<td>System.String</td>
<td>The manufacturer's model number for the module.</td>
</tr>
<tr>
<td>CardSerial</td>
<td>System.String</td>
<td>The serial number of the module. This MIB object will return the module serial number for any module that either a numeric or an alphanumeric serial number is being used.</td>
</tr>
<tr>
<td>HWVersion</td>
<td>System.String</td>
<td>The hardware version of the module.</td>
</tr>
<tr>
<td>FWVersion</td>
<td>System.String</td>
<td>The firmware version of the module.</td>
</tr>
<tr>
<td>SWVersion</td>
<td>System.String</td>
<td>The software version of the module.</td>
</tr>
<tr>
<td>Slot</td>
<td>System.Int32</td>
<td>This value is determined by the chassis slot number where the module is located. Valid entries are 1 to the value of chassisNumSlots.</td>
</tr>
<tr>
<td>Parent</td>
<td>System.Int32</td>
<td>The value of the instance of the entPhysicalIndex object, defined in ENTITY-MIB, for the entity physical index corresponding to this module.</td>
</tr>
</tbody>
</table>
### Property Description Table

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OperStatus</td>
<td>System.String</td>
<td>The operational status of the module. If the status is not ok, the value of moduleTestResult gives more detailed information about the module's failure condition(s). Possible Values: other(1) ok(2) minorFault(3) majorFault(4)</td>
</tr>
<tr>
<td>SlotsOnCard</td>
<td>System.Int32</td>
<td>The number of ports supported by the module.</td>
</tr>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of interfaces for which card data is reported.)</td>
</tr>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM first discovered the device during inventory.</td>
</tr>
</tbody>
</table>

### NCM.CatalystCards Entity Relationships

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsCatalystCards (System.Hosting)</td>
</tr>
</tbody>
</table>
**Chapter 8: Working with Config Change Templates**

**NCM.CiscoCards**

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CardIndex</td>
<td>System.Int32</td>
<td>Index into cardTable (not physical chassis slot number).</td>
</tr>
<tr>
<td>CardType</td>
<td>System.Int32</td>
<td>Functional type of this card. (integer value)</td>
</tr>
<tr>
<td>CardName</td>
<td>System.String</td>
<td>Functional type of this card. (Parsed from type name value).</td>
</tr>
<tr>
<td>CardDescr</td>
<td>System.String</td>
<td>Text description of this card.</td>
</tr>
<tr>
<td>CardSerial</td>
<td>System.String</td>
<td>The serial number of this card, or zero if unavailable.</td>
</tr>
<tr>
<td>HWVersion</td>
<td>System.String</td>
<td>Hardware revision level of this card, or an empty string if unavailable.</td>
</tr>
<tr>
<td>SWVersion</td>
<td>System.String</td>
<td>Version of the firmware or microcode installed on this card, or an empty string if unavailable.</td>
</tr>
<tr>
<td>Slot</td>
<td>System.Int32</td>
<td>Number of slots on this card, or 0 if no slots or not applicable, or -1 if not determinable.</td>
</tr>
<tr>
<td>Parent</td>
<td>System.Int32</td>
<td>CardIndex of the parent card which directly contains this card, or 0 if contained by the chassis, or -1 if not applicable nor determinable.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| OperStatus    | System.String| The operational status of the card.  
cardOperStatus is up when a card is recognized by the device and is enabled for operation. cardOperStatus is down if the card is not recognized by the device, or if it is not enabled for operation. cardOperStatus is standby if the card is enabled and acting as a standby slave.  
Possible Values:  
not-specified(1)  
up (2)  
down (3)  
standby (4)  
standbyMaster (5)  
activeMaster (6)  
outOfService (7)  
masterBooting(8)  
activeMasterBooting(9)  
standbyMasterBooting(10)  
slaveBooting(11) |
| SlotsOnCard   | System.Int32 | Number of slots on this card, or 0 if no slots or not applicable, or -1 if not determinable                                           |
| NodeID        | System.String| A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of interfaces for which card data is reported.) |
Chapter 8: Working with Config Change Templates

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM first discovered the device during inventory.</td>
</tr>
</tbody>
</table>

**NCM.CiscoCards Entity Relationships**

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsCiscoCards (System.Hosting)</td>
</tr>
</tbody>
</table>

**NCM.CiscoCdp**

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifIndex</td>
<td>System.Int32</td>
<td>An indication of the type of address contained in the corresponding instance of cdpCacheAddress (parse just ifIndex from value for example 1,2,3)</td>
</tr>
<tr>
<td>CDPIndex</td>
<td>System.String</td>
<td>An indication of the type of address contained in the corresponding instance of cdpCacheAddress (full value. For example 1.6, 2.108, 2.3</td>
</tr>
<tr>
<td>RemoteDevice</td>
<td>System.String</td>
<td>The Device-ID string as reported in the most recent CDP message. The zero-length string indicates no Device-ID field (TLV) was reported in the most recent CDP message.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RemoteIPAddress</td>
<td>System.String</td>
<td>The (first) network-layer address of the device's SNMP-agent as reported in the most recent CDP message. For example, if the corresponding instance of cacheAddressType had the value 'ip(1)', then this object would be an IP address.</td>
</tr>
<tr>
<td>RemoteVersion</td>
<td>System.String</td>
<td>The Version string as reported in the most recent CDP message. The zero-length string indicates no Version field (TLV) was reported in the most recent CDP message.</td>
</tr>
<tr>
<td>RemotePort</td>
<td>System.String</td>
<td>The Port-ID string as reported in the most recent CDP message. This will typically be the value of the ifName object (e.g., 'Ethernet0'). The zero-length string indicates no Port-ID field (TLV) was reported in the most recent CDP message.</td>
</tr>
<tr>
<td>RemoteCapability</td>
<td>System.String</td>
<td>The Device's Functional Capabilities as reported in the most recent CDP message. For latest set of specific values, see the latest version of the CDP specification. The zero-length string indicates no Capabilities field (TLV) was reported in the most recent CDP message.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RemotePlatform</td>
<td>System.String</td>
<td>The Device's Hardware Platform as reported in the most recent CDP message. The zero-length string indicates that no Platform field (TLV) was reported in the most recent CDP message.</td>
</tr>
<tr>
<td>RemoteDuplex</td>
<td>System.String</td>
<td>The remote device's interface's duplex mode, as reported in the most recent CDP message. The value unknown(1) indicates no duplex mode field (TLV) was reported in the most recent CDP message. Possible Values: unknown(1) halfduplex(2) fullduplex(3)</td>
</tr>
<tr>
<td>RemoteNativeVLAN</td>
<td>System.Int32</td>
<td>The remote device's interface's native VLAN, as reported in the most recent CDP message. The value 0 indicates no native VLAN field (TLV) was reported in the most recent CDP message</td>
</tr>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of remote devices for which remote device data is reported.)</td>
</tr>
</tbody>
</table>
### NCM.CiscoCdp Entity Relationships

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM first discovered the device during inventory.</td>
</tr>
</tbody>
</table>

### NCM.CiscoCdp Entity Relationships

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsCiscoCdp (System.Hosting)</td>
</tr>
</tbody>
</table>

### NCM.CiscoChassis

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chassisType</td>
<td>System.Int32</td>
<td>Chassis type (integer value). Possible Values: unknown(1) multibus(2) agsplus(3)</td>
</tr>
<tr>
<td>chassisName</td>
<td>System.String</td>
<td>Chassis type (parsed string value). Possible Values: unknown(1) multibus(2) agsplus(3)</td>
</tr>
</tbody>
</table>
## Property Name | Datatype | Description
--- | --- | ---
chassisVersion | System.String | Chassis hardware revision level, or an empty string if unavailable.
chassisID | System.String | Unique ID string. Defaults to chassis serial number if available, otherwise empty. Can also be set with 'snmp-server chassis-id'.
chassisSerialNumberString | System.String | The serial number of the chassis. This MIB object will return the chassis serial number for any chassis that either a numeric or an alphanumeric serial number is being used.
romSysVersion | System.String | ROM system software version or an empty string if unavailable.
processorRAM | System.Int32 | Bytes of RAM available to CPU.
nvRAMSize | System.Int32 | Bytes of nonvolatile configuration memory.
nvRAMUsed | System.Int32 | Bytes of non-volatile configuration memory in use.
chassisSlots | System.Int32 | Number of slots in this chassis, or -1 of neither applicable nor determinable.
<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>romID</td>
<td>System.String</td>
<td>This variable contains a printable octet string which contains the System Bootstrap description and version identification.</td>
</tr>
<tr>
<td>whyReload</td>
<td>System.String</td>
<td>This variable contains a printable octet string which contains the reason why the system was last restarted.</td>
</tr>
<tr>
<td>freeMem</td>
<td>System.Int32</td>
<td>Return the amount of free memory in bytes. Note: This MIB object is obsolete as of IOS release 11.1. IOS release 11.1 introduced the CISCO-MEMORY-POOL-MIB which better instruments all of the memory pools.</td>
</tr>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of nodes for which data is reported.)</td>
</tr>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM last discovered the device during inventory.</td>
</tr>
</tbody>
</table>
Chapter 8: Working with Config Change Templates

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM first discovered the device during inventory.</td>
</tr>
</tbody>
</table>

**NCM.CiscoChassis Entity Relationships**

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsCiscoChassis (System.Hosting)</td>
</tr>
</tbody>
</table>

**NCM.CiscoFlash**

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FlashSize</td>
<td>System.Int32</td>
<td>Total size of the Flash device. For a removable device, the size will be zero if the device has been removed.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name</td>
<td>System.String</td>
<td>Flash device name. This name is used to refer to the device within the system. Flash operations get directed to a device based on this name. The system has a concept of a default device. This would be the primary or most used device in case of multiple devices. The system directs an operation to the default device whenever a device name is not specified. The device name is therefore mandatory except when the operation is being done on the default device, or the system supports only a single Flash device. The device name will always be available for a removable device, even when the device has been removed.</td>
</tr>
</tbody>
</table>
Chapter 8: Working with Config Change Templates

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FlashDescription</td>
<td>System.String</td>
<td>Description of a Flash device. The description is meant to explain what the Flash device and its purpose is. Current values are: System flash - for the primary Flash used to store full system images. Boot flash: for the secondary Flash used to store bootstrap images. The ciscoFlashDeviceDescr, CiscoFlashDeviceController (if applicable), and ciscoFlashPhyEntIndex objects are expected to collectively give all information about a Flash device. The device description will always be available for a removable device, even when the device has been removed.</td>
</tr>
<tr>
<td>PartitionCount</td>
<td>System.Int32</td>
<td>Flash device partitions actually present. Number of partitions cannot exceed the minimum of ciscoFlashDeviceMaxPartitions and (ciscoFlashDeviceSize / ciscoFlashDeviceMinPartitionSize). Will be equal to at least 1, the case where the partition spans the entire device (actually no partitioning). A partition will contain one or more minimum partition units (where a minimum partition unit is defined by ciscoFlashDeviceMinPartitionSize).</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MinPartitionSize</td>
<td>System.Int32</td>
<td>This object will give the minimum partition size supported for this device. For systems that execute code directly out of Flash, the minimum partition size needs to be the bank size. (Bank size is equal to the size of a chip multiplied by the width of the device. In most cases, the device width is 4 bytes, and so the bank size would be four times the size of a chip). This has to be so because all programming commands affect the operation of an entire chip (in our case, an entire bank because all operations are done on the entire width of the device) even though the actual command may be localized to a small portion of each chip. So when executing code out of Flash, one needs to be able to write and erase some portion of Flash without affecting the code execution. For systems that execute code out of DRAM or ROM, it is possible to partition Flash with a finer granularity (for eg., at erase sector boundaries) if the system code supports such granularity. This object will let a management entity know the minimum partition size as defined by the system. If the system does not support partitioning, the value will be equal to the device size in ciscoFlashDeviceSize. The maximum number of partitions that could be configured will be equal to the minimum of ciscoFlashDeviceMaxPartitions and (ciscoFlashDeviceSize / CiscoFlashDeviceMinPartitionSize)</td>
</tr>
</tbody>
</table>
Chapter 8: Working with Config Change Templates

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller</td>
<td>System.String</td>
<td>Flash device controller. The h/w card that actually controls Flash read/write/erase. Relevant for the AGS+ systems where Flash may be controlled by the MC+, STR or the ENVM cards, cards that may not actually contain the Flash chips. For systems that have removable PCMCIA flash cards that are controlled by a PCMCIA controller chip, this object may contain a description of that controller chip. Where irrelevant (Flash is a direct memory mapped device accessed directly by the main processor), this object will have an empty (NULL) string.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WriteProtectJumper</td>
<td>System.String</td>
<td>This object gives the state of a jumper (if present and can be determined) that controls the programming voltage called Vpp to the Flash device. Vpp is required for programming (erasing and writing) Flash. For certain older technology chips it is also required for identifying the chips (which in turn is required to identify which programming algorithms to use; different chips require different algorithms and commands). The purpose of the jumper, on systems where it is available, is to write protect a Flash device. On most of the newer remote access routers, this jumper is unavailable since users are not expected to visit remote sites just to install and remove the jumpers when upgrading software in the Flash device. The unknown(3) value will be returned for such systems and can be interpreted to mean that a programming jumper is not present or not required on those systems. On systems where the programming jumper state can be read back through a hardware register, the installed (1) or notInstalled (2) value will be returned. This object is expected to be used in conjunction with the ciscoFlashPartitionStatus object whenever that object has the readOnly(1) value. In such a case, this object will indicate whether the programming jumper is a possible reason for the readOnly state. Possible Values: installed(1) notInstalled(2) unknown(3)</td>
</tr>
</tbody>
</table>
**Chapter 8: Working with Config Change Templates**

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxPartitions</td>
<td>System.Int32</td>
<td>Max number of partitions supported by the system for this Flash device. Default will be 1, which actually means that partitioning is not supported. Note that this value will be defined by system limitations, not by the flash device itself (for eg., the system may impose a limit of 2 partitions even though the device may be large enough to be partitioned into 4 based on the smallest partition unit supported). On systems that execute code out of Flash, partitioning is a way of creating multiple file systems in the Flash device so that writing into or erasing of one file system can be done while executing code residing in another file system. For systems executing code out of DRAM, partitioning gives a way of subdividing a large Flash device for easier management of files.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Initialized</td>
<td>System.DateTime</td>
<td>System time at which device was initialized. For fixed devices, this will be the system time at boot up. For removable devices, it will be the time at which the device was inserted, which may be boot up time, or a later time (if device was inserted later). If a device (fixed or removable) was repartitioned, it will be the time of repartitioning. The purpose of this object is to help a management station determine if a removable device has been changed. The application should retrieve this object prior to any operation and compare with the previously retrieved value. Note that this time will not be real time but a running time maintained by the system. This running time starts from zero when the system boots up. For a removable device that has been removed, this value will be zero.</td>
</tr>
</tbody>
</table>
### Chapter 8: Working with Config Change Templates

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removable</td>
<td>System.String</td>
<td>Whether Flash device is removable. Generally, only PCMCIA Flash cards will be treated as removable. Socketed Flash chips and Flash SIMM modules will not be treated as removable. Simply put, only those Flash devices that can be inserted or removed without opening the hardware casing will be considered removable. Further, removable Flash devices are expected to have the necessary hardware support: 1) online removal and insertion; 2) interrupt generation on removal or insertion.</td>
</tr>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)</td>
</tr>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM first discovered the device during inventory.</td>
</tr>
</tbody>
</table>
NCM.CiscoFlash Entity Relationships

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsCiscoFlash (System.Hosting)</td>
</tr>
</tbody>
</table>

NCM.CiscoFlashFiles

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FlashFileName</td>
<td>System.String</td>
<td>Flash file name as specified by the user copying in the file. The name should not include the colon (:) character as it is a special separator character used to delineate the device name, partition name, and the file name.</td>
</tr>
<tr>
<td>FlashFileSize</td>
<td>System.Int32</td>
<td>Size of the file in bytes. Note that this size does not include the size of the filesystem file header. File size will always be non-zero.</td>
</tr>
<tr>
<td>FlashCheckSum</td>
<td>System.String</td>
<td>File checksum stored in the file header. This checksum is computed and stored when the file is written into Flash. It serves to validate the data written into Flash. Whereas the system will generate and store the checksum internally in hexadecimal form, this object will provide the checksum in a string form. The checksum will be available for all valid and invalid-checksum files.</td>
</tr>
</tbody>
</table>
## Property Name | Datatype | Description
--- | --- | ---
FlashFileStatus | System.String | Status of a file. A file could be explicitly deleted if the file system supports such a user command facility. Alternately, an existing good file would be automatically deleted if another good file with the same name were copied in. Note that deleted files continue to occupy prime Flash real estate. A file is marked as having an invalid checksum if any checksum mismatch was detected while writing or reading the file. Incomplete files (files truncated either because of lack of free space or a network download failure) are also written with a bad checksum and marked as invalid. Possible Values: deleted(1) invalidChecksum(2) valid(3)
NodeID | System.String | A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)
LastDiscovery | System.DateTime | A SWIS-generated date and time marker for when NCM last discovered the device during inventory.
FirstDiscovery | System.DateTime | A SWIS-generated date and time marker for when NCM first discovered the device during inventory.
NCM.CiscoFlashFiles Entity Relationships

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsCiscoFlashFiles (System.Hosting)</td>
</tr>
</tbody>
</table>

NCM.CiscoImageMIB

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>System.String</td>
<td>The string of this entry.</td>
</tr>
<tr>
<td>Value</td>
<td>System.String</td>
<td>The string of this entry.</td>
</tr>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)</td>
</tr>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM first discovered the device during inventory.</td>
</tr>
</tbody>
</table>

NCM.CiscoImageMIB Entity Relationships

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsCiscoImageMIB (System.Hosting)</td>
</tr>
</tbody>
</table>
### NCM.CiscoMemoryPools

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoolName</td>
<td>System.String</td>
<td>A textual name assigned to the memory pool. This object is suitable for output to a human operator, and may also be used to distinguish among the various pool types, especially among dynamic pools.</td>
</tr>
<tr>
<td>PoolUsed</td>
<td>System.Int32</td>
<td>Indicates the number of bytes from the memory pool that are currently in use by applications on the managed device.</td>
</tr>
<tr>
<td>PoolFree</td>
<td>System.Int32</td>
<td>Indicates the number of bytes from the memory pool that are currently unused on the managed device. Note that the sum of ciscoMemoryPoolUsed and ciscoMemoryPoolFree is the total amount of memory in the pool</td>
</tr>
<tr>
<td>PoolLargestFree</td>
<td>System.Int32</td>
<td>Indicates the largest number of contiguous bytes from the memory pool that are currently unused on the managed device.</td>
</tr>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)</td>
</tr>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM first discovered the device during inventory.</td>
</tr>
</tbody>
</table>
### NCM.CiscoMemoryPools Entity Relationships

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsCiscoMemoryPools (System.Hosting)</td>
</tr>
</tbody>
</table>

### NCM.EntityLogical

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>System.String</td>
<td>A textual description of the logical entity. This object should contain a string which identifies the manufacturer's name for the logical entity, and should be set to a distinct value for each version of the logical entity.</td>
</tr>
<tr>
<td>TDomain</td>
<td>System.String</td>
<td>Indicates the kind of transport service by which the logical entity receives network management traffic. Possible values for this object are presently found in the Transport Mappings for SNMPv2 document (RFC 1906 [RFC1906]).</td>
</tr>
</tbody>
</table>
### Chapter 8: Working with Config Change Templates

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>System.String</td>
<td>An indication of the type of logical entity. This will typically be the OBJECT IDENTIFIER name of the node in the SMI's naming hierarchy which represents the major MIB module, or the majority of the MIB modules, supported by the logical entity. For example: a logical entity of a regular host/router &gt; mib-2 a logical entity of a 802.1d bridge -&gt; dot1dBridge a logical entity of a 802.3 repeater -&gt; snmpDot3RptrMgmt If an appropriate node in the SMI's naming hierarchy cannot be identified, the value 'mib-2' should be used.</td>
</tr>
<tr>
<td>Community</td>
<td>System.String</td>
<td>An SNMPv1 or SNMPv2C community-string which can be used to access detailed management information for this logical entity. The agent should allow read access with this community string (to an appropriate subset of all managed objects) and may also return a community string based on the privileges of the request used to read this object. Note that an agent may return a community string with read-only privileges, even if this object is accessed with a read-write community string. However, the agent must take care not to return a community string which allows more privileges than the community string used to access this object.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TAddress</td>
<td>System.String</td>
<td>The transport service address by which the logical entity receives network management traffic, formatted according to the corresponding value of entLogicalTDomain. For snmpUDPDomain, a TAddress is 6 octets long, the initial 4 octets containing the IP-address in network-byte order and the last 2 containing the UDP port in network-byte order. Consult 'Transport Mappings for Version 2 of the Simple Network Management Protocol' (RFC 1906 [RFC1906]) for further information on snmpUDPDomain.</td>
</tr>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)</td>
</tr>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM first discovered the device during inventory.</td>
</tr>
</tbody>
</table>

### NCM.EntityLogical Entity Relationships

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsEntityLogical (System.Hosting)</td>
</tr>
</tbody>
</table>
## NCM.EntityPhysical

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
</table>
| EntityName          | System.String  | The textual name of the physical entity. The value of this object should be the name of the component as assigned by the local device and should be suitable for use in commands entered at the device's `console`. This might be a text name, such as `console` or a simple component number (e.g. port or module number), such as `1`, depending on the physical component naming syntax of the device. If there is no local name, or this object is otherwise not applicable, then this object contains a zero-length string.  

Note: The value of entPhysicalName for two physical entities will be the same in the event that the console interface does not distinguish between them, e.g., slot-1 and the card in slot-1. |
<p>| EntityDescription   | System.String  | A textual description of physical entity. This object should contain a string which identifies the manufacturer's name for the physical entity, and should be set to a distinct value for each version or model of the physical entity.                                                                                                                                                       |</p>
<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EntityName</td>
<td>System.String</td>
<td>An indication of the vendor-specific hardware type of the physical entity. Note that this is different from the definition of MIB-II's sysObjectID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>An agent should set this object to a enterprise-specific registration identifier value indicating the specific equipment type in detail. The associated instance of entPhysicalClass is used to indicate the general type of hardware device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If no vendor-specific registration identifier exists for this physical entity, or the value is unknown by this agent then the value { 0 } is returned.</td>
</tr>
<tr>
<td>ContainedIn</td>
<td>System.String</td>
<td>The value of entPhysicalIndex for the physical entity which 'contains' this physical entity. A value of zero indicates this physical entity is not contained in any other physical entity. Note that the set of 'containment' relationships define a strict hierarchy; that is, recursion is not allowed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In the event a physical entity is contained by more than one physical entity (e.g., double-wide modules), this object should identify the containing entity with the lowest value of entPhysicalIndex.</td>
</tr>
</tbody>
</table>
## Chapter 8: Working with Config Change Templates

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EntityClass</td>
<td>System.String</td>
<td>An indication of the general hardware type of the physical entity. An agent should set this object to the standard enumeration value which most accurately indicates the general class of the physical entity or the primary class if there is more than one. If no appropriate standard registration identifier exists for this physical entity, then the value 'other(1)' is returned. If the value is unknown by this agent, then the value 'unknown(2)' is returned.</td>
</tr>
<tr>
<td>Position</td>
<td>System.Int32</td>
<td>An indication of the relative position of this 'child' component among all its 'sibling' components. Sibling components are defined as entPhysicalEntries which share the same instance values of each of the entPhysicalContainedIn and entPhysicalClass objects.</td>
</tr>
<tr>
<td>HardwareRevision</td>
<td>System.String</td>
<td>The vendor-specific hardware revision string for the physical entity. The preferred value is the hardware revision identifier actually printed on the component itself (if present).</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note that if revision information is stored internally in a non-printable (e.g. binary) format, then the agent must convert such information to a printable format, in an implementation-specific manner. If no specific hardware revision string is associated with the physical component, or this information is unknown to the agent, then this object will contain a zero-length string.</td>
</tr>
<tr>
<td>FirmwareRevision</td>
<td>System.String</td>
<td>The vendor-specific firmware revision string for the physical entity.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note that if revision information is stored internally in a non-printable (e.g., binary) format, then the agent must convert such information to a printable format, in an implementation-specific manner. If no specific firmware programs are associated with the physical component, or this information is unknown to the agent, then this object will contain a zero-length string.</td>
</tr>
<tr>
<td>SoftwareRevision</td>
<td>System.String</td>
<td>The vendor-specific software revision string for the physical entity.</td>
</tr>
</tbody>
</table>
Chapter 8: Working with Config Change Templates

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Note that if revision information is stored internally in a non-printable (e.g., binary) format, then the agent must convert such information to a printable format, in an implementation-specific manner. If no specific software programs are associated with the physical component, or this information is unknown to the agent, then this object will contain a zero-length string.</td>
</tr>
<tr>
<td>Serial</td>
<td>System.String</td>
<td>The vendor-specific serial number string for the physical entity. The preferred value is the serial number string actually printed on the component itself (if present).</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>System.String</td>
<td>The name of the manufacturer of this physical component. The preferred value is the manufacturer name string actually printed on the component itself (if present).</td>
</tr>
<tr>
<td>Model</td>
<td>System.String</td>
<td>The vendor-specific model name identifier string associated with this physical component. The preferred value is the customer-visible part number, which may be printed on the component itself. If the model name string associated with the physical component is unknown to the agent, then this object will contain a zero-length string.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Alias</td>
<td>System.String</td>
<td>This object is an 'alias' name for the physical entity as specified by a network manager, and provides a non-volatile 'handle' for the physical entity.</td>
</tr>
<tr>
<td>AssetID</td>
<td>System.String</td>
<td>This object is a user-assigned asset tracking identifier for the physical entity as specified by a network manager, and provides non-volatile storage of this information.</td>
</tr>
<tr>
<td>FieldReplaceable</td>
<td>System.String</td>
<td>This object indicates whether or not this physical entity is considered a 'field replaceable unit' by the vendor. If this object contains the value 'true (1)' then this entPhysicalEntry identifies a field replaceable unit. For all entPhysicalEntries which represent components that are permanently contained within a field replaceable unit, the value 'false(2)' should be returned for this object.</td>
</tr>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)</td>
</tr>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM first discovered the device during inventory.</td>
</tr>
</tbody>
</table>
Chapter 8: Working with Config Change Templates

NCM.EntityPhysical Entity Relationships

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsEntityPhysical (System.Hosting)</td>
</tr>
</tbody>
</table>

NCM. Interfaces

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InterfaceID</td>
<td>System.String</td>
<td>[Swis]</td>
</tr>
<tr>
<td>InterfaceIndex</td>
<td>System.Int32</td>
<td>A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one reinitialization of the entity's network management system to the next reinitialization.</td>
</tr>
<tr>
<td>InterfaceDescription</td>
<td>System.String</td>
<td>A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the interface hardware/software.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VLANID</td>
<td>System.Int32</td>
<td>The set of the device’s member ports that belong to the VLAN. Each octet within the value of this object specifies a set of eight ports, with the first octet specifying ports 1 through 8, the second octet specifying ports 9 through 16, etc. Within each octet, the most significant bit represents the lowest numbered port, and the least significant bit represents the highest numbered port. Thus, each port of the VLAN is represented by a single bit within the value of this object. If that bit has a value of ‘1’ then that port is included in the set of ports; the port is not included if its bit has a value of ‘0’. A port number is the value of dot1dBasePort for the port in the BRIDGE-MIB (RFC 1493).</td>
</tr>
</tbody>
</table>
### Property Name | Datatype | Description
--- | --- | ---
PortStatus | System.String | An indication of the current VLAN status of the port. A status of inactive(1) indicates that a dynamic port does not yet have a VLAN assigned, or a port is assigned to a VLAN that is currently not active. A status of active(2) indicates that the currently assigned VLAN is active. A status of shutdown(3) indicates that the port has been disabled as a result of VQP shutdown response.

Possible Values:
inactive(1)  
active(2)  
shutdown(3)

VLANType | System.Int32 | The type of this VLAN
<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InterfaceName</td>
<td>System.String</td>
<td>The textual name of the interface. The value of this object should be the name of the interface as assigned by the local device and should be suitable for use in commands entered at the device's <code>console</code>. This might be a text name, such as <code>le0</code> or a simple port number, such as <code>1</code>, depending on the interface naming syntax of the device. If several entries in the ifTable together represent a single interface as named by the device, then each will have the same value of ifName. If there is no local name, or this object is otherwise not applicable, then this object contains a 0-length string.</td>
</tr>
<tr>
<td>InterfaceAlias</td>
<td>System.String</td>
<td>This object is an 'alias' name for the interface as specified by a network manager, and provides a non-volatile 'handle' for the interface.</td>
</tr>
<tr>
<td>InterfaceType</td>
<td>System.Int32</td>
<td>The type of interface. Additional values for ifType are assigned by the Internet Assigned Numbers Authority (IANA), through updating the syntax of the IANAIfType textual convention.</td>
</tr>
</tbody>
</table>
## Chapter 8: Working with Config Change Templates

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InterfaceTypeName</td>
<td>System.String</td>
<td>The type of interface. Additional values for ifType are assigned by the Internet Assigned Numbers Authority (IANA), through updating the syntax of the IANAifType textual convention.</td>
</tr>
<tr>
<td>InterfaceTypeDescription</td>
<td>System.String</td>
<td>The type of interface. Additional values for ifType are assigned by the Internet Assigned Numbers Authority (IANA), through updating the syntax of the IANAifType textual convention.</td>
</tr>
<tr>
<td>InterfaceSpeed</td>
<td>System.Single</td>
<td>An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reportable by this object then this object should report its maximum value (4, 294, 967, 295) and ifHighSpeed must be used to report the interface’s speed. For a sub-layer which has no concept of bandwidth, this object should be zero.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MACAddress</td>
<td>System.String</td>
<td>The interface's address at its protocol sublayer. The interface's media specific MIB must define the bit and byte ordering and format of the value contained by this object. For interfaces which do not have such an address (e.g. a serial line), this object should contain an octet string of zero length.</td>
</tr>
<tr>
<td>AdminStatus</td>
<td>System.String</td>
<td>The desired state of the interface. The testing(3) state indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with ifAdminStatus in the down(2) state. As a result of either explicit management action or per configuration information retained by the managed system, ifAdminStatus is then changed to either the up (1) or testing (3) states (or remains in the down (2) state).</td>
</tr>
</tbody>
</table>
### Property Name | Datatype | Description
--- | --- | ---
OperStatus | System.String | The current operational state of the interface. The testing (3) state indicates that no operational packets can be passed. If ifAdminStatus is down (2) then ifOperStatus should be down (2). If ifAdminStatus is changed to up (1) then ifOperStatus should change to up (1) if the interface is ready to transmit and receive network traffic; it should change to dormant(5) if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it should remain in the down (2) state if and only if there is a fault that prevents it from going to the up (1) state.

InterfaceMTU | System.Int32 | The size of the largest packet which can be sent/received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.
<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LastChange</td>
<td>System.DateTime</td>
<td>The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this object contains a zero value.</td>
</tr>
<tr>
<td>PhysicalInterface</td>
<td>System.Char</td>
<td>This object has the value 'true (1)' if the interface sublayer has a physical connector and the value 'false(2)' otherwise.</td>
</tr>
<tr>
<td>Promiscuous</td>
<td>System.Char</td>
<td>This object has a value of false (2) if this interface only accepts packets/frames that are addressed to this station. This object has a value of true(1) when the station accepts all packets/frames transmitted on the media. The value true(1) is only legal on certain types of media. If legal, setting this object to a value of true(1) may require the interface to be reset before becoming effective. The value of ifPromiscuousMode does not affect the reception of broadcast and multicast packets/frames by the interface.</td>
</tr>
</tbody>
</table>
Chapter 8: Working with Config Change Templates

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)</td>
</tr>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM first discovered the device during inventory.</td>
</tr>
</tbody>
</table>

**NCM.Interfaces Entity Relationships**

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsInterfaces (System.Hosting)</td>
</tr>
<tr>
<td>IpAddresses</td>
<td>NCM.IpAddresses</td>
<td>NCM.InterfaceHostsIpAddresses (System.Hosting)</td>
</tr>
</tbody>
</table>
## NCM.IpAddresses

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InterfaceIndex</td>
<td>System.Int32</td>
<td>The index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of RFC 1573's ifIndex.</td>
</tr>
<tr>
<td>IPAddress</td>
<td>System.String</td>
<td>The IP address to which this entry's addressing information pertains.</td>
</tr>
<tr>
<td>IPAddrIPSort</td>
<td>System.Double</td>
<td>Store IP address in double representation</td>
</tr>
<tr>
<td>SubnetMask</td>
<td>System.String</td>
<td>The subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.</td>
</tr>
<tr>
<td>InterfaceID</td>
<td>System.String</td>
<td>Interfaceld from interfaces table</td>
</tr>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)</td>
</tr>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM first discovered the device during inventory.</td>
</tr>
</tbody>
</table>
NCM.IpAddresses Entity Relationships

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>NCM.Interfaces</td>
<td>NCM.InterfaceHostsIpAddresses (System.Hosting)</td>
</tr>
</tbody>
</table>

NCM.MacForwarding

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>System.Int32</td>
<td>Either the value '0', or the port number of the port on which a frame having a source address equal to the value of the corresponding instance of dot1dTpFdbAddress has been seen. A value of '0' indicates that the port number has not been learned but that the bridge does have some forwarding/filtering information about this address (e.g. in the dot1dStaticTable). Implementers are encouraged to assign the port value to this object whenever it is learned even for addresses for which the corresponding value of dot1dTpFdbStatus is not learned (3).</td>
</tr>
<tr>
<td>MAC</td>
<td>System.String</td>
<td>A unicast MAC address for which the bridge has forwarding and/or filtering information.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Source</td>
<td>System.String</td>
<td>The status of this entry. The meanings of the values are: other(1): none of the following. This would include the case where some other MIB object (not the corresponding instance of dot1dTpFdbPort, nor an entry in the dot1dStaticTable) is being used to determine if and how frames addressed to the value of the corresponding instance of dot1dTpFdbAddress are being forwarded.</td>
</tr>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)</td>
</tr>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM first discovered the device during inventory.</td>
</tr>
</tbody>
</table>

**NCM.MacForwarding Entity Relationships**

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsMacForwarding (System.Hosting)</td>
</tr>
</tbody>
</table>
### NCM.Nodes

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AgentIP</td>
<td>System.String</td>
<td>Ip address of device entered by customer manually</td>
</tr>
<tr>
<td>Status</td>
<td>System.Byte</td>
<td>NCM only specific status of device: Unknown = 0 (not polled yet) Up = 1 (based on ICMP pool) Down = 2 (based on ICMP pool) Warning = 3 (based on ICMP pool) MonitoringDisabled = 10 (NCM node monitoring is disabled by user) UnManaged = 9 (device is unmanaged in NCM)</td>
</tr>
<tr>
<td>Community</td>
<td>System.String</td>
<td>SNMP community string entered by user</td>
</tr>
<tr>
<td>ReverseDNS</td>
<td>System.String</td>
<td>DNS name of device</td>
</tr>
<tr>
<td>SysName</td>
<td>System.String</td>
<td>An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.</td>
</tr>
<tr>
<td>SysDescr</td>
<td>System.String</td>
<td>A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contains printable ASCII characters.</td>
</tr>
<tr>
<td>SysContact</td>
<td>System.String</td>
<td>The textual identification of the contact person for this managed node, together with information on how to contact this person.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SysLocation</td>
<td>System.String</td>
<td>The physical location of this node (e.g., <code>telephone closet, 3rd floor</code>).</td>
</tr>
<tr>
<td>SystemOID</td>
<td>System.String</td>
<td>The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining <code>what kind of box' is being managed. For example, if vendor </code>Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its `Fred Router'.</td>
</tr>
<tr>
<td>Vendor</td>
<td>System.String</td>
<td>Vendor of device- determined based on SystemOID.</td>
</tr>
<tr>
<td>VendorIcon</td>
<td>System.String</td>
<td>Vendor icon of device- determined based on SystemOID.</td>
</tr>
<tr>
<td>MachineType</td>
<td>System.String</td>
<td>Machine Type - determined based on SystemOID.</td>
</tr>
<tr>
<td>LastBoot</td>
<td>System.DateTime</td>
<td>The time (in hundredths of a second) since the network management portion of the system was last re-initialized.</td>
</tr>
<tr>
<td>OSImage</td>
<td>System.String</td>
<td>Determined based on SysDescr</td>
</tr>
<tr>
<td>OSVersion</td>
<td>System.String</td>
<td>Determined based on SysDescr</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SNMPLevel</td>
<td>System.Byte</td>
<td>SNMP version selected by user (1, 2 or 3)</td>
</tr>
<tr>
<td>SNMPContext</td>
<td>System.String</td>
<td>SNMPv3 credentials entered by user</td>
</tr>
<tr>
<td>SNMPUsername</td>
<td>System.String</td>
<td>SNMPv3 credentials entered by user</td>
</tr>
<tr>
<td>SNMPAuthType</td>
<td>System.String</td>
<td>SNMPv3 credentials entered by user</td>
</tr>
<tr>
<td>SNMPAuthPass</td>
<td>System.String</td>
<td>SNMPv3 credentials entered by user</td>
</tr>
<tr>
<td>SNMPEncryptType</td>
<td>System.String</td>
<td>SNMPv3 credentials entered by user</td>
</tr>
<tr>
<td>SNMPEncryptPass</td>
<td>System.String</td>
<td>SNMPv3 credentials entered by user</td>
</tr>
<tr>
<td>SNMPStatus</td>
<td>System.String</td>
<td>status of SNMP connection to device (OK, No SNMP support, SNMP error description if any)</td>
</tr>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of devices for which data is reported.)</td>
</tr>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>A SWIS-generated date and time marker for when NCM first discovered the device during inventory.</td>
</tr>
<tr>
<td>Type</td>
<td>Entity</td>
<td>Joined Data Entity</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Interfaces</td>
<td>NCM.Interfaces</td>
<td>NCM.NodeHostsInterfaces (System.Hosting)</td>
</tr>
<tr>
<td>MacForwarding</td>
<td>NCM.MacForwarding</td>
<td>NCM.NodeHostsMacForwarding (System.Hosting)</td>
</tr>
<tr>
<td>VLANs</td>
<td>NCM.VLANs</td>
<td>NCM.NodeHostsVLANs (System.Hosting)</td>
</tr>
<tr>
<td>BridgePorts</td>
<td>NCM.BridgePorts</td>
<td>NCM.NodeHostsBridgePorts (System.Hosting)</td>
</tr>
<tr>
<td>ArpTables</td>
<td>NCM.ArpTables</td>
<td>NCM.NodeHostsArpTables (System.Hosting)</td>
</tr>
<tr>
<td>CiscoCards</td>
<td>NCM.CiscoCards</td>
<td>NCM.NodeHostsCiscoCards (System.Hosting)</td>
</tr>
<tr>
<td>CiscoCdp</td>
<td>NCM.CiscoCdp</td>
<td>NCM.NodeHostsCiscoCdp (System.Hosting)</td>
</tr>
<tr>
<td>CiscoChassis</td>
<td>NCM.CiscoChassis</td>
<td>NCM.NodeHostsCiscoChassis (System.Hosting)</td>
</tr>
<tr>
<td>CiscoFlash</td>
<td>NCM.CiscoFlash</td>
<td>NCM.NodeHostsCiscoFlash (System.Hosting)</td>
</tr>
<tr>
<td>CiscoFlashFiles</td>
<td>NCM.CiscoFlashFiles</td>
<td>NCM.NodeHostsCiscoFlashFiles (System.Hosting)</td>
</tr>
<tr>
<td>CiscoImageMIB</td>
<td>NCM.CiscoImageMIB</td>
<td>NCM.NodeHostsCiscoImageMIB (System.Hosting)</td>
</tr>
<tr>
<td>CiscoMemoryPools</td>
<td>NCM.CiscoMemoryPools</td>
<td>NCM.NodeHostsCiscoMemoryPools (System.Hosting)</td>
</tr>
</tbody>
</table>
Chapter 8: Working with Config Change Templates

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>EntityLogical</td>
<td>NCM.EntityLogical</td>
<td>NCM.NodeHostsEntityLogical (System.Hosting)</td>
</tr>
<tr>
<td>EntityPhysical</td>
<td>NCM.EntityPhysical</td>
<td>NCM.NodeHostsEntityPhysical (System.Hosting)</td>
</tr>
<tr>
<td>PortsTcp</td>
<td>NCM.PortsTcp</td>
<td>NCM.NodeHostsPortsTcp (System.Hosting)</td>
</tr>
<tr>
<td>PortsUdp</td>
<td>NCM.PortsUdp</td>
<td>NCM.NodeHostsPortsUdp (System.Hosting)</td>
</tr>
<tr>
<td>RouteTable</td>
<td>NCM.RouteTable</td>
<td>NCM.NodeHostsRouteTable (System.Hosting)</td>
</tr>
</tbody>
</table>

**NCM.PortsTcp**

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>The unique identifier of a network node subject to configuration actions.</td>
</tr>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>Date and time NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>Date and time NCM first discovered the device during inventory.</td>
</tr>
<tr>
<td>TCPLocalAddress</td>
<td>System.String</td>
<td>The local IP address for this TCP connection. In the case of a connection in the listen state which is willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TCPLocalPort</td>
<td>System.Int32</td>
<td>The local port number for this TCP connection.</td>
</tr>
<tr>
<td>TCPLocalPortName</td>
<td>System.String</td>
<td>Port description based on TCPLocalPort value</td>
</tr>
<tr>
<td>TCPRemoteAddress</td>
<td>System.String</td>
<td>The remote IP address for this TCP connection.</td>
</tr>
<tr>
<td>TCPRemotePort</td>
<td>System.Int32</td>
<td>The remote port number for this TCP connection.</td>
</tr>
<tr>
<td>TCPState</td>
<td>System.String</td>
<td>The state of this TCP connection. The only value which may be set by a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>management station is deleteTCB(12). Accordingly, it is appropriate for an</td>
</tr>
<tr>
<td></td>
<td></td>
<td>agent to return a 'badValue' response if a management station attempts to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>set this object to any other value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If a management station sets this object to the value deleteTCB(12), then</td>
</tr>
<tr>
<td></td>
<td></td>
<td>this has the effect of deleting the TCB (as defined in RFC 793) of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>corresponding connection on the managed node, resulting in immediate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>termination of the connection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>As an implementation-specific option, a RST segment may be sent from the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>managed node to the other TCP endpoint (note however that RST segments are</td>
</tr>
<tr>
<td></td>
<td></td>
<td>not sent reliably).</td>
</tr>
<tr>
<td>TCPRemotePortName</td>
<td>System.String</td>
<td>Port description based on TCPRemotePort value</td>
</tr>
</tbody>
</table>
Chapter 8: Working with Config Change Templates

NCM.PortsTcp Entity Relationships

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsPortsTcp (System.Hosting)</td>
</tr>
</tbody>
</table>

NCM.PortsUdp

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>The unique identifier of a network node subject to configuration actions.</td>
</tr>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>Date and time NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>Date and time NCM first discovered the device during inventory.</td>
</tr>
<tr>
<td>UDPAddress</td>
<td>System.String</td>
<td>The local IP address for this UDP listener. In the case of a UDP listener which is willing to accept datagrams for any IP interface associated with the node, the value 0.0.0.0 is used.</td>
</tr>
<tr>
<td>UDPPort</td>
<td>System.Int32</td>
<td>The local port number for this UDP listener.</td>
</tr>
<tr>
<td>UDPPortName</td>
<td>System.String</td>
<td>Port description based on UDPPort value (like 161- SNMP)</td>
</tr>
</tbody>
</table>

NCM.PortsUdp Entity Relationships

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsPortsUdp (System.Hosting)</td>
</tr>
</tbody>
</table>
NCM.RouteTable

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>The unique identifier of a network node subject to configuration actions.</td>
</tr>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>Date and time NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>Date and time NCM first discovered the device during inventory.</td>
</tr>
<tr>
<td>InterfaceIndex</td>
<td>System.Int32</td>
<td>The index value which uniquely identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>InterfaceID</td>
<td>System.String</td>
<td>Indicate the mask to be logical-ANDed with the destination address before being compared to the value in the ipRouteDest field. For those systems that do not support arbitrary subnet masks, an agent constructs the value of the ipRouteMask by determining whether the value of the correspondent ipRouteDest field belong to a class-A, B, or C network, and then using one of: mask network 255.0.0.0 class-A 255.255.0.0 class-B 255.255.255.0 class-C If the value of the ipRouteDest is 0.0.0.0 (a default route), then the mask value is also 0.0.0.0. It should be noted that all IP routing subsystems implicitly use this mechanism.</td>
</tr>
<tr>
<td>Destination</td>
<td>System.String</td>
<td>The type of route. Note that the values direct(3) and indirect(4) refer to the notion of direct and indirect routing in the IP architecture. Setting this object to the value invalid(2) has the effect of invalidating the corresponding entry in the ipRouteTable object. That is, it effectively disassociates the destination identified with said entry from the route identified with said entry. It is an implementation-specific matter as to whether the agent removes an invalidated entry from the table.</td>
</tr>
</tbody>
</table>
Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant ipRouteType object.

Possible Values:
- other(1)
- invalid(2)
- direct(3)
- indirect(4)
<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mask</td>
<td>System.String</td>
<td>The routing mechanism via which this route was learned. Inclusion of values for gateway routing protocols is not intended to imply that hosts should support those protocols. Possible Values: other(1) local(2) netmgmt(3) icmp(4) egp(5) ggp(6) hello(7) rip(8) is-is(9) es-is(10) ciscoIgrp(11) bbnSpflgp(12) ospf(13) bgp(14)</td>
</tr>
<tr>
<td>NextHop</td>
<td>System.String</td>
<td>The number of seconds since this route was last updated or otherwise determined to be correct. Note that no semantics of 'too old' can be implied except through knowledge of the routing protocol by which the route was learned.</td>
</tr>
<tr>
<td>RouteType</td>
<td>System.String</td>
<td>The IP address of the next hop of this route. (In the case of a route bound to an interface which is realized via a broadcast media, the value of this field is the agent's IP address on that interface.)</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RouteProtocol</td>
<td>System.String</td>
<td>The primary routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.</td>
</tr>
<tr>
<td>RouteAge</td>
<td>System.Int32</td>
<td>An alternate routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.</td>
</tr>
<tr>
<td>NextHopAS</td>
<td>System.Int32</td>
<td>An alternate routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.</td>
</tr>
<tr>
<td>Metric1</td>
<td>System.Int32</td>
<td>An alternate routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.</td>
</tr>
<tr>
<td>Metric2</td>
<td>System.Int32</td>
<td>An alternate routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.</td>
</tr>
</tbody>
</table>
### Property Name | Datatype | Description
--- | --- | ---
Metric3 | System.Int32 | The index value which uniquely identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.

Metric4 | System.Int32 | Indicate the mask to be logical-ANDed with the destination address before being compared to the value in the ipRouteDest field. For those systems that do not support arbitrary subnet masks, an agent constructs the value of the ipRouteMask by determining whether the value of the correspondent ipRouteDest field belong to a class-A, B, or C network, and then using one of:

- mask network
  - 255.0.0.0 class-A
  - 255.255.0.0 class-B
  - 255.255.255.0 class-C

  If the value of the ipRouteDest is 0.0.0.0 (a default route), then the mask value is also 0.0.0.0. It should be noted that all IP routing subsystems implicitly use this mechanism.
<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metric5</td>
<td>System.Int32</td>
<td>The type of route. Note that the values direct(3) and indirect(4) refer to the notion of direct and indirect routing in the IP architecture.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Setting this object to the value invalid(2) has the effect of invalidating the corresponding entry in the ipRouteTable object. That is, it effectively disassociates the destination identified with said entry from the route identified with said entry. It is an implementation-specific matter as to whether the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant ipRouteType object. Possible Values: other(1) invalid(2) direct(3) indirect(4)</td>
</tr>
</tbody>
</table>

NCM.RouteTable Entity Relationships

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsRouteTable (System.Hosting)</td>
</tr>
</tbody>
</table>
### NCM.VLANs

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NodeID</td>
<td>System.String</td>
<td>The unique identifier of a network node subject to configuration actions.</td>
</tr>
<tr>
<td>LastDiscovery</td>
<td>System.DateTime</td>
<td>Date and time NCM last discovered the device during inventory.</td>
</tr>
<tr>
<td>FirstDiscovery</td>
<td>System.DateTime</td>
<td>Date and time NCM first discovered the device during inventory.</td>
</tr>
<tr>
<td>VLANID</td>
<td>System.Int32</td>
<td>The set of the device's member ports that belong to the VLAN. Each octet within the value of this object specifies a set of eight ports, with the first octet specifying ports 1 through 8, the second octet specifying ports 9 through 16, etc. Within each octet, the most significant bit represents the lowest numbered port, and the least significant bit represents the highest numbered port. Thus, each port of the VLAN is represented by a single bit within the value of this object. If that bit has a value of '1' then that port is included in the set of ports ; the port is not included if its bit has a value of '0'. A port number is the value of dot1dBasePort for the port in the BRIDGE-MIB (RFC 1493).</td>
</tr>
<tr>
<td>VLANName</td>
<td>System.String</td>
<td>The name of this VLAN. This name is used as the ELAN-name for an ATM LAN-Emulation segment of this VLAN.</td>
</tr>
</tbody>
</table>
### NCM.VLANs Entity Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLANMTU</td>
<td>System.Int32</td>
<td>The MTU size on this VLAN, defined as the size of largest MAC-layer (information field portion of the) data frame which can be transmitted on the VLAN.</td>
</tr>
<tr>
<td>VLANType</td>
<td>System.Int32</td>
<td>The type of this VLAN</td>
</tr>
<tr>
<td>VLANState</td>
<td>System.Int32</td>
<td>The state of this VLAN. Possible Values: operational(1) suspended(2) mtuTooBigForDevice(3) mtuTooBigForTrunk(4)</td>
</tr>
</tbody>
</table>

### NCM.VLANs Entity Relationships

<table>
<thead>
<tr>
<th>Type</th>
<th>Entity</th>
<th>Joined Data Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>NCM.Nodes</td>
<td>NCM.NodeHostsVLANs (System.Hosting)</td>
</tr>
</tbody>
</table>
Chapter 9: Managing Inventory

The inventory engine of SolarWinds Network Configuration Manager compliments the product's configuration management functions. You can perform on all of your nodes, node groups, or single nodes. You can view collected inventory statistics in the detail view of each device.

For more information:
Running a Complete Inventory Scan
Running an Inventory Scan
Scheduling an Inventory Scan
Adjusting Inventory Settings
Viewing Inventory Status
Running a Complete Inventory Scan

A full inventory scan can take anywhere from a few minutes to several hours to complete. The time period varies based on the number of nodes and the type of statistics you want to collect. For more information on how to establish what statistics are collected, see Adjusting Inventory Settings.

To perform an inventory of all NCM nodes:

1. From the web console, click **CONFIGS > Configuration Mangement.**
2. Use the **Group by** control to select **[No grouping]**.
3. Select all nodes.
4. Click **Update Inventory**.

To run an inventory scan as a recurrent job, see Baselining Your Entire Network

Running an Inventory Scan

Complete the following procedure to run an individual inventory scan on a single node.

To inventory a single node:

1. Open the Orion Web Console.
2. Click **CONFIGS > Configuration Management.**
3. Use the **Search** tool or the **Group by** options to find the node.
4. Select the node and click **Update Inventory**.

For information on scheduling a recurrent inventory scan job, see Scheduling an Inventory Scan

For information on baselining the network, see Baselining Your Entire Network.

Scheduling an Inventory Scan

1. From the web console, click **CONFIGS > Jobs.**
2. Click **Create New Job.**
3. Name the job, and then select **Update Inventory** from **Job Type**.
4. Select the Schedule Type.
   - *If you are creating a Basic schedule*, select the frequency of the job: once, daily, weekly, or monthly.
   - *If you are creating an Advanced schedule*, use the five fields to create an appropriate cron expression.

5. Add a comment if desired, and then click Next.

6. Select the nodes to target with this job, and then click Next.

7. Select an email notification option, and then click Next.

8. Select the information types to include in the Inventory job, and then click Next.

9. Review the settings for the job, and then click Finish.

### Adjusting Inventory Settings

1. From the web console, click **Settings > NCM Settings**.
2. Under NCM Node Management, click **Node Inventory**.
3. Select the information types to collect.
4. Adjust the number of devices that should be inventoried concurrently. The default is five.

5. *If you have VLANs extended across network trunks*, and you want to inventory the relevant devices, select **Extend VLANs inventory**.
   
   SolarWinds recommends against this situation due to the slow performance of the inventory process.

6. *If the inventory process causes the NCM server to hang or if the process takes too long*, select **Disable inventory lookup**.
   
   You would then need to analyze the cause of the problem (for example, server capacity) before selecting this option again.

7. Click **Submit**.
Viewing Inventory Status

1. From the web console, click CONFIGS > Configuration Management.
2. Click the Inventory Status tab.
3. Click a column to change the sort order.
Chapter 10: Managing Inventory Reports

SolarWinds NCM includes standard reports that display configuration information for each node and statistics collected by the inventory engine.

All NCM reports are available from the web console at HOME > Reports.

For more information:
- Viewing Reports
- Creating and Scheduling Reports
- Exporting Reports to PDF and Printing
- Printing Reports
- Deleting a Report
**Viewing Reports**

1. From the web console, click HOME > Reports.
2. Use the Group by control and the Search field to find a report.
3. Select a report, and then click View Report.

**Note:** By default, newly created users do not have a configured report folder. If a new user is not seeing reports, you may need to select a Report Folder for the new user. For details, see "Configuring an Account Report Folder" in the SolarWinds Network Performance Administrator Guide.

**Creating and Scheduling Reports**

1. From the web console, click CONFIGS > Jobs.
2. Click Create New Job.
3. Name the job, and then select Run Report from Job Type.
4. Select the Schedule Type.
   - *If you are creating a Basic schedule,* select the frequency of the job: once, daily, weekly, or monthly.
   - *If you are creating an Advanced schedule,* use the five fields to create an appropriate cron expression.
5. Add a comment if desired, and then click Next.
6. Click Next.
7. Select an email notification option, and then click Next.
8. Select a report on the Job Details resource. For more information, see Available Reports.
9. Set a limitation for the number of records that can be exported, if necessary.
10. Click Next.
11. Review the settings for the job, and then click Finish.

**Exporting Reports to PDF and Printing**

1. From the web console, click CONFIGS > Reports.
2. Use the Group by control and the Search field to find reports.
3. Select a report, and then click View Report.
4. Click Export to PDF.
5. Save the PDF to your computer.
6. Open the PDF in Adobe Acrobat, and then print if necessary.

Printing Reports

1. From the web console, click HOME > Reports.
2. Use the Group by control and the Search field to find a report.
3. Select a report, and then click View Report.
4. Click Print.

Deleting Reports

1. From the web console, click HOME > Reports.
2. Click Manage Reports.
3. Select a report, and then click Delete.
Managing Policy Reports

Policy reports help ensure device configurations conform to both internal business practices and federal regulations, such as Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability (HIPAA), and Computer Inventory of Survey Plans (CISP). Policy reports scan configuration files and report any discovered rule violations. For example, a rule requires that configurations do not include the read-only community string public. You can run a report on your configuration files, and then display any configurations that violate the rule. Your policy report lists violations, including the line number where the violation occurred. Several example reports, policies, and rules are included with SolarWinds Network Configuration Manager.

For more information:
- Creating a Policy Report
- Creating a Policy
- Creating a Policy Rule
- Rules
- Editing a Policy Rule
- Deleting a Policy Rule
- Policy Reports
- Editing a Policy Report
- Generating a Policy Report
- Exporting a Policy Report (to thwack)
- Exporting a Policy Report (as a file)
- Scheduling a Policy Report
- Deleting a Report
- Enabling the Config and Policy Caches
Managing Policy Reports

Creating a Policy Report

1. From the web console, click **CONFIGS > Compliance**.
2. Click **Manage Policy Reports**.
3. Click **Add New Report**.
4. Name the report, and then enter a description.
5. Select Save in Folder and Display settings.
6. Select policies from folders in All Policies, and then click **Add**.
   
   **Note:** If your policy is not listed, see [Creating a Policy](#).

7. Click **Submit**.

For more information:

- [Editing a Policy Report](#)
- [Creating a Policy](#)
- [Editing a Policy Rule](#)
- [Creating a Policy Rule](#)

Creating a Policy

A policy is a collection of rules against which device configurations are reviewed for compliance. Policies are used in producing reports on device compliance.

1. From the web console, click **CONFIGS > Compliance**.
2. Click **Manage Policy Reports**.
3. On the Manage Policies tab, click **Add New Policy**.
4. Name the policy, and then enter a description.
5. Select Save in Folder and Select Nodes settings.
6. Select the most recent config type to search for with this policy.
7. Select rules from folders in All Policy Rules, and then click **Add**.
Note: If your rule is not listed, see Creating a Policy Rule.

8. Click Submit.

To include this policy in a report, see Creating a Policy Report.

Creating a Policy Rule

A rule verifies policy compliance of a device by specifying a string that either must or must not be present in a configuration file. Rules are collected into policies and applied to specific network devices. Reports of policy violations are generated based on a schedule.

Basic String Matching

1. From the web console, click CONFIGS > Compliance.
2. Click Manage Policy Reports.
4. Name the rule, and then enter a description.
5. Select the Alert Level and Save in Folder settings.
6. Select the type of alert trigger.
7. Enter a string and select the String type.
8. Create a script in Remediation to modify the lines of configuration if they do not comply with the policy rule.

Notes:

- To function properly, a remediation script must include CLI statements that run on the relevant devices. When executed, the script runs through the default communication protocol (Telnet, SSH).
- Your script should put the device into configuration mode, if needed, issue a series of config commands, and then exit config mode.

9. Select a Remediation Script type.

Your selection determines how NCM executes commands against targeted devices to remediate a policy rule violation.

CLI allows NCM to use the commands in the script to change the config.
Managing Policy Reports

**Config Change Template** launches the Config Change Template wizard to guide you through executing the script.

10. Click **Test** to validate the rule against a device configuration.
11. Select a config to test the rule against.
12. Click **Test Rule Against Selected Config**.

   **Notes:**
   - Test your rule against at least two nodes and configurations, one known to comply with the rule, the other known not to comply.
   - In testing a rule against a noncompliant configuration, expect a result that includes the rule and its violation.

13. Click **Select Different Config** to continue your rule test on another config.
14. Click **Close**, and then click **Submit**.

To include this rule in a policy, see [Creating a Policy](#).

**Advanced String Matching**

1. From the web console, click **CONFIGS > Compliance**.
2. Click **Manage Policy Reports**.
3. On the Manage Rules tab, click **Add New Rule**.
4. Name the rule, and then enter a description.
5. Select the Alert Level and Save in Folder settings.
6. Select the type of alert trigger.
7. Select **Advanced Config Search**.
8. Select the appropriate option in the String Type list.
9. Type your string or expression in the **String** field.

   See [Regular Expression Pattern Matching Examples](#) for help with regular expressions.

   **Note:** If there are some special non-printable characters at the end of the lines in a downloaded config, the $ operator might not match the line end. A test would be to copy lines from a config to a plain text file (in Notepad, for example). If you see extra, empty lines that are not in the pasted content then there are mostly likely non-printable characters in them.

10. If you want to build conditions into your search, click **Add Another String** and create the string, as before.

11. Repeat this step for as many strings as you need to define your search.

   For example, let’s assume that you need to search configs for occurrences of the string `access list` in conjunction with different names (Joe, Sam, Tom). To build the appropriate conditions into the search, you would create the following logic:

   ```
   Must Contain ^(?=.*?\bAccess-list\b)(?=.*?\bjoe\b).*$
   OR Must Contain ^(?=.*?\bAccess-list\b)(?=.*?\bsam\b).*$
   OR Must Contain ^(?=.*?\bAccess-list\b)(?=.*?\tom\b).*$
   ```

   A violation of this rule logic occurs if NCM finds in a line in a config that includes the string `Access-list` and the string *joe*, *sam*, or *tom*.

12. Adjust the operators (And/Or) to determine relationships between strings in the execution of your search. The default operator is **and**.

13. Use parentheses to group strings into conditional relationships and to establish relationships between string groups.

   For example, if you had three strings defined, you might put opening and closing parentheses around the first two strings, linking the two with the **and** operator. Then you might use the **or** operator to evaluate the last string by itself. The result will be a search that looks for both of the first two configs. If it finds them, the alert is triggered. If it does not find them, but the last string is found, the alert is also triggered. Finally, the alert is triggered if both the first two strings and the last string are found.
14. Select the search context under Search Config File/Block.

15. Create a script in Remediation to modify the lines of configuration if they do not comply with the policy rule.

**Notes:**

- To function properly, a remediation script must include CLI statements that run on the relevant devices. When executed, the script runs through the default communication protocol (Telnet, SSH).
- Your script should put the device into configuration mode, if needed, issue a series of config commands, and then exit config mode.

16. Select a Remediation Script type.

Your selection determines how NCM executes commands against targeted devices to remediate a policy rule violation.

**CLI** allows NCM to use the commands in the script to change the config.  
**Config Change Template** launches the Config Change Template wizard to guide you through executing the script.

17. Click **Test** to validate the rule against a device configuration.

18. Select a config to test the rule against.

19. Click **Test Rule Against Selected Config**.

**Notes:**

- Test your rule against at least two nodes and configurations, one known to comply with the rule, the other known not to comply.
- In testing a rule against a non-compliant configuration, expect a result that includes the rule and its violation. For example, if you were attempting to disable Reverse-Telnet with your rule, you would see something like this in case the config under test violates the rule:

  ```
  Pattern 'line con 0.*\n(.*)\n.*transport input none' was not found
  ```

  This tells you that the NCM policy software used the regular expression specified under String Matching to search the specified config file and no matches were found. Since it expected to find the specified string, the software generates an alert.
Rules

20. Click **Select Different Config** to continue your rule test on another config.
21. Click **Close**, and then click **Submit**.

To include this rule in a policy, see [Creating a Policy](#).

### Rules

Rules describe what is to be found (or not found) in device configuration files. Rules contain the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>How the rule will be shown in display lists and Reports</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the rule</td>
</tr>
<tr>
<td>Alert Level</td>
<td>Severity of the alert:</td>
</tr>
<tr>
<td></td>
<td>• Informational</td>
</tr>
<tr>
<td></td>
<td>• Warning</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td>Grouping</td>
<td>Folder to which the rule belongs</td>
</tr>
<tr>
<td>Pattern Must Exist</td>
<td>Whether the pattern should be found or not</td>
</tr>
<tr>
<td>String</td>
<td>Regular expression or string that defines the search object</td>
</tr>
<tr>
<td>String Type</td>
<td>Type of search expression:</td>
</tr>
<tr>
<td></td>
<td>• Regular expression</td>
</tr>
<tr>
<td></td>
<td>• Find string</td>
</tr>
</tbody>
</table>

If the Advanced Config Search feature is activated, string matching includes these additional properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>And/Or</td>
<td>Operator that defines the relationship between two strings</td>
</tr>
</tbody>
</table>
Managing Policy Reports

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parentheses</td>
<td>Operator that logically groups strings</td>
</tr>
<tr>
<td>Must/Must Not Contain</td>
<td>Determines if the alert triggers based on the presence or absence of a string</td>
</tr>
<tr>
<td>String</td>
<td>Regular expression or string that defines the search object</td>
</tr>
<tr>
<td>String Type</td>
<td>Type of search expression</td>
</tr>
<tr>
<td></td>
<td>• Regular expression</td>
</tr>
<tr>
<td></td>
<td>• Find string</td>
</tr>
</tbody>
</table>

Editing a Policy Rule

1. From the web console, click **CONFIGS > Compliance**.
2. Click **Manage Policy Reports**.
3. Click the Manage Rules tab.
4. Select a rule, and then click **Edit**.
5. Edit the appropriate values.
   See **Creating a Policy Rule** for information on working with the rule template.
6. Review the rule details, and then click **Submit**.

Deleting a Policy Rule

1. From the web console, click **CONFIGS > Compliance**.
2. Click **Manage Policy Reports**.
3. Click the Manage Rules tab.
4. Select a rule, and then click **Delete**.
5. Click **Yes**.
Policies

A policy is a collection of one or more rules. These rules define the type of configuration file to search and the nodes that are included in the search.

Editing a Policy

1. From the web console, click CONFIGS > Compliance.
2. Click Manage Policy Reports.
3. Click the Manage Policies tab.
4. Select a policy, and then click Edit.
5. Edit the appropriate values.
   See [Creating a Policy](#) for information on working with the policy template.
6. Review the policy details, and then click Submit.

Deleting a Policy

1. From the web console, click CONFIGS > Compliance.
2. Click Manage Policy Reports.
3. Click the Manage Policies tab.
4. Select a policy, and then click Delete.
5. Click Yes.

Policy Reports

Reports provide a way to group policies, either by the devices that they will be executed against or by the type of report in which they are used. Report properties include Name, Comment, Grouping, and the policies included in the Report.

Editing a Policy Report

1. From the web console, click CONFIGS > Compliance.
2. Click Manage Policy Reports.
3. Select a report, and then click Edit.
4. Edit the appropriate values.
Managing Policy Reports

See Creating a Policy Report for information on working with the policy template.

5. Review the report details, and then click Submit.

Generating a Policy Report

1. From the web console, click CONFIGS > Compliance.
2. Click a report in the list to view it.
3. Click a rule or violation icon to display the Violation Details.
4. Click View Config to see the config file for the node.
5. Click a Management option to execute a remediation script on this node or all nodes in violation.
6. In the Execute {ReportName} Remediation Script resource, enter or modify the script so that it includes commands that will be accepted by your device.
7. To review or modify the nodes against which your script will run, click Select Nodes.
8. Click Execute Script.

Exporting a Policy Report (to thwack)

1. From the web console, click CONFIGS > Compliance.
2. Click Manage Policy Reports.
3. Select a report, and then click Export to thwack.
4. If prompted, enter your user name and password, and then click Log In.

Exporting a Policy Report (as a file)

1. From the web console, click CONFIGS > Compliance.
2. Click Manage Policy Reports.
3. Select a report, and then click Export as File.
4. Click Export as File. Verify that a pop-up blocker does not prevent the file from being downloaded.
5. Download the file to a local folder.
Deleting a Report

1. From the web console, click HOME > Reports.
2. Click Manage Reports.
3. Select a report in the list.
4. Click Delete.

Scheduling a Policy Report

1. From the web console, click CONFIGS > Jobs.
2. Click Create New Job.
   
   Note: Do not use special characters in the name.
3. Name the job, and select Generate a Policy Report from Job Type.
4. Select the Schedule Type.
   
   - If you are creating a Basic schedule, select the frequency of the job: once, daily, weekly, or monthly.
   
   - If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if desired, and then click Next.
6. Click Next.
7. Select an email notification option, and then click Next.
8. Select the policy report to generate as part of the job.
9. If you want to suppress notifications when no violations are found, select Send notification only when there are policy violations.
10. Click Next.
11. Review the settings for the job, and then click Finish.

Enabling the Config and Policy Caches

Note: If enabled, the config and policy caches are updated daily at 11:55 PM.

1. From the web console, click Settings > NCM Settings.
2. Under Advanced, click Advanced Settings.
3. Under Cache Settings, select **Enable Config and Policy Caches**.
4. Click **Submit**.

**Manually Refresh the Policy Cache**

1. From the web console, click **CONFIGS > Compliance**.
2. Click **Update All**.

**Note:** When you run a policy report or a scheduled job from SolarWinds NCM, the data returned is a snapshot of current policy compliance and does not rely on the policy cache.
Chapter 12: Managing Jobs

SolarWinds Network Configuration Manager provides job scheduling for configuration management to help automate the management of network devices. You can schedule numerous operations, including configuration file uploads and downloads, node reboots, and command script execution.

**Note:** Orion Platform Administrator, NCM Administrator and NCM Engineer roles have full access to all jobs in the job list. Other assigned NCM roles can access and manage only the jobs they create, but not others.

For more information:
- Enabling and Disabling a Job
- Starting and Stopping a Job
- Creating or Editing a Job
- Viewing Job Logs
Enabling and Disabling a Job

Enable or disable operations apply to jobs that run according to a schedule. You can delete any job you no longer use.

For more information:
- Enabling a Job
- Disabling a Job

Enabling a Job

You must enable a job before you can start it. A job that is not enabled will not start.

1. From the web console, click CONFIGS > Jobs.
2. Select a disabled job in the list.
3. Click Enable.

Disabling a Job

Disable a job to suspend it, but not delete it.

1. From the web console, click CONFIGS > Jobs.
2. Select a scheduled job in the list.
3. Click Disable.
Starting and Stopping a Job

Though using a schedule is the most efficient way to manage jobs, you can manually start and stop jobs if necessary.

For more information:
Starting a Job
Stopping a job

Starting a Job
You can start any job that is enabled.

1. From the web console, click CONFIGS > Jobs.
2. Select a job in the list.
3. If the job is disabled, click Enable.
4. Click Start Job.

Stopping a job
A job currently running shows the status running.

1. From the web console, click CONFIGS > Jobs.
2. Select a running job in the list.
3. Click Stop Job.
Chapter 12: Managing Jobs

Creating or Editing a Job

When processing an active job, SolarWinds NCM uses credential settings of the user who last edited the job. For example, if the user has user level login credentials set, NCM uses the connection profile associated with the device.

1. From the web console, click CONFIGS > Jobs.
2. If you are creating a new job, click Create New Job.
3. If you want to edit an existing job, select a job, and then click Edit.
4. Name the job, and then select a Job Type.
   Note: Do not use special characters in the name.
5. Select the Schedule Type.
   - If you are creating a Basic schedule, select the frequency of the job: once, daily, weekly, or monthly.
   - If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
6. Add a comment if desired, and then click Next.
7. Select the nodes to target with this job, and then click Next.
8. Select an email notification option, and then click Next.
9. Add details based on the specific job, and then click Next.
10. Review the settings for the job, and then click Finish.
Viewing Job Logs

View the job log to verify that a job was run as scheduled, or to view the history of the job.

1. From the web console, click **CONFIGS > Jobs**.
2. Select the job in the list.
3. Sort by the Last Date Run column.
4. Click the page icon in the History column to view the log.
Deleting a Job

Permanently remove a job, rather than temporarily disable it.

1. From the web console, click CONFIGS > Jobs.
2. Select a disabled job in the list.
3. Click Delete.
Chapter 13: Approving Device Configuration Changes

SolarWinds Network Configuration Manager enables you to define a semi-automated approval process for making configuration changes on network devices.

SolarWinds NCM uses roles to determine which Orion accounts are able to perform the tasks of changing device configurations (*WebUploader*), approving those changes (*Administrator*), and changing the roles of Orion accounts (*Engineer, Administrator*).

SolarWinds NCM uses email to relay config change approval requests. As part of setting up the config change approval system, you must provide SMTP information.

For more information:

- Enabling and Disabling Config Change Approval
- Setting Up the Config Change Approval System
- Creating and Editing an NCM Account
Setting Up the Config Change Approval System

The Setup Wizard guides you through the process of specifying an email server for notifications, addresses of change approvers, and accounts of team members who manage device configurations.

1. From the web console as an administrator, click CONFIGS > NCM Settings.
2. Under Config Management Change Approval, click Setup Wizard.
3. Select an approval mode, and then click Submit.
4. Enter SMTP settings and click Submit.
5. Enter Admin Email settings.
   - If you are using one-level approval, the address(es) in the To: box receives notifications of pending device config changes.
   - The address in the From: field is shown as the sending address for config change approval requests.
   - The Subject: field appears in the subject line of config change approval requests.
   - Add an additional message regarding to inform approvers of the standard action to take.
6. Click Submit.
7. If you selected one-level approval, click Manage Users to adjust the NCM role for accounts that will be submitting upload requests, and then follow the steps in Creating and Editing an NCM Account. Otherwise, click Finish.
8. If you selected a form of two-level approval, select a user and enter a valid address for Approval Level 1 and Approval Level 2, and then click Finish.
   - Note: For each user in the list that you want to have a WebUploader role but neither the Engineer or Administrator role, select the user name, and then click Edit.
9. When you are finished managing users and adding level 1 and level 2 addresses, click Submit.
When you enable the change approval system, SolarWinds NCM prevents the system from executing device uploads until an NCM administrator has approved the scheduled job.

To enable the system, see Enabling and Disabling Config Change Approval.
Chapter 13: Approving Device Configuration Changes

Enabling and Disabling Config Change Approval

Before you enable the system, set it up by following the steps in Setting Up the Config Change Approval System.

1. From the web console, click CONFIGS > NCM Settings.
2. Under Config Management Change Approval, click Enable Approval System.
3. Click Enable.
   
   Note: The default setting is to allow any NCM user with the WebUploader role or higher to make and push a device configuration change with no approval necessary. Enabling the Change Approval System without changing the default setting is the same as not enabling the system at all.
4. Make your selection, and then click Submit.

   When you enable the change approval system, SolarWinds NCM prevents the system from executing device uploads until an NCM administrator has approved the scheduled job.

To disable the change approval system:

1. From the web console, click CONFIGS > NCM Settings.
2. Under Config Management Change Approval, click Disable Approval System.

   When you disable the system, SolarWinds NCM processes device configuration changes normally, either as scheduled or immediately, depending on the actions of the relevant team member with the WebLoader account privileges.
Managing NCM Approval Requests

Use this resource to view requests and, as an NCM administrator, to approve and decline them.

1. From the web console, click **CONFIGS > NCM Settings**.
2. Under Config Management Change Approval, click **Pending Approval**.
3. Select a request in the list, and then click **Approve** or **Decline**.
Creating and Editing an NCM Account

Only a user with Administrator privileges can create a new account and prepare it for use with NCM.

Creating a New Account

1. From the web console, click Settings.
2. Under User Accounts, click Manage Accounts.
3. Click Add New Account.
4. Select Orion individual account, and then click Next.
5. Enter credentials for the new account, and then click Next.
6. Define settings for the Orion individual account.
   - Decide if this account should have Administrator Rights and Node Management Rights.
   - Accept the current defaults under Default Menu Bar and Views and Orion General Settings. The account holder will be able to customize these settings.
   - Assign the appropriate NCM role in the Network Configuration Manager Settings. The account must at least have the WebUploader for the user make and upload configuration changes to network devices.
7. Click Submit.

Editing an Existing Account

1. From the web console, click Settings.
2. Under User Accounts, click Manage Accounts.
3. Select an account, and then click Edit.
4. Edit settings for the Orion individual account.
   - Decide if this account should have Administrator Rights and Node Management Rights.
   - Assign the appropriate NCM role in the Network Configuration Manager Settings. The account must at least have the WebUploader for the user make and upload configuration changes to network devices.

5. Click **Submit**.

### Deleting an Account

1. From the web console, click **Settings**.
2. Under User Accounts, click **Manage Accounts**.
3. Select an account, and then click **Delete**.

### Understanding Device Access

A SolarWinds NCM user logs on directly at the network device with unencrypted credentials and can perform actions the NCM role gives permission for.

If the network administrator wants to use the same credentials for SolarWinds NCM to log on to all network devices, the NCM software provides a Global Login and an option to enable global login settings on all devices. See [Setting Node Communication Defaults](#).

### Third Party Authentication

If a network administrator sets up third-party authentication, such as a Radius or TACACS server, the admin should create valid accounts and permissions in the authentication server database for appropriate SolarWinds NCM users.

**Note:** Only NCM interacts with network devices, not the authentication server. Though the network device must handle interaction with Radius, TACACS, or any other authentication server, special logic in the relevant NCM component (SWTelnet9) handles the RADIUS authentication prompt, since devices connected to the RADIUS server may have a slightly different logon flow.
Chapter 14: Understanding the Orion Web Console

The Orion Web Console, provided with SolarWinds Network Configuration Manager, offers access to your device configs without requiring physical access to your SolarWinds NCM server. You can perform the following actions, provided you have the appropriate role:

- View configurations
- Select configuration backup status
- Compare configurations and view differences
- Download configurations
- Upload configurations
- Execute scripts on nodes
- Create and manage config change templates

For more information:

- Launching and Logging On to Orion Web Console
- Understanding Orion Web Console Resources
- Personalizing the Web Console
- Integrating with Engineer's Toolset
Chapter 14: Understanding the Orion Web Console

Launching and Logging On to Orion Web Console

To launch the Orion Web Console, point a remote browser to the SolarWinds NCM server:

http://hostnameOrIPAddress:port

- `hostnameOrIPAddress` is the hostname or IP address of the SolarWinds NCM server.
- `port` is the Orion Web Console port defined for the website. The default is 8787.

To log on to the Orion Web Console, use Windows or SolarWinds NCM credentials. You must have previously defined the credentials using the user access control settings, and associated the credentials with the `WebViewer` role.

Understanding Orion Web Console Resources

Each view in the Orion Web Console provides several resources. The following sections are divided by the view on which the resources are displayed. You can customize your views, and add and remove resources based on the account you log on with. For more information about customizing your views, see Personalizing the Web Console.

For more information:

Home
All Active Alerts Resource
Config Summary
Node Details
Configuration Management
Config Change Templates
Reports
Compliance
Jobs
End of Support
Home displays the following resources:

**All Nodes**

Provides an expandable and customizable list of the nodes which have been added to SolarWinds NCM. Expanding groups, and then devices, allows you to reveal individual configurations.

**All Active Alerts**

Provides a list of all alerts that have been triggered but not acknowledged. Click on an alert for more details.

**All Active Alerts Resource**

If there are any alerts that have triggered involving the viewed node, or, if any device on the network triggers an alert if this resource is on the Network Summary Home view, they will display in the All Triggered Alerts resource. For each alert, this resource presents the date and time of the alert, the network device that triggered the alert, the current value of the alert if available, and a description of the alert.

**Config Summary**

From the web console, click CONFIGS > Config Summary. Config Summary displays the following resources:

**NCM Node List**

Displays a list of the nodes currently managed in NCM. (All NCM nodes must also be managed as an Orion node.)

**Search NCM**

Search configurations on all or some managed nodes for specific text.
If you specify All or a configuration search option, you can specify whether you want to search all downloaded configuration files or only the most recently downloaded configurations. You can also specify a date range and the type of configurations to search (running or startup). If you choose to specify the nodes to search, select the nodes you want to include in the search.

**Last 5 Config Changes**

Displays a list of detected configuration changes, including the node name and date and time of upload. Click **View Change Report** to see additions, deletions, and modifications.

**Overall Configuration Changes Snapshot**

Displays a pie chart representing the percentage of changed versus unchanged configurations over a specific period of time. To change the time period, click **Edit**.

**Overall Running vs. Startup Config Conflicts**

Displays a pie chart designating the percentage of devices running different configurations than their startup configurations.

**Overall Policy Report Violations**

Displays a stacked bar chart of devices statuses in relation to a specific policy report.

**Policy Violations**

Displays a list of the policy reports available and a brief overview of the contents of each report.

**Firmware Vulnerabilities**

Displays a list of firmware vulnerability warnings provided by National Institute of Standards and Technology (NIST), with indications of severity and correlation with any nodes NCM currently manages.

**Overall Baseline vs. Running Config Conflicts**

Displays a pie chart representing the percentage of baseline configs versus running config conflicts over a specific period of time.
Overall Devices Backed Up vs. Not Backed Up
Displays a pie chart representing the percentage of backed up devices versus devices which have not been backed up over a specific period of time. To change the time period, click Edit.

Overall Devices Backed Up vs. All Devices
Displays a pie chart designating the percentage of device that have been backed up using SolarWinds NCM in comparison to those that have not been backed up.

Overall Devices Inventoried vs. Not Inventoried
Displays a pie chart designating the percentage of devices inventoried in relation to those that have not.

NCM Events
Specify a time period and the configuration events you want to see displayed. To modify the time period, click Edit.

Node Details
Navigate to Node Details by clicking the name of a node in the SolarWinds NCM Web Console. Node Details displays the following resources:

Node Details
Displays an overview of the device you selected, including the IP Address, OS Version, Location, OS image, among other information.

Config List
Displays a list of the last X number of configurations downloaded from this device.

Download Config
Download the startup or running configuration from the current node.

Execute Script
Execute a script against the current node.

Upload Config
Upload a configuration file you have previously downloaded from the selected node.
Chapter 14: Understanding the Orion Web Console

Inventory Details
Displays a list of inventory reports that pertain to the selected device.

Policy Violations
Displays a list of the policy reports available that pertain to the selected device.

Last 10 Config Changes
Displays a list of detected configuration changes, listing the user committing the change, the time of upload, and the type of configuration.

Compare Configurations
Select two configurations from different time periods to compare to each other.

Config Change Report
Specify a time period and a node, and then display a change report that covers the set time range.

NCM Events
Specify a time period and the configuration events you want to see displayed. To modify the time period, click Edit.

Configuration Management
Configuration Management displays the following resources:

Download
Download running, startup, or custom configurations for the selected nodes.

Compare noes(s) configs
Select two configurations to compare to each other. You can select configurations from the same device archived at different times, a startup versus a running configuration, or configurations from different devices.

Run config change report
Specify a time period and a node, and then display a change report that covers the set time range.

Note: Consult this Knowledge Base article for special setup needed to ensure the accuracy of Config Change Reports based on a date range.
Upload
Select a configuration to upload to one or more nodes.

Execute Script
Enter or load a script from a text file to execute against the selected nodes.

Transfer Status
Displays the most recent actions taken on a node.

Config Change Templates
Config Change Templates displays the following resources:

Config Change Templates
Create, edit, import, export, tag, and delete config change templates.

Shared Config Change Templates on thwack
View and download config change templates from thwack.

Reports
Reports displays the supplied inventory reports and those you created with SolarWinds NCM. SolarWinds NCM provides over 40 unique inventory reports and allows you to create your own. For more information, see Managing Inventory Reports.

Compliance
Compliance displays the supplied policy reports and those you created with SolarWinds NCM. SolarWinds NCM provides several policy compliance tests, and allows you to create your own. To ensure you are viewing the latest information, click Update All.

Jobs
Jobs displays the supplied inventory reports and those you created. SolarWinds NCM provides 40 unique inventory reports and allows you to create your own. For more information, see Creating or Editing a Job.

End of Support
End of Support tracks the end of support and sales statuses of your NCM nodes. For more information, see Managing End of Support and End of Sales (EOS)
Chapter 14: Understanding the Orion Web Console

Searching

The Advanced Search function searches node properties, specific node configurations, all node configurations, and only the most recent downloaded configurations for specific text. You can also search within your search results.

1. From the web console, click **CONFIGS > Config Summary**.
2. Under Search NCM, click **Advanced Search**.

Personalizing the Web Console

On Config Summary, click **Customize Page**.

You can then select the resources to include, drag-and-drop them from one column to another, or drag-and-drop them in a different order in the same column. Changes are saved as preferences associated with the logged on user account. For more information about user accounts and roles, see [Managing Web Accounts](#).

Integrating with Engineer's Toolset

Under Node Details, if you have Engineer's Toolset installed on the local computer, you can take advantage of the following integrations:

- Web browse to the selected node
- Telnet to the selected node
- Ping the selected node
- Run a trace route to the selected node
- Remote desktop to the selected node
Chapter 15: Integrating NCM Actions into Orion Alerts

Orion alerting software can alert on polled, syslog, and trap data. Alerts are defined in terms of thresholds related to data in the Orion database. Scans in the form of SQL queries at set intervals detect recorded values that exceed thresholds, triggering an alert if relevant conditions pertain.

When an Orion alert is triggered, the software evaluates suppression criteria. If an alert is not qualified to be suppressed, the software executes a defined action. If no action is defined, the software merely displays the alert on the web console.

Throughout this workflow, timers are used to allow the software to do its work at each step and to ensure that the alerting workflow had appropriate redundancy for timely reporting of alerts.

For more information:

Types of NCM Alert Actions
Using the Default NCM Alert
Adding Scripted Commands to the Default NCM Alert
Creating New Alerts
Available Alert Actions
Setting Trigger Conditions
Setting Reset Conditions
Setting the Time of Day or Schedule
Setting Trigger Actions & Escalation Levels
Setting Reset Actions
Acknowledging Advanced Alerts in the Web Console
Types of NCM Alert Actions

In executing one of its alert-related actions, NCM requires an NCM role with sufficient permissions and cannot use device access credentials to authorize its action.

**Note:** As a security enhancement related to executing NCM actions, NCM account passwords are not stored in the database. As part of configuring NCM 7.4, the installation software removes passwords from the database as part of the Configuration Wizard session.

Sequence the actions with an awareness that some NCM actions require others to complete first. For example, NCM cannot execute a notification email action before it downloads the config from an NCM managed device.

You can use three types of NCM actions in processing an Orion advanced alert:

- Backup Running Config
- Execute Config Script
- Show Last Config Changes

**Backup Running Config**

NCM downloads the latest configuration from the context node. It is the same as running **Node Details > Configs > Download Config**. Unlike a normal execution of this action, however, the results of this download are written to an alerts table in the Orion database and this data is used when an alert is processed.

**Execute Config Script**

NCM executes the command(s) that you entered in the **Command Script to Execute** field. For example, if you enter `show version`, and include it as a Trigger Action on an alert, NCM runs the `show` command as part of alert processing and includes the results with the alert notification.

**Show Last Config Changes**

NCM performs a SQL query to find the most recent changes and compares those changes either to the baseline config or the next-to-last downloaded config, depending on how you set up your alert action.
When the alert triggers, the results of the NCM action are stored in the Orion database (in ${Notes}) and used as part of runtime processing of an alert. You can also view this information as part of the Alert Details on any relevant alert reported through the Orion Web Console (Home > Alerts). For detailed information, see Viewing Alerts in the Orion Web Console.

If an alert is triggered for a node without relevant config history, NCM cannot contribute any data and the Orion alert is processed without it. So selecting this action only makes sense if you already have a history of device configurations.

**Using the Default NCM Alert**

When you install SolarWinds NCM, the software automatically creates a predefined alert called *Alert me and trigger an NCM action* in the Orion Alert Manager.

By default, if changes is device configuration trigger it, this predefined alert does these three things in order:

- Backs up the running config on the alerting device.
- Determines the last config changes made on the device.
- Sends an email regarding the alert to a relevant administrator that includes the results of both NCM actions.

**To use the default NCM alert:**

1. From the web console, click HOME > Alerts.
2. Click Manage Alerts.
3. Select Group by > Object Type, and then select Node.
4. Select Alert me and trigger an NCM action.
5. *If you want to edit the configuration*, click Edit Alert.
6. *If you want to make a copy of the alert before editing it*, click Duplicate & Edit.
7. Edit the Alert Properties, and then set Enable On/Off to On.
8. On Trigger Condition, define the conditions in which the software launches the alert. The default conditions are any node in the NCM environment that responds in 200 ms or more.
9. On Reset Condition, define the conditions in which the software resets the alert. The default condition is that the triggered nodes respond in 100 ms or less.

10. On Time of Day, define the days and times during which the software actively evaluates the database for trigger conditions. The default range is 24/7.

11. On Trigger Actions, create actions to execute when the software triggers the alert, and then enter your NCM credentials.

12. On Reset Conditions, define actions to execute when the software resets the alert. Default actions are to back up the config running on the alerting device, determine the last config changes, and send an email to an appropriate contact. For other available NCM actions, see Types of NCM Alert Actions.

13. On Reset Actions, create actions to execute when the resets the alert, and then click Next. By default, resetting an alert sends an email notification.

14. On Summary, review and edit settings. We recommend enabling Alert Integration.

15. Click Submit.

Adding Scripted Commands to the Default NCM Alert

You can modify the default NCM advanced alert to execute specific command scripts at the time the alert is triggered. The following example adds a simple `show version` command as a scripted action.

1. From the web console, click HOME > Alerts.
2. Click Manage Alerts.
3. Select Group by > Object Type, and then select Node.
4. Select Alert me and trigger an NCM action.
5. Click Duplicate & Edit.
7. Select Execute an NCM action, and then click Configure Action.
8. Select **Execute Config Script**, and then enter the relevant command in **Command Script to Execute**. For example:
   
   ```
   show version
   ```
   
   When executed, this command runs on the context node, receives detailed software and hardware information, and includes it in the `$\{Notes\}` macro of an Orion database alerts table.

9. Click **Add Action**.

10. Drag the new action into the desired position in the list.

   By default, the software positions a new action at the end of the action list. In this case, it makes sense to position this action third, after NCM backs up the running config and determines the last config changes.

11. Click **Summary**.

12. On Summary, review and edit settings. We recommend enabling Alert Integration.

13. Click **Submit**.

---

**Navigating to the Alert Manager**

Use the Alert Manager to create, edit, delete, enable, or disable alerts. You can access the Alert Manager in one of four ways:

- **Settings Page (Recommended)**
  - Click **Settings**. Under Alerts & Reports, click **Manage Alerts**.

- **Active Alerts Details**
  - From the Active Alerts Details page, click **Manage Alerts** in the Management resource.

- **All Active Alerts Resource**
  - From the All Active Alerts resource, click **Manage Alerts** in the right side.

- **Node Details**
  - On the Node Details page, navigate to the **All Alerts this Object can trigger** resource, and then click **Manage Alerts**.
Available Alert Actions

Orion Platform products provide a variety of actions to signal an alert condition on your network. For information on configuring each action, refer to the following list.

The following actions are available:

Alert Preconfiguration Tasks

Some alerts require extra configuration, separate software installations, or specific information input.

Alert actions that require set up before creating or configuring alerts include:

- Sending an Email/Page
- Dialing Paging or SMS Service
- Playing a Sound
- Sending an SNMP Trap
  - Using Text to Speech Output

Note: Make sure there are monitored objects in the Orion Platform database before creating or configuring alerts. Monitored objects can include items such as nodes, databases, and applications.

Adding an SMTP Server

You must add and configure a designated SMTP server if you want to complete an email action with any SolarWinds Orion Platform product.

To add an SMTP server in the Orion Web Console:

1. Log in to the Orion Web Console using an account with administrative privileges.
2. Click Settings in the top right corner of the web console.
3. In the Reports and Alerts grouping, click Manage SMTP Servers.
4. Click Add SMTP Server.
5. Provide the Hostname or IP Address of your SMTP Server and the designated SMTP Port Number.

Note: The SMTP server hostname or IP address field is required. You cannot send an email without identifying the SMTP server.
6. *If you want to use SSL encryption for your alert email*, check *Use SSL*.  
   **Note:** Opting to use SSL automatically changes the SMTP port number to 465.

7. *If your SMTP server requires authentication*, check *This SMTP Server requires Authentication*, and then provide requested credentials.

8. Click *Save*.

**Creating and Configuring Advanced Alerts**

SolarWinds NCM allows you to configure advanced alerts with the following features:

- Sustained state trigger and reset conditions
- Multiple condition matching
- Automatic alert escalation
- Separate actions for triggers and resets

Configure alerts with the Manage Alerts resource: **HOME > Alerts > Manage Alerts**.

**For more information:**

- [Creating New Alerts](#)
- [Alert Preconfiguration Tasks](#)
- [Available Alert Actions](#)
- [Setting Trigger Conditions](#)
- [Setting Reset Conditions](#)
- [Setting the Time of Day or Schedule](#)
- [Setting Trigger Actions & Escalation Levels](#)
- [Setting Reset Actions](#)
- [Navigating to the Alert Manager](#)
- [Viewing Alerts in the Orion Web Console](#)
- [Acknowledging Advanced Alerts in the Web Console](#)
Chapter 15: Integrating NCM Actions into Orion Alerts

Creating New Alerts

SolarWinds NCM provides an Alert Wizard to guide you through creating or editing alerts.

To create a new alert definition, Navigating to the Alert Manager, and then click Add New Alert.

You can also select an alert that is similar to the alert you want to create and then click Duplicate & Edit.

There are seven tabs on the Add New Alert screen:

- **Properties**
- **Trigger Condition**
- **Reset Condition**
- **Time of Day**
- **Trigger Actions**
- **Reset Actions**
- **Summary**

When creating a new alert, you must fill out required information on each tab before proceeding to the next tab.

**Note:** You can skip to different steps if you clicked Duplicate & Edit or if you are editing a saved alert.

Best Practices and Tips for Alerting

Use the following best practices and tips to help you configure and test your alerts.

Use the Out of the Box Alerts as Templates

SolarWinds recommends using the alerts that are included when you install the product as templates for your new alerts.

Find an alert that is similar to one you want to create and then click Duplicate & Edit. Fields are pre-populated, allowing you to skip to specific parts of the Alert Wizard where there is data you want to change.
Restrict Who Receives Alerts

During your initial evaluation and testing, send alerts to a few people instead of to a large distribution list. This can prevent overloading your email server while you fine-tune your alerts.

Plan which Devices to Monitor

To reduce the number of alerts sent out, consider which devices are most important. For example, you may want to receive alerts only for mission critical interfaces instead of every interface on a device.

Establish Dependencies

Establish dependencies to prevent you from receiving duplicate alerts that stem from a single network event. For example, you may want to be emailed if servers in your server farm go down, but if the router goes down and the servers can no longer be polled, you do not want to receive notifications for all of your servers.

Setting Alert Properties

After creating a new alert, use the Alert Properties to describe the alert, including which users can view the alert.

Enter the following information as necessary:

Name of alert definition

This is a required field. SolarWinds recommends a name that describes the condition and most visible alert action. For example, you can use "Email NetAdmins when router goes down" as the name of an alert. The name is displayed in the Alert Manager and can be used to sort your alerts. If you intend to create a large number of alerts, consider a naming convention that allows you to quickly scan through the Alert Manager.

Description of alert definition

Describe the alert. This is displayed on the Manage Alerts page, so important information should be near the front.

Enabled (On/Off)

Choose to evaluate the alert immediately after it is created and saved. The alert is enabled. If you are in the process of refining your alert, you may want to disable this alert until it is ready for use.
Chapter 15: Integrating NCM Actions into Orion Alerts

Evaluation Frequency
Set how frequently you want to evaluate the conditions. SolarWinds recommends using intervals longer than 1 minute to evaluate alert conditions. Shorter frequencies can put an undue burden on your network performance or computing resources.

If you elect to alert on an event, such as a changed IP address, the condition is not evaluated by frequency, but by when the change is reported based on the polling interval.

Severity of Alert
Control the appearance of the alert in the Active Alerts resource and group or filter alerts more easily.

Alert Custom Properties
Organize your alerts. For example, you can create a "Responsible Team" custom property and use it to help audit who receives specific alerts. You must create a custom property for alerts before you can assign a custom property to an alert.

Alert Limitation Category
Restrict who can view the alerts. For example, managed service providers can restrict alerts to their specific customers. If you create a new limitation, go to Settings > Users and add the new limitation to the appropriate user accounts.

Setting Trigger Conditions
Set a trigger condition to define what event must occur to activate your alert. Trigger conditions can be as simple as a node going down or as complex as multiple SQL statements.

Note: While SolarWinds provides a method to create SQL conditions manually, SolarWinds support is not provided. Visit thwack, SolarWinds' community website, for support from other users.

The trigger condition is the most complex step in creating an alert. Before you begin, you may want to revisit the Best Practices and Tips for Alerting topic.

Trigger conditions are built using child conditions that are evaluated in order. Child conditions are represented as a line item under the Actual Trigger Condition. You can have multiple trigger condition blocks with multiple child conditions.
To set trigger conditions:

1. Choose the objects to monitor in the **I want to alert on field**.
2. Establish how much of your environment to monitor in **The scope of alert**.
   You can monitor all objects in your environment or filter your environment to a specific set of objects.
3. Create your trigger condition.
   a. Choose if the child conditions must be true or false to trigger the alert.
      - **All child conditions must be satisfied (AND)** - Every child condition must be met
      - **At least one child condition must be satisfied (OR)** - At least one child condition must be true
      - **All child conditions must NOT be satisfied** - Every child condition must be false
      - **At least one child condition must NOT be satisfied** - At least one child condition must be false
   b. Click the + sign to add child conditions.
      - **Add Single Value Comparison (Recommended)** - The child condition evaluates a single field, like Status
      - **Add Double Value Comparison** - The child condition evaluates two conditions, such as Status and OS
      - **Add And/Or block** - Adds a sub condition block
      Tip: Use the X at the end of each child condition to delete it, or use the drop-down at the top of the block to delete the entire condition.
   c. Select the object you want the child condition to evaluate, and then select which field you want to evaluate. In the example screenshot, the object is "Node" and the field is "Status".
      Tip: You can evaluate objects based on variables or macros.
   d. Select how you want to compare the polled value of the field to the value entered here, and then enter the value. In the example screenshot, the comparison is "is equal to" and the value is "Down".
e. To use more complex conditions, such as evaluating when an application on a specific server is down and different application on another server is down, enable complex conditions under Advanced options. See Building Complex Conditions for more information, or visit thwack, SolarWinds' community website, for support from other users.

f. Choose how long the condition must exist before an alert is triggered. This prevents receiving alerts when the alert condition, such as high CPU utilization, occurs briefly or only once during a certain time period.

- To immediately send an alert when the condition is met, clear any selection for Condition must exist for more than.
- To wait before sending an alert, select Condition must exist for more than, and enter how long the condition must exist. This option prevents multiple alerts firing if the condition is temporary.

### Setting Reset Conditions

Use the reset condition to define what must occur to remove an alert instance from the active alerts list. For example, the "Email me when a Node goes down" alert automatically resets when the node comes back up. You can use the built-in reset conditions or create your own.

Reset conditions remove alerts from Active Alerts. You can also create reset actions that occur when the reset conditions are met.

For example, you can create an alert that triggers when nodes in your lab go down. If node 192.168.4.32 goes down, the alert fires for that specific instance of the trigger condition and any escalation levels you create continue until you reset the alert. After the alert is reset, all trigger actions stop and a new alert fires the next time node 192.168.4.32 goes down. If you have created reset actions, the reset actions fire.

**Note:** When the alert is reset, escalation actions are halted.

Select one of the following reset conditions:
Setting Reset Conditions

- **Reset this alert when trigger condition is no longer true (Recommended)**
  
  SolarWinds recommends using this reset condition. If the trigger condition is no longer true when the objects are next polled, this selection automatically resets the alert.

  You can use the **Condition must exist for more than** option in the trigger conditions in conjunction with this reset condition. Trigger conditions that involve volatile components, such as high CPU utilization, can trigger excessively with this reset condition.

- **Reset this alert automatically after**
  
  Select to reset an alert after a set amount of time has passed. If this interval is less than the amount of time you wait for different escalation levels, the escalation levels that occur after this interval do not fire. This reset condition is especially useful to remove event-based alerts from Active Alerts.

  For example, if the trigger conditions still exists after 48 hours, you can use this to trigger your alert actions again. The alert is reset and triggers as soon as the trigger condition is detected, which is as soon as the objects are polled for this example.

- **No reset condition - Trigger this alert each time the trigger condition is met**
  
  The alert fires each time the trigger conditions are met.

  For example, when the alert for node 192.168.4.32 going down fires, a new alert for 192.168.4.32 fires every time the node is down when it is polled.

- **No reset condition**
  
  The alert is active and is never reset. To re-trigger the alert, the alert must be manually cleared from the Active Alerts view.
Chapter 15: Integrating NCM Actions into Orion Alerts

- **Create a special reset condition for this alert**
  Select to build a specific reset condition.
  For example, you can choose to reset the condition when the node has been up for more than 10 minutes.
  See *[Setting Trigger Conditions](#)* or *[Building Complex Conditions](#)* for more information on creating conditions.

**Alert Suppression Example**

A typical usage of alert suppression would be the case where you do not want to trigger a specific alert when a main router is down. In this case, the suppression condition is configured as, "MyMainRouter has Status equals Down". If MyMainRouter is really down, then any alerts to which this suppression condition has been applied, regardless of what or where the monitored object is, will not trigger, as long as MyMainRouter remains down.

**Warning:** Be careful to avoid mismatching alert trigger and suppression conditions, as it is possible for a poorly stated suppression condition on a single monitored object to disable alert triggers for all net objects. The following conditions provide an example of such a case:

**Alert trigger condition:** Node Response Time is greater than 100 ms

**Alert suppression condition:** Node Location is not equal to "Austin"

This combination of conditions will NOT have the result of triggering alerts for all Nodes located in Austin having a response time greater than 100 ms. This combination of conditions WILL, however, only trigger alerts for any nodes showing a response time greater than 100 ms alert if all monitored nodes are located in Austin. If there is at least one node with a location other than Austin, the alert will be suppressed for all nodes, including the ones that are actually located in Austin.

**Building Complex Conditions**

Complex conditions are generally enabled by users who are comfortable with building normal trigger conditions or who have trialed alerts using the normal trigger conditions and require more control over the trigger conditions to better refine the environmental conditions that trigger an alert.
Important: Do not use complex conditions until you have tested the trigger conditions individually. Creating an alert with complex conditions without testing it may prevent you from receiving important alerts.

To enable complex conditions:

1. Navigate to the Trigger Condition page.
2. Expand Advanced options.
3. Select Enable complex conditions.

Setting the Time of Day or Schedule

You can configure when an alert monitors your network. By default, alerts monitor your network for changes all the time. Schedule when you want to monitor your network for the trigger conditions you created for the alert. You can create multiple schedules that control when an alert is enabled or disabled. For example, you can disable an alert during maintenance windows.

Note: Alerts must be enabled to allow schedules to run.

To schedule your alert:

1. Select Specify time of day schedule for this alert
2. Click Add Schedule.

You can have multiple schedules for a single alert. For example, you can schedule the alert to monitor your network during off hours, and disable the alert during your maintenance windows.

Enter the following information to schedule a monitoring period:

- **Schedule Name**
  This is not required, but may help you organize or troubleshoot your schedules. If you do not enter a name, a name is automatically generated from the time period.

- **Enable or Disable alert during following time period**
  If you choose to disable the alert, it is enabled all other times unless otherwise scheduled.
Chapter 15: Integrating NCM Actions into Orion Alerts

- **Frequency**
  Choose when to monitor on a high level, such as daily, weekly, or monthly.

- **Enable every**
  These options change based on the frequency.

  - *If you selected Daily...*
    You can choose to enable or disable the alert every few days, up to every 31 days. You can also select specific business days. For example, you may want to disable network or disk activity alerts if you run daily, off-site backups of your critical data.

    - **Enter a time period**
      - To monitor or not for the entire 24 hour period, select **All Day**.
      - To monitor or not during a specific time period during the day, enter a time and click **Add Time Period**.

      To monitor or not for a time period that spans midnight enter a time in the **From** field that is later in the day than the time in the **To** field. For example, to schedule an alert between 11PM to 3AM, enter 11PM (or 23:00) in the **From** field and 3AM (or 3:00) in the **To** field.

  - *If you selected Weekly...*
    Choose which days the alert is enabled or disabled. You may want to disable alerts during a weekly maintenance window.

    - **Enter a time period**
      - To monitor or not for the entire 24 hour period, select **All Day**.
      - To monitor or not during a specific time period during the day, enter a time and click **Add Time Period**.
To monitor or not for a time period that spans midnight enter a time in the From field that is later in the day than the time in the To field. For example, to schedule an alert between 11PM to 3AM, enter 11PM (or 23:00) in the From field and 3AM (or 3:00) in the To field.

If you selected Monthly...

Choose which months the alert is enabled or disabled. This option is useful when you have quarterly or monthly maintenance windows. Choose either a specific date or a day.

Enter a time period

To monitor or not for the entire 24 hour period, select All Day.

To monitor or not during a specific time period during the day, enter a time and click Add Time Period.

To monitor or not for a time period that spans midnight enter a time in the From field that is later in the day than the time in the To field. For example, to schedule an alert between 11PM to 3AM, enter 11PM (or 23:00) in the From field and 3AM (or 3:00) in the To field.

Starting on

Choose a date to being the schedule.

- Right now - Start the schedule immediately.

- Specific Date - Select a time and day to begin the schedule.

Ending on

Choose and end date for the schedule, if necessary.

3. Click Add Schedule to create the schedule.
Chapter 15: Integrating NCM Actions into Orion Alerts

Setting Trigger Actions & Escalation Levels

Use trigger actions to define what happens when trigger conditions are met. By default, a triggered alert creates an entry in the Active Alerts resource with a configurable message. All other trigger actions, such as Send an Email/Page or Write to a Log, must be configured.

You can also set up escalations levels so the alert triggers different actions if it has not been acknowledged quickly enough.

Trigger Actions

By default, what you enter into the Message displayed when this alert is triggered field is displayed in the All Active Alerts resource.

To add a trigger action:

1. Click Add Action.

2. Select an action from the list.
   See Alert Trigger Actions for a complete list of available actions.

3. Click Configure Action.

4. Enter the necessary information for the action.

   Each action requires different information. Select from the list of Alert Trigger Actions for more information per action.

   Some actions require extra configuration steps, specific information, or special software. See Preconfiguration Tasks.

   Each action has the following sections:

   - **Name of action** - This is not required, but can make it easier to organize your Trigger actions.

   - **Time of Day**... - You can choose different actions to occur at different times of the day or month. For example, if you want to send a page, you might send it to a different person on weekends or holidays than during the week.
Execution settings - You can select both options, neither option, or a single option.

- Do not execute this action if the alert has been acknowledged already (Recommended)
- Repeat this action every X minutes until the alert is acknowledged

5. Click **Add Action**.

**Escalation Levels**

Escalation levels in SolarWinds NCM refer to user-defined time intervals between when an alert is activated and when a user acknowledges that alert. You can configure the alert to perform different actions per escalation level.

Escalation Level 1 contains all initial actions that you want to occur when the trigger conditions are met and the alert activates.

Escalation Levels 2 and above include all actions you want to occur if no one acknowledged the alert during the previous escalation levels.

For example, if an alert for a critical server activates and all of the recipient or first-level responders are out for training and do not acknowledge the alert, then the actions fire in the second escalation level. These actions may include emailing managers or other backup staff.

**To escalate alerts:**

1. In an existing alert, click **Trigger Actions**.
2. Below the action, click **Add Escalation Level**.
3. Choose how long you want to wait after the previous escalation level before performing the actions in the new escalation level.
4. Enter new actions in this escalation level.

You can copy all of the actions as Reset Actions to record that the issue has been acknowledged or resolved. Click **Copy Actions to Reset Actions Tab**.
Chapter 15: Integrating NCM Actions into Orion Alerts

Setting Reset Actions

Use reset actions to perform specific tasks when an alert is no longer active, such as writing to the log that the issue has been acknowledged. Reset actions are usually used to notify others that the situation has been resolved or to write the resolution to a log file.

Choose actions that occur when the reset conditions are met and the alert is no longer active.

To add a reset action:

1. Click Add Action.
2. Select an action from the list.
   See Alert Actions for a complete list of available actions.
3. Click Configure Action.
4. Enter the necessary information for the action.
   Each action requires different information.
   Some actions require extra configuration steps, specific information, or special software. See Preconfiguration Tasks.
   Each action has the following sections:

   - **Name of action** - This is not required, but can make it easier to organize your Trigger actions.

   - **Time of Day** - You can choose different actions to occur at different times of the day or month. For example, if you want to send a page, you might send it to a different person on weekends or holidays than during the week.

   - **Execution settings** - You can select both options, neither option, or a single option.
     - Do not execute this action if the alert has been acknowledged already (Recommended)
     - Repeat this action every X minutes until the alert is acknowledged

5. Click Add Action.
To perform the same actions as when the alert was triggered, click **Copy Actions From Trigger Actions Tab**. Use the copied trigger actions as a base and modify them to reflect that the alert is no longer active.

**Escalating Alerts**

Escalation levels in Orion platform products refer to user-defined time intervals between when an alert is activated and when a user acknowledges that alert. You can configure the alert to perform different actions per escalation level.

Escalation Level 1 contains all initial actions that you want to occur when the trigger conditions are met and the alert activates.

Escalation Levels 2 and above include all actions you want to occur if no one acknowledged the alert during the previous escalation levels.

For example, if an alert for a critical server activates and all of the recipient or first-level responders are out for training and do not acknowledge the alert, then the actions fire in the second escalation level. These actions may include emailing managers or other backup staff.

**To escalate alerts:**

1. In an existing alert, click **Trigger Actions**.
2. Below the action, click **Add Escalation Level**.
3. Choose how long you want to wait after the previous escalation level before performing the actions in the new escalation level.
4. Enter new actions in this escalation level.
5. After you have completed added escalation levels and actions, click **Next** to configure the reset actions or click **Summary** to review your changes and save them.

You can copy all of the actions as Reset Actions to record that the issue has been acknowledged or resolved. Click **Copy Actions to Reset Actions Tab**.

**Adding Alert Actions**

SolarWinds Network Configuration Manager provides a variety of actions to signal an alert condition on your network. These alert actions are available for both basic and advanced alerts, and the following procedure assigns actions to the alert conditions that you have defined for your network.
Chapter 15: Integrating NCM Actions into Orion Alerts

1. Click **Start > All Programs > SolarWinds > Network Performance monitor > System Manager**.
2. Click **Alerts > Active Alerts**, and then click either **Configure Basic Alerts** or **Configure Advanced Alerts**, as appropriate.
3. Check the alert to which you want to add the action, and then click **Edit Alert**.
4. Click **Actions**, and then select the action you want to edit.
5. Click **Add Alert Action**, and then click the action to add to your chosen alert.

For more information about individual alert actions, see the SolarWinds Orion Common Components Administrator's Guide.

**Available Alert Actions**

The following sections detail the configuration of available alert actions:

- **Sending an Email/Page**
- **Playing a Sound**
- **Using Text to Speech Output**
- **Logging an Advanced Alert to a File**
- **Dialing Paging or SMS Service**
- **Logging an Alert to the Windows Event Log**
- **Logging an Alert to the Event Log**
- **Sending a Syslog Message**
- **Executing an External Program**
- **Emailing a Web Page**
- **Sending a Windows Net Message**
- **Sending an SNMP Trap**
- **Using Get or Post URL Functions**

**Sending an Email/Page**

This action sends an email from the product to a selected recipient.
IMPORTANT: Before configuring this alert you must first configure the default SMTP server the product uses to send email. You can change the default SMTP server later or use different SMTP servers for specific alerts.

Configure the SMTP server in the alert action or from the Settings page. You need the following information:

- The SMTP host name or IP address
- The SMTP port number
- Whether the SMTP server uses SSL
- The SMTP credentials, if necessary
- Default sender email address

For more instructions about configuring the SMTP server, see Adding an SMTP Server.

The following procedure configures an email/page action for an alert.

To configure an email/page action for an alert:

1. When editing or adding an alert, click Add Action in an Action section of the Alert Wizard.
2. Select the Send an Email/Page option, then click Configure Action.
3. Enter a name for the action in the Name of Action field.
4. Under Recipients:
   a. Complete the To, CC, and BCC fields.
   b. You can optionally edit sender details by expanding [+Sender Details] and editing the Name of Sender and the Reply Address.
      Note: You must provide at least one email address in the To field, and multiple addresses must be separated with commas. Some pager systems require a valid reply address to complete the page.
5. Expand Message.
   a. Select the format (Plain text or HTML) for your alert email.
   b. Enter the Subject and Message of your alert trigger email/page.
      Note: Messaging is disabled if both the Subject and Message fields are empty.
c. Optionally click **Insert Variable** to add variables using the following procedure:
   i. Select a **Variable Category**, and then select the variable to add.
   ii. To define a SQL variable, check **Define SQL Variable**.
   iii. Click [+] next to the name of a variable to add one or more variables to the **Custom SQL Variable** window.
   iv. When done, click **Insert Variable**.

6. Expand **SMTP Server**.
   a. Enter the Name of the **SMTP Server**.
   b. Enter the **Hostname or IP Address of your SMTP Server** and the designated **SMTP Port Number**.
   **Note:** The SMTP server hostname or IP address field is required. You cannot send an email/page alert without identifying the SMTP server.
   c. To use SSL/TLS encryption for your alert email, check **Use SSL**.
   d. If your SMTP server requires authentication, check **This SMTP Server requires Authentication**.
   e. Choose a **Secondary SMTP Server** from the list, if desired.

7. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule.
   a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

8. Expand **Execution Settings**.
   a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.

9. When done, click **Add Action**.
Playing a Sound

The Play a Sound action uses the default sound player SolarWinds Desktop Notification client to play the sound on your computer when an alert arrives.

You must download and install the client on every computer that you want to play a sound when an alert arrives. After installing the desktop notification client, configure which sound you want to play when an alert is received.

Computers that do not have the desktop notification client installed on them do not play a sound when an alert arrives. If you want an alert notification sound to play on your desktop or laptop, you must install and configure the desktop notification client on that computer.

Download the desktop notification client from <Your SolarWinds Orion server>/DesktopNotificationTool/SolarWinds.DesktopNotificationTool.msi. Run the installer and follow the on-screen instructions to install the client.

The desktop notification client requires the following information to connect to your SolarWinds Orion server and receive alerts:

- Orion Server Name or IP Address
- Orion User Name
- Password

You can use the server name and credentials that you use to logon to your SolarWinds product.

SolarWinds can be configured to play a sound upon alert trigger or reset. This alert action is frequently used in NOC environments. The SolarWinds Desktop Notification client must be installed on each computer that you want to play a sound. The following procedure configures a sound to play for an alert.

**To configure a play sound action for an alert:**

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Play a Sound** option, and then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Play a sound settings**: 
   
a. If not installed, click **Download our desktop notification client** to download and install the notification client. 
   
i. From the notification client, select an alert sound. 

b. Optionally click **Insert Variable** to insert variables into the message body: 
   
i. Select a **Variable Category**, and then select the variable to add. 
   
ii. To define a SQL variable, check **Define SQL Variable**. 
   
iii. Click [+] next to the name of a variable to add one or more variables to the **Custom SQL Variable** window. 
   
iv. When done, click **Insert Variable**. 

5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule. 
   
a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action. 

6. Expand **Execution Settings**. 
   
a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated. 

7. When done, click **Add Action**. 

**Logging an Advanced Alert to a File** 

Orion can be configured to log alerts to a designated file. The following procedure logs an advanced alert to a designated file.
To configure a log-the-alert-to-a-file action:

2. Click Log the Alert to a File, and then click Configure Action.
3. Name the action.
4. Enter a maximum file size, as needed.
5. Enter a message, using variables as needed.
6. Click Time of Day on Trigger Actions in the Alert Wizard and do one of two things.
   - Accept the default (Schedule is controlled on the alert level, no additional schedule for this action needed).
   - Use Add Schedule to setup constraints for when to play the sound.
7. Enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
8. Click Execution Settings
9. To disable the action when the alert has been acknowledged, check Do not execute this Action if the Alert has been Acknowledged.
10. To execute the action repeatedly as long as the trigger condition exists, check Execute this Action repeatedly while the Alert is Triggered and then provide an appropriate action execution interval.
11. Click Add Action.

Logging an Alert to the Windows Event Log

You may specify that an alert be logged to the Windows Event Log either on the SolarWinds server or on a remote server. The following procedure logs an alert to the Windows Event Log on a designated server.

To configure alert logging to the Windows Event Log:

1. When editing or adding an alert, click Add Action in an Action section of the Alert Wizard.
2. Select the Windows Event Log option, then click Configure Action.
3. Enter a name for the action in the Name of Action field.
Chapter 15: Integrating NCM Actions into Orion Alerts

4. Under **Event Log Settings**:
   a. Select either **Use Event Log Message on Network Performance Monitor Server** or **Use Event Log Message on a Remote Server**. **Note**: If the latter option is selected, enter the **Remote Server Name or IP Address** in the field provided.
   b. Enter the **Message** of your alert trigger.
   c. Optionally click **Insert Variable** to add variables using the following procedure:
      i. Select a **Variable Category**, and then select the variable to add.
      ii. To define a SQL variable, check **Define SQL Variable**.
      iii. Click [+] next to the name of a variable to add one or more variables to the **Custom SQL Variable** window.
      iv. When done, click **Insert Variable**.

5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.
   a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

6. Expand **Execution Settings**.
   a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.

7. When done, click **Add Action**.

**Logging an Alert to the Event Log**

You can specify that an alert should be logged to the NetPerfMon (NPM) Event Log either on the NCM or on a remote server. The following procedure logs an alert to the NPM Event Log on a designated server.
To configure alert logging to the NetPerfMon Event Log:

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Log the Alert to the NetPerfMon Event Log** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Log the Alert to the NetPerfMon Event Log settings**:
   a. Enter the **Message** of your alert trigger in the field provided.
   b. Optionally click **Insert Variable** to add variables using the following procedure:
      i. Select a **Variable Category**, and then select the variable to add.
      ii. To define a SQL variable, check **Define SQL Variable**.
      iii. Click [+ ] next to the name of the variable to add one or more variables to the **Custom SQL Variable** window.
      iv. When done, click **Insert Variable**.
5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.
   a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
6. Expand **Execution Settings**.
   a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
7. When done, click **Add Action**.
Chapter 15: Integrating NCM Actions into Orion Alerts

Sending a Syslog Message

SolarWinds can log received alerts to the Syslog of a designated machine. The following procedure configures an alert to send a message to a designated Syslog server.

To configure an alert to send a Syslog message:

1. When editing or adding an alert, click Add Action in an Action section of the Alert Wizard.
2. Select the Send a SysLog Message option, then click Configure Action.
3. Enter a name for the action in the Name of Action field.
4. Under Send a SysLog message settings:
   a. Enter the Hostname or IP Address of the Syslog Server in the field provided.
      Note: Multiple Syslog servers should be separated by commas.
   b. Select a Severity and a Facility from the drop down lists.
5. Enter the Message of your alert trigger in the field provided.
   a. Optionally click Insert Variable to add variables using the following procedure:
      i. Select a Variable Category, and then select the variable to add.
      ii. To define a SQL variable, check Define SQL Variable.
      iii. Click [+] to add one or more variables to the Custom SQL Variable window.
      iv. When done, click Insert Variable.
6. Expand Time of Day. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.
   a. Select either Schedule is controlled on the alert level, no additional schedule for this action needed or Use special Time of Day schedule for this action. If you choose the latter, Click Add Schedule and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
7. Expand **Execution Settings**.
   
   a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.

8. When done, click **Add Action**.

**Executing an External Program**

There are several circumstances where you may want to execute a program when a specific network event occurs. Use the **Edit Execute Program Action** window to specify the executable that should be started when the specified alert is triggered or reset, as shown in the following procedure.

External programs selected for this action must be executable using a batch file called from the command line. Programs executed this way run in the background. However, you can set the SolarWinds Alerting Engine Service to **Interact with Desktop**. SolarWinds recommends that scripts and batch files be placed on the root of c:\ to simplify the path for the batch file.

**To configure an alert to execute an external program:**

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.

2. Select the **Execute an External Program** option, then click **Configure Action**.

3. Enter a name for the action in the **Name of Action** field.

4. Under **Execute an External Program settings**:
   
   a. Enter the **Network path to external program** in the field provided. **For example:** Use `c:\test.bat`, where `c:\` is the disk on your main Orion poller and `test.bat` is your external program to be executed.

   b. Select either **Define User** or **No User Defined** for **Optional Windows Authentication**
5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.
   
a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

6. Expand **Execution Settings**.
   
a. Check either **Do not execute this action if the alert has been acknowledged already** (Recommended) or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.

7. When done, click **Add Action**.

**Executing a Visual Basic Script**

In some situations you may want to execute a Visual Basic (VB) script when a network event occurs. The Edit Execute VB Script Action window is used to specify the name and complete path of the file that shall be executed when the specified alert is triggered or reset.

To configure alerts to execute a Visual Basic (VB) script:

1. Click **VB Script**.
2. Select an available **VB Script Interpreter**.
3. Specify a VB script to execute either by typing the complete path and name of the VB script into the **VB Script to execute** field or by clicking **Browse (...)** to browse your folder structure and select the script.
4. Click **Time of Day**, and then enter the time period and select the days on which you want to execute the selected VB script.
5. Click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:
   
   * To disable the script when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
To execute the script repeatedly as long as the trigger condition exists, check *Execute this Action repeatedly while the Alert is Triggered* and then provide an appropriate action execution interval.

To delay script execution, check *Delay the execution of this Action*, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the script executes.

6.  *If you are finished configuring your VB script execution action*, click OK.

**Emailing a Web Page**

The Edit E-mail Web Page Action window includes several sections for configuration. The following procedure configures an e-mail URL action for an alert.

**To configure an email web page action for an alert:**

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Email a Web Page** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Recipients**:
   a. Complete the **To**, **CC**, and **BCC** fields.
   b. You can optionally edit sender details by expanding **[+] Sender Details** and editing the **Name of Sender** and the **Reply Address**.

   **Note**: You must provide at least one email address in the **To** field, and multiple addresses must be separated with commas. Some pager systems require a valid reply address to complete the page.
5. Expand **Message**.
   a. Enter the **Subject** and **Message** of your alert trigger email/page.

   **Note**: Messaging is disabled if both the **Subject** and **Message** fields are empty.
Optionally click **Insert Variable** to add variables using the following procedure:

i. Select a **Variable Category**, and then select the variable to add.

ii. **To define a SQL variable**, check **Define SQL Variable**.

iii. Click [+]/next to the name of a variable to add one or more variables to the **Custom SQL Variable** window.

iv. When done, click **Insert Variable**.

c. For the **Optional Web Server Authentication** section, select **User currently logged in**, **Another user**, or **No user defined**.

6. Expand **SMTP Server**.

a. Enter the Name of the **SMTP Server**.

b. Enter the **Hostname or IP Address of your SMTP Server** and the designated **SMTP Port Number**.

   **Note:** The SMTP server hostname or IP address field is required. You cannot send an email/page alert without identifying the SMTP server.

c. To use SSL/TLS encryption for your alert email, check **Use SSL**.

d. If your SMTP server requires authentication, check **This SMTP Server requires Authentication**.

e. Choose a **Secondary SMTP Server** from the list, if desired.

7. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule.

a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

8. Expand **Execution Settings**.

a. Check either **Do not execute this action if the alert has been acknowledged already** (Recommended) or **Repeat this action**
every X minutes until the alert is acknowledged. If you choose the latter, specify the frequency to have this action repeated.

9. When done, click Add Action.

Using Text to Speech Output

The Text to Speech Output action uses the SolarWinds Desktop Notification client and your computer's speech synthesizer to convert text messages-to-speech messages. The action notifies users of new alerts by reading the alert out loud. This capability is especially helpful for users who are visually impaired or who are not always at their desks to read alerts onscreen.

Download and install the client on each computer that you want to play a sound. Then configure which synthesizer you want to play.

You can specify a phrase that will be spoken upon alert trigger and a separate phrase for the alert reset. SolarWinds uses Microsoft® Speech Synthesis Engine version 5.0. If you are under active SolarWinds maintenance, you may also install and use other text-to-speech engines by visiting the SolarWinds website. The following procedure configures text-to-speech output for an alert trigger or reset.

Note: Due to restrictions on Windows service applications, the Text to Speech action is not available to SolarWinds installations on Windows 7 or Windows Server 2008 and higher.

To configure a text-to-speech output action for an advanced alert:

1. When editing or adding an alert, click Add Action in an Action section of the Alert Wizard.
2. Select the Text to Speech Output option, then click Configure Action.
3. Enter a name for the action in the Name of Action field.
4. Under Text to Speech Output settings:
   a. If not installed, click Download our desktop notification client to download and install the notification client.
      i. From the notification client, configure text to speech output.
b. Optionally click Insert Variable to insert variables into the Text field:
   i. Select a Variable Category, and then select the variable to add.
   ii. To define a SQL variable, check Define SQL Variable.
   iii. Click [+] next to the name of a variable to add one or more variables to the Custom SQL Variable window.
   iv. When done, click Insert Variable.

5. Expand Time of Day. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.
   a. Select either Schedule is controlled on the alert level, no additional schedule for this action needed or Use special Time of Day schedule for this action. If you choose the latter, Click Add Schedule and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

   a. Check either Do not execute this action if the alert has been acknowledged already (Recommended) or Repeat this action every X minutes until the alert is acknowledged. If you choose the latter, specify the frequency to have this action repeated.

7. When done, click Add Action.

Sending a Windows Net Message

Alerts can be configured to display a pop-up Windows Net Message either on a specific computer or on all computers in a selected domain or workgroup. The following steps configure Windows Net messaging for triggered or reset alerts.

Note: The only operating systems supporting Windows Net Messaging on which SolarWinds supports SolarWinds installations are Windows Server 2003 and Windows XP. SolarWinds only supports evaluation installations of SolarWinds on Windows XP.
To send a Windows Net message upon alert:

1. When editing or adding an alert, click Add Action in an Action section of the Alert Wizard.
2. Select the Send Net Message option, then click Configure Action.
3. Enter a name for the action in the Name of Action field.
4. Under Send a Net Message settings:
   a. Optionally check Send to all Computers in the Domain or Workgroup.
   b. Enter Computer Name or IP address in the field provided. **Note:** You can enter multiple computers or IP addresses by separating them with commas.
   c. Enter the Message of your alert trigger in the field provided.
   d. Optionally click Insert Variable to add variables using the following procedure:
      i. Select a Variable Category, and then select the variable to add.
      ii. To define a SQL variable, check Define SQL Variable.
      iii. Click [+] next to the name of a variable to add one or more variables to the Custom SQL Variable window.
      iv. When done, click Insert Variable.
5. Expand Time of Day. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.
   a. Select either Schedule is controlled on the alert level, no additional schedule for this action needed or Use special Time of Day schedule for this action. If you choose the latter, Click Add Schedule and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
6. Expand **Execution Settings**.
   a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.

7. When done, click **Add Action**.

**Sending an SNMP Trap**

Configure this action to enable SolarWinds NCM to send an SNMP notification. Creating this action requires the following information:

- UDP port number
- SNMP version number
- SNMP credentials

The following steps configure an alert to send an SNMP trap on the trigger or reset action.

**To send an SNMP trap:**

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Send SNMP Trap** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Send SNMP Trap Message**:
   a. Enter **SNMP Trap Destinations** in the field provided.  
      **Note:** Multiple IP Addresses should be separated by commas or semicolons.
   b. Select a **Trap Template** from the drop down lists.
5. Enter the **Message** of your alert trigger in the field provided.
   a. Optionally click **Insert Variable** to add variables using the following procedure:
i. Select a **Variable Category**, and then select the variable to add.

ii. To define a SQL variable, check **Define SQL Variable**.

iii. Click [+] to add one or more variables to the **Custom SQL Variable** window.

iv. When done, click **Insert Variable**.

6. Expand **SNMP Properties**.
   a. Enter a **UDP Port** number in the field provided.
   b. Select an **SNMP Version** from the drop down list.
   c. Enter the **SNMP Community String** in the field provided.

7. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not set the overall alert schedule.
   a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

8. Expand **Execution Settings**.
   a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.

9. When done, click **Add Action**.

**Using Get or Post URL Functions**

SolarWinds can be configured to communicate alerts using HTTP GET or POST functions. As an example, a URL may be used as an interface into a trouble ticket system, and, by correctly formatting the GET function, new trouble tickets may be created automatically. The following procedure configures SolarWinds to use GET or POST HTTP functions to communicate alert information.
To configure SolarWinds to use GET or POST URL functions with alerts:

1. When editing or adding an alert, click Add Action in an Action section of the Alert Wizard.
2. Select the Send a GET or POST Request to a Web Server option, then click Configure Action.
3. Enter a name for the action in the Name of Action field.
4. Under HTTP request settings:
   a. Enter a URL in the field provided.
   b. Select either Use HTTP GET or Use HTTP POST.
5. Expand Time of Day. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.
   a. Select either Schedule is controlled on the alert level, no additional schedule for this action needed or Use special Time of Day schedule for this action. If you choose the latter, Click Add Schedule and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
   a. Check either Do not execute this action if the alert has been acknowledged already (Recommended) or Repeat this action every X minutes until the alert is acknowledged. If you choose the latter, specify the frequency to have this action repeated.
7. When done, click Add Action.

Dialing Paging or SMS Service

This action forwards alerts to a paging or SMS service. Enable this capability by downloading and installing NotePager Pro from Notepage.net to your SolarWinds NCM server.

For instructions on configuring this action, see the NotePage Technical Support page, at http://www.notepage.net/solar-winds/technicalsupport.htm.
After NotePager Pro is installed, SolarWinds can be configured to communicate alerts using paging and SMS services. For more information about installation and configuration, see SolarWinds Network Performance Monitor Integration at www.notepage.net.

Viewing Alerts from Mobile Devices

NCM is capable of detecting when you are accessing the Orion Web Console from a mobile device. This mobile alerts view allows you to view and acknowledge existing active alerts.

To view and acknowledge alerts from a mobile device:

1. Using a browser on your mobile device, log in to your Orion Web Console as a user with alert management rights.
2. Click Alerts in the Views toolbar.
   
   **Note:** If you want to view the mobile alerts view from a desktop or server browser, add ?IsMobileView=true to the URL of the Alerts view in your Orion Web Console.

3. Check alerts you want to acknowledge, and then click **Acknowledge**.

Clickable links in alert messages provide more information about triggered alerts.

Viewing Alerts in the Orion Web Console

The Triggered Alerts for All Network Devices page provides a table view of your alerts log. You can customize the list view by using the following procedure to select your preferred alert grouping criteria.

To view alerts in the Web Console:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Click **Alerts** in the Views toolbar.
3. **If you want to filter your alerts table view by device**, select the device to which you want to limit your alerts view in the **Network Object** field.
4. **If you want to filter your alerts table by type of device**, select the device type to which you want to limit your alerts view in the **Type of Device** field.
5. **If you want to limit your alerts table to show a specific type of alert**, select the alert type in the **Alert Name** field.
6. In the **Show Alerts** field, provide the number of alerts you want to view.
Chapter 15: Integrating NCM Actions into Orion Alerts

7. **If you want to show all alerts, even if they have already been cleared or acknowledged**, check **Show Acknowledged Alerts**.

8. Click **Refresh** to complete your Alerts view configuration.

### Acknowledging Advanced Alerts in the Web Console

SolarWinds NCM allows you to acknowledge advanced alerts in the Orion Web Console, allowing you to eliminate time lost either when multiple users attempt to resolve the same issue or when a user tries to address an issue that has already been resolved.

1. From the web console, click **HOME > Alerts**.

2. **If you want to limit the list of alerts to only those dealing with a single device**, select the specific device from the **Object that triggered this alert list**.

   **Note:** This option is only available if alerts fire on multiple network devices.

3. **If you want to limit the list of alerts to only those dealing with a single type of device**, select the device type from the **Type of device** list.

   **Note:** This option is only available if Orion is monitoring multiple types of network devices.

4. **If you want to limit the list of alerts to only those of a single type**, select the specific alert type from the **Alert Name** list.

   **Note:** This option is only available when multiple types of SolarWinds NCM alerts have been triggered.

5. **If you want to limit the list of alerts to only those that have been acknowledged**, select the user from the **Acknowledged by** list.

6. Select the alerts you want to acknowledge, and then click **Acknowledge**.

### Escalated Advanced Alerts

By creating an escalated alert, SolarWinds NCM enables you to customize a series of alerts to trigger successive actions as an alert condition persists. The following topics provide both a scenario where an escalated alert may be useful and the steps required to create one using the Orion Advanced Alert Manager.

[Escalated Alert Example](#)
Escalated Alert Example

WidgetCo is a business with a small IT staff, consisting of two technicians and an IT manager. To ensure that issues are addressed appropriately, the IT manager has created multiple escalated alerts for a range of potential network events, including device failures and excessive disk space or bandwidth usage. Typically, the escalated alerts configured by the WidgetCo IT manager proceed as follows:

1. Immediately, as soon as NCM recognizes an alert condition, NCM generates both an email and a page that are sent to one of the two technicians. An entry is also recorded in the Orion events log.
2. If the alert is not acknowledged in the Orion Web Console within 20 minutes, a second alert is fired, generating another email and another page, both sent to both technicians. An entry is also recorded in the Orion events log.
3. If the second alert is not acknowledged within 20 minutes, NCM fires a third alert that sends both an email and a page to both technicians and to the IT manager. An entry is also recorded in the Orion events log.

Escalated alerts ensure that everyone on the WidgetCo IT staff is notified of any significant network alert conditions within 45 minutes without burdening the IT manager with excessive alert notifications. The following section provides a procedure to create a similar escalated alert scheme.

Viewing Alerts from Mobile Devices

SolarWinds NCM is capable of detecting when you are accessing the Orion Web Console from a mobile device. This mobile alerts view allows you to view and acknowledge existing active alerts.

1. Using a browser on your mobile device, log on to your Orion Web Console as a user with alert management rights.
2. Click Alerts in the Views toolbar.
3. If you want to view the mobile alerts view from a desktop or server browser, add ?IsMobileView=true to the end of the Alerts view URL.
4. Select the alerts you want to acknowledge, and then click Acknowledge.
Clickable links in alert messages provide more information about triggered alerts.

**Syslog Alert Variables**

The following variables can be used in Syslog alert messages. You must begin each variable with a dollar sign and enclose each variable identifier in curly braces as, for example, `${VariableName}`.

**Syslog Date/Time Variables**

**Other Syslog Variables**

**Syslog Date/Time Variables**

<table>
<thead>
<tr>
<th>Syslog Date/Time Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${AbreviatedDOW}</code></td>
<td>Current day of the week. Three character abbreviation.</td>
</tr>
<tr>
<td><code>${AMPM}</code></td>
<td>AM or PM corresponding to current time (before or after noon)</td>
</tr>
<tr>
<td><code>${D}</code></td>
<td>Current day of the month</td>
</tr>
<tr>
<td><code>${DD}</code></td>
<td>Current day of the month, two digit number and zero padded</td>
</tr>
<tr>
<td><code>${Date}</code></td>
<td>Current date, Short Date format</td>
</tr>
<tr>
<td><code>${DateTime}</code></td>
<td>Current date and time, Windows Control Panel defined Short Date and Short Time format</td>
</tr>
<tr>
<td><code>${DayOfWeek}</code></td>
<td>Current day of the week</td>
</tr>
<tr>
<td><code>${DayOfYear}</code></td>
<td>Numeric day of the year</td>
</tr>
<tr>
<td><code>${H}</code></td>
<td>Current hour</td>
</tr>
<tr>
<td><code>${HH}</code></td>
<td>Current hour, two digit format and zero padded</td>
</tr>
<tr>
<td><code>${Hour}</code></td>
<td>Current hour, 24-hour format</td>
</tr>
<tr>
<td><code>${LocalDOW}</code></td>
<td>Current day of the week, localized language format</td>
</tr>
</tbody>
</table>
### Syslog Date/Time Variables

<table>
<thead>
<tr>
<th>Syslog Date/Time Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${LongDate}</td>
<td>Current date, Long Date format</td>
</tr>
<tr>
<td>${LocalMonthName}</td>
<td>Current month name in the local language</td>
</tr>
<tr>
<td>${LongTime}</td>
<td>Current Time, Long Time format</td>
</tr>
<tr>
<td>${M}</td>
<td>Current numeric month</td>
</tr>
<tr>
<td>${MM}</td>
<td>Current month, two digit number and zero padded</td>
</tr>
<tr>
<td>${MMM}</td>
<td>Current month, three character abbreviation</td>
</tr>
<tr>
<td>${MediumDate}</td>
<td>Current date, Medium Date format</td>
</tr>
<tr>
<td>${Minute}</td>
<td>Current minute, two digit format and zero padded</td>
</tr>
<tr>
<td>${Month}</td>
<td>Full name of the current month</td>
</tr>
<tr>
<td>${N}</td>
<td>Current month and day</td>
</tr>
<tr>
<td>${S}</td>
<td>Current second</td>
</tr>
<tr>
<td>${Second}</td>
<td>Current second, two digit format and zero padded</td>
</tr>
<tr>
<td>${Time}</td>
<td>Current Time, Short Time format</td>
</tr>
<tr>
<td>${Year2}</td>
<td>Two digit year</td>
</tr>
<tr>
<td>${Year}</td>
<td>Four digit year</td>
</tr>
</tbody>
</table>

### Other Syslog Variables

<table>
<thead>
<tr>
<th>Syslog Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${Application}</td>
<td>SolarWinds application information</td>
</tr>
<tr>
<td>${Copyright}</td>
<td>Copyright information</td>
</tr>
<tr>
<td>${DNS}</td>
<td>Fully qualified node name</td>
</tr>
<tr>
<td>Syslog Variable</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>${IP_Address}</td>
<td>IP address of device triggering alert</td>
</tr>
<tr>
<td>${Message}</td>
<td>Status of device triggering alert</td>
</tr>
<tr>
<td>${MessageType}</td>
<td>Assigned alert name</td>
</tr>
<tr>
<td>${Release}</td>
<td>Release information</td>
</tr>
<tr>
<td>${Severity}</td>
<td>A network health score providing 1 point for an interface in a warning state, 1000 points for a down interface, and 1 million points for a down node.</td>
</tr>
<tr>
<td>${Version}</td>
<td>Version of the SolarWinds software package</td>
</tr>
</tbody>
</table>
Chapter 16: Creating and Managing Reports

The Orion platform database accumulates much information that can be presented in a variety of formats.

**Note:** Since NCM now uses Orion Platform reporting ([HOME > Reports](#)), the NCM reporting page ([CONFIGS > Reports](#)) is deprecated.

**For more information:**
- Predefined Reports
- Viewing Reports in the Orion Web Console
- Creating a New Web-Based Report
- Creating, Assigning and Editing Report Schedules in Report Manager
- Exporting and Importing Reports
Chapter 16: Creating and Managing Reports

Predefined Reports

NCM
NCM Audit
NCM Reports: Brocade Inventory
NCM Reports: Cisco Inventory
NCM Reports: Inventory
NCM Reports: Node Details
NCM Reports: Polling Status
NCM Reports: Route Tables Inventory
NCM Reports: Security
NCM Reports: Windows Server Inventory

Orion Platform
Current Node Status
Current Volume Status
Daily Node Availability
Events
Historical CPU and Memory Reports
Historical Response Time Reports
Historical VMware ESX Server Reports
Groups: Current Groups and Groups Members Status
Groups: Daily Group Availability
Groups: Group Availability (with members)
Groups: Historical Groups Status
Historical Volume Usage Reports
Inventory

360
Creating a New Web-Based Report

While modifying an existing web-based report is often the simplest and the most direct way to create a new report, you can easily create an entirely new web-based report.

To create a new web-based report:

1. Log in to the Orion Web Console.
2. Click Home > Reports.
3. Click Manage Reports.
5. Select and add the first resource to be added to the first column of your report. For more information, see Adding Content to a Web-Based Report Column.
6. Click Select and Continue. The Layout Builder view is displayed with the selected resource added. You can edit this and add further content later.
7. To change the size of your new report, either click Fit to window width to fit the new report to the current browser window, or enter a new value, in pixels (px), in the Report width field.
8. In the Header area, configure your new report as follows:
   a. Enter a Title and Subtitle.
   b. To replace the default logo, confirm that Logo is checked, and click Browse for logo to select your new logo.
9. In the Content area, configure your new report as follows:
   a. Either select the required Page Layout from the selector on the right or provide the number of Layout columns.
   b. For each column, click Add Content to add resources to your report. For more information, see Adding Content to a Web-Based Report Column.
   c. Click Add section to add further rows of content to this report.
10. To include a footer in your report, confirm that Footer is checked, and complete the following steps:
   - To include the report creation date in the footer, confirm that Creation date is checked.
   - To provide custom text in the footer, confirm that Custom text is checked, and then provide the custom text you want to include.

11. Click Next to display the Preview view.

12. If the preview is not how you want your report to be, click Back, and make the required edits.

13. If the report preview is acceptable, click Next to display the Properties view.

14. To store this report as one of your Favorite Reports, check My Favorite Reports. Marking a report as a favorite promotes it to the top of any reports list in which it appears.

15. Provide an appropriate Report Description.

16. Select the appropriate Report Category.
   Note: This report will be included in the selected Group by category on the Manage Reports view.

17. If there are any defined custom properties that may apply to this report, they are listed in the Custom Properties area. Provide appropriate values for all listed custom properties.
   Note: You may leave any custom property field blank, but your SQL database will record the field as 'empty' because SQL does not recognize NULL as a valid entry.

18. Enter any comments appropriate for this report in the Comments box. In addition to providing information about your report, you can use this to group reports on the initial Report page.

19. To apply or change limitations for this report, expand Report Limitation, and then select an appropriate Report limitation category.
   Note: Web-based reports can be restricted to specific users. Users may be assigned specific report limitation categories, and they may only view reports that are in the same report limitation category.

20. Click Next to display the Schedule Report view.
21. **To schedule this report to be generated, emailed, saved and/or printed at set times:**
   
   a. Select **Schedule this report to run regularly**.
   
   b. **If you have already set up report schedules**, click **Assign Schedule**, and select from the list.
   
   c. **To set up a new schedule**, click **Create new schedule**. For more information, see Creating a Report Schedule While Creating or Editing a Report.

22. Click **Next** to display the Summary view.

23. **If you do not want to schedule this report**, check **No schedule needed**.

24. Review the report configuration. Click **Edit** to return to any sections you want to amend or click **Submit** to save the report.
Chapter 16: Creating and Managing Reports

Viewing Reports in the Orion Web Console

The following procedure opens reports for viewing in the Orion Web Console.

To view reports in the Orion Web Console:

1. Open the Orion Web Console.
2. Click HOME > Reports.
3. Select a report group name to expand the report group.
4. Click the title of the report you want to view.

The report displays directly in the console browser.

Note: By default, newly created users do not have a configured report folder. If a new user is not seeing reports, you may need to select a Report Folder for the new user. For details, see "Configurating an Account Report Folder" in the SolarWinds Network Performance Administrator Guide.
Running a Config Change Report (Once)

1. From the web console, click **CONFIGS > Jobs**.
2. Click **Create New Job**.
3. Name the job, and then select **Generate a Config Change Report** from **Job Type**.
   - **Note**: Do not use special characters in the job name.
4. Select **Basic** as the **Schedule Type**.
5. Select **Once**, and then enter a day and time that is at least 15 minutes from the current NCM server time.
6. Add a comment if desired, and then click **Next**.
7. Select the nodes to target with this job, and then click **Next**.
8. Select an email notification option, and then click **Next**.
9. Select the type of config change report to generate, and then click **Next**.
10. Select **Only send devices that had changes** if desired, and then click **Next**.
11. Review the settings for the job, and then click **Finish**.

**Notes:**

- To create a config change report to run recurrently, see [Scheduling a Config Change Report (Recurrent)](https://example.com/scheduling).
- When processing an active job, NCM uses credential settings of the user who last edited the job. For example, if the user has user-level logon credentials, NCM uses the connection profile associated with the device.
Chapter 16: Creating and Managing Reports

Scheduling a Config Change Report (Recurrent)

1. From the web console, click CONFIGS > Jobs.
2. Click Create New Job.
3. Name the job, and then select Generate a Config Change Report from Job Type.
   
   **Note:** Do not use special characters in the name.
4. Select the Schedule Type.
   - *If you are creating a Basic schedule*, select the frequency of the job: once, daily, weekly, or monthly.
   - *If you are creating an Advanced schedule*, use the five fields to create an appropriate cron expression.
5. Add a comment if desired, and then click Next.
6. Select the nodes to target with this job, and then click Next.
7. Select an email notification option, and then click Next.
8. Select the type of config change report to generate, and then click Next.
9. Review the settings for the job, and then click Finish.

**Note:** When processing an active job, NCM uses credential settings of the user who last edited the job. For example, if the user has user level logon credentials set, NCM uses the connection profile associated with the device. For details on managing a connection profile, see Manage Connection Profiles.
Creating a Report Schedule While Creating or Editing a Report

You can directly assign a report to a schedule while editing the report.

To create a new schedule while creating or editing a report:

1. Click on the **Schedule Report** tab to display the Schedule Report view.
2. Click **Schedule this report to run regularly**.
3. Click **Create new schedule** in the dropdown.
4. Enter an appropriate **Schedule Name** and **Description**.
5. Click **Add Frequency** and then complete the following steps:
   a. Enter a name for this frequency.
   b. Select:
      - **Specific Date(s)** to select specific dates and times
      - **Daily** to schedule the report actions to run every day
      - **Weekly** to schedule the report actions to run once or more a week
      - **Monthly** to select the month and the day of the month to run the report actions.
   c. If you selected **Specific Date(s)**, select the date(s) and time(s) when you want the scheduled report actions to occur and then click **Add Frequency**.
      
      **Note:** Click **Add Time** to select additional dates and times.
   d. If you selected **Daily**, complete the following steps:
      i. Select the number of days between scheduled report actions.
         
         **Note:** to run the report on work days, select **Business Day (Mon - Fri)**.
      ii. Select the time(s) to run your report actions.
         
         **Note:** Click **Add Time** to add additional dates and times.
iii. *If you do not want the schedule to start immediately upon completion*, select **Specific Date(s)** in the **Starting On** field, and then select the date and time when you want the schedule to start.

iv. *If you want the schedule to end at some point*, check **Ending On**, and then select the date and time when you want the schedule to end.

v. Click **Add Frequency**.

e. *If you selected Weekly*, complete the following steps:

i. Check the days of the week to run the report actions.

ii. Select the time(s). You can click **Add Time** to add additional dates and times.

iii. *If you do not want the schedule to start immediately upon completion*, select **Specific Date(s)** in the **Starting On** field, and then select the date and time to start.

iv. *If you want the schedule to end at some point*, check **Ending On**, and then select the date and time for it to end.

v. Click **Add Frequency**. You can add multiple frequencies, if required.

f. *If you selected Monthly*, complete the following steps:

i. Select the months, days and times when you want to run your report actions.

    **Note:** Click **Add Time** to add additional dates and times.

ii. *If you do not want the schedule to start immediately upon completion*, select **Specific Date(s)** in the **Starting On** field, and then select the date and time when you want the report schedule to start.

iii. *If you want the schedule to end at some point*, check **Ending On**, and then select the date and time when you want the report schedule to end.

iv. Click **Add Frequency**.
6. Click **Add Action**, and select the action (Email, Print, or Save to Disk) to be executed on the configured schedule, and then click **Configure Action**.

7. Enter a **Name** for the action.

8. *If you selected Email:*

   a. In the **To** field, enter the email addresses of all recipients, separated by semicolons.
   
   b. If you need to add CC or BCC addresses, click **CC** and/or **BCC**, and enter the email addresses of these recipients.
   
   c. **To change the default name and address of the sender**, click "-" and enter the appropriate **Name of Sender** and **Reply Address**.
   
   d. Click **Message**, and enter the **Subject** and **Message** for the email. You can compose the message as **HTML** or **Plain Text**.
   
   e. **If you also want a printable version of your emailed reports**, check **Retrieve a Printable Version of Reports**.
   
   f. Check the format(s) in which you want to provide the emailed report: **PDF**, **CSV**, **Excel**, or **HTML**.
   
   g. **To include the URL of the emailed report so recipients can access it remotely**, check **Include Report’s URL**
   
   h. Click **SMTP Server**.
   
   i. If you have already configured an SMTP server, select the **Name of SMTP Server**, and then click **Save**.
   
   j. **If you have not already configured an SMTP server**, select **Add New Server**, and then complete the following steps:
      
      i. Provide the **Hostname or IP Address** of your SMTP Server and the designated **SMTP Port Number**.

         **Note:** The SMTP server hostname or IP address field is required. You cannot send an email without identifying the SMTP server.
      
      ii. **If you want to use SSL encryption for your emailed report**, check **Use SSL**. This changes the SMTP port number to 465.
iii. **If your SMTP server requires authentication**, check This SMTP Server requires Authentication, and then provide requested credentials.

k. Click Add Action.

9. **If you selected Print:**

   a. Provide a Windows User name, using domain\username format, and **Password** for a user with access to the printer on which you want to print your report.
   
   b. Click **Printer Settings**.
   
   c. Click **Select**, and then select the printer to which you want to send the report.
   
   d. Click **Select**.
   
   e. Enter the number of **Copies**, the **Layout**, whether you want **Color** or **Black and white** printing, and the **Margins** to be applied.
   
   f. Click Add Action.

10. **If you selected Save to Disk:**

    a. Enter the **Network Share Location** where you want to save the report.
    
    b. If you also want a printable version of your saved report, check **Retrieve a Printable Version of Reports**.
    
    c. Enter the Windows **User name**, using domain\username format, and **Password** for a user with access to the Network Share Location.
    
    d. Select the format(s) in which you want to provide the saved report (PDF, CSV, or Excel).
    
    e. Click Add Action. You can add multiple actions.
Creating, Assigning and Editing Report Schedules in Report Manager

The section contains procedures for the following scheduling tasks:

- Creating a new schedule
- Editing a schedule
- Assigning a report to a schedule
- Unassigning a report from a schedule

To create a new schedule from the Manage Report page:

1. Select the report for which you want to set up a schedule.
2. Click on Schedule Report > Create New Schedule to display the Properties view.
3. Enter an appropriate Schedule Name and Description of Report Schedule.
4. To add additional reports to this schedule, click Assign another Report, select the report(s) to be included in this schedule, and click Assign Report(s).
5. To assign webpages to this schedule, so that a snapshot of the selected website is included with the reports, click Assign Webpage and enter the URL in the field displayed. You can assign multiple webpages. Remember to start each with http:// or https:// as appropriate.
6. To specify a user account so that its limitations are applied to this schedule, expand Advanced Settings, click Another User and enter the User name or Account ID and Password.
7. Click Next to display the Frequency view.
8. Click Add Frequency and then complete the following steps:
   a. Enter a name for this frequency.
   b. Select:
      - Specific Date(s) to select specific dates and times
      - Daily to schedule the report actions every day
      - Weekly to schedule the report actions once or more a week
- **Monthly** if you want to select the month and the day of the month to schedule the report actions.

c. **If you selected Specific Date(s)**, select the date(s) and time(s) when you want the scheduled report actions to occur and click **Add Frequency**.

   **Note:** Click **Add Time** to select additional dates and times.

d. **If you selected Daily**, complete the following steps:

   i. Select the number of days between scheduled report actions.

      **Note:** To run the report on work days, select **Business Day (Mon - Fri)**.

   ii. Select the time(s) to run your report actions.

      **Note:** Click **Add Time** to add additional dates and times.

   iii. **If you do not want the schedule to start immediately upon completion**, select **Specific Date(s)** in the **Starting On** field, and select the date and time when you want the schedule to start.

   iv. **If you want the schedule to end at some point**, check **Ending On**, and select the date and time when you want the schedule to end.

   v. Click **Add Frequency**.

e. **If you selected Weekly**, complete the following steps:

   i. Check the days of the week to run the report actions.

   ii. Select the time(s). You can click **Add Time** to add additional dates and times.

   iii. **If you do not want the schedule to start immediately upon completion**, select **Specific Date(s)** in the **Starting On** field, and then select the date and time to start.

   iv. **If you want the schedule to end at some point**, check **Ending On**, and then select the date and time for it to end.
v. Click **Add Frequency**. You can add multiple frequencies, if required.

f. *If you selected Monthly*, complete the following steps:

i. Select the months, days of the month and times at which you want to run this schedule.

   **Note:** Click **Add Time** to add additional dates and times.

ii. *If you do not want the schedule to start immediately*, select **Specific Date(s)** in the **Starting On** field, and then select the date and time when you want the report schedule to start.

iii. *To set an end date and time for the schedule*, check **Ending On**, and then select the date and time when you want the report schedule to end.

iv. Click **Add Frequency**.

9. Click **Next** to display the Actions view.

10. Click **Add Action**, and select the action (**Email**, **Print**, or **Save to Disk**) to be executed on the configured schedule, and then click **Configure Action**.

11. Enter a **Name** for the action.

12. *If you selected Email:*

   a. In the **To** field, enter the email addresses of all recipients, separated by semicolons.

   b. **To add CC or BCC addresses**, click **CC** and/or **BCC**, and enter the email addresses of these recipients.

   c. **To change the default name and address of the sender**, click "-" and enter the appropriate **Name of Sender** and **Reply Address**.

   d. Click **Message**, and enter the **Subject** and **Message** for the email. You can compose the message as **HTML** or **Plain Text**.

   e. *If you also want a printable version of your emailed reports*, check **Retrieve a Printable Version of Reports**.

   f. Check the format(s) in which you want to provide the emailed report: **PDF**, **CSV**, **Excel**, or **HTML**.
g. *To include the URL of the emailed report so the recipients can access it remotely,* check *Include Report’s URL.*

h. Click **SMTP Server.**

i. *If you have already configured an SMTP server,* select the **Name of SMTP Server,** and click **Save.**

j. *If you have not already configured an SMTP server,* select **Add New Server,** and complete the following steps:

   i. Provide the **Hostname or IP Address** of your SMTP Server and the designated **SMTP Port Number.**

      **Note:** The SMTP server hostname or IP address field is required. You cannot send an email without identifying the SMTP server.

   ii. *To use SSL encryption for your emailed report,* check **Use SSL.** This changes the SMTP port number to 465.

   iii. *If your SMTP server requires authentication,* check **This SMTP Server requires Authentication,** and provide requested credentials.

k. Click **Add Action.**

13. *If you selected Print:*

   a. Provide a **Windows User** name, using **domain\username** format, and **Password** for a user with access to the printer on which you want to print your report.

   b. Click **Printer Settings.**

   c. Click **Select,** and then select the printer to which you want to send the report.

   d. Click **Select.**

   e. Enter the number of **Copies,** the **Layout,** whether you want **Color** or **Black and white** printing, and the **Margins** to be applied.

   f. Click **Add Action.**
14. If you selected Save to Disk:
   a. Enter the Network Share Location where you want to save the report.
   b. If you also want a printable version of your saved report, check Retrieve a Printable Version of Reports.
   c. Enter the Windows User name, using domain\username format, and Password for a user with access to the Network Share Location.
   d. Select the format(s) in which you want to provide the saved report (PDF, CSV, or Excel).
   e. Click Add Action. You can add multiple actions.

15. Click Next to display the Summary view.
16. If the schedule summary is correct, click Create Schedule.
17. The schedule is display in the Schedule Manager.

To edit a schedule

1. Click the Schedule Manager tab.
2. Select the schedule you want to edit and click Edit Schedule.
3. The Properties view for the schedule is displayed.

To assign a report to a schedule or multiple schedules

1. Select the report you want to assign.
2. Click Schedule Report > Assign Existing Schedule.
3. Confirm that you want to assign the report by selecting the schedule or schedules in the Assign existing schedule list and clicking Assign Schedule(s).

To unassign a report from a schedule or multiple schedules

1. Select the report you want to unassign.
2. Click Schedule Report > Unassign Schedule.
3. Confirm that you want to remove the report by selecting the schedule or schedules in the Unassign schedule from report list and clicking Unassign Schedule(s).
Exporting and Importing Reports

Import and export reports from Manage Reports in Orion Web Console.

To import a report:

1. Log in on the Orion Web Console.
2. Click HOME > Reports, and then click Manage Reports.
3. Click Export/Import Report and then click Import Report.
4. Locate the report and click Open.
   NCM save the report to the report list.
5. Use Group by to locate the report to export.
6. Select the report and click Export/Import, and then click Export Report.
7. Select Save File and find the appropriate location.

To export a report:

1. Log in on the Orion Web Console.
2. Click HOME > Reports, and then click Manage Reports.
3. Use Group by to locate the report to export.
4. Select the report and click Export/Import, and then click Import Report.
5. Select Save File and find the appropriate location.
NCM Reports: Brocade Inventory

Brocade Agent Config Module
Displays information on Brocade agent config modules running in chassis.

Brocade Chassis Serial Number
Displays serial number for Brocade chassis.

Brocade Chassis Unit Serial Number
Displays serial number for units within Brocade chassis.
Current Node Status

Average Response Time
Displays both average and peak response times for all monitored nodes.

Current CPU Load
Displays current CPU load percentage for all monitored nodes with CPUs.

Current Response Time
Displays the IP address and current, average, and peak response times for all monitored nodes.

Current Status of each Node
Displays the IP address and a verbal statement of the current operational status of all monitored nodes.

Down Nodes
Displays all monitored nodes that are currently down.

Last Boot Time for each Node
Displays the machine type and the date and time of last boot for all nodes.
Current Volume Status

Orion provides an **Available Space on each Volume** report that displays the volume size, available space on the volume, and a percentage measure of the available space on the volume for all monitored volumes. Volumes are listed beneath their respective parent nodes.
Daily Node Availability

Availability - Last Month
Displays the IP address and average daily availability of all monitored nodes over the current month.

Availability - This Month
Displays the IP address and average daily availability of all monitored nodes over the current month.

Availability - This Year
Displays the IP address and average daily availability of all monitored nodes over the last 12 months.
Events

All Down Events
Displays a list of all events in the database involving nodes that have stopped responding to polling over the last 12 months. For each down event, this report displays the down event date and time, the node name and IP address, and a verbal statement of the down event.

Down Events - Windows Devices
Displays a list of all events in the database involving Windows devices that have stopped responding to polling over the last month. For each down event, this report displays the down event date and time, the node name, and a verbal statement of the down event.

Last 250 Events
Displays the last 250 events involving any monitored device. For each event, this report displays the event date and time, the node involved, and a message describing the event.

Nodes that went down - Last 24 Hours
Displays a list of all nodes that have stopped responding over the last 24 hours. For every event of a node going down, this report displays the event date and time, an icon representing the current node status, the node name, and a verbal statement of the down event.

Triggered Alerts - Last 30 Days
Displays a list of all triggered alerts over the past 30 days. For each triggered alert event, this report displays the date and time of the alert trigger, the node that triggered the alert, and a message describing the triggered alert event.

Triggered and Reset Alerts - Last 30 Days
Displays a list of all triggered and reset alerts over the past 30 days. For each triggered or reset alert event, this report displays the date and time of the alert event, the node that triggered or reset the alert, and a message describing the alert event.
Groups: Current Groups and Groups Members Status

Current Status of each Group
  Current Status of each Group

Current Status of each Group Member
  Current Status of each Group Member

Groups and Group Members
  Groups and Group Members
### Groups: Daily Group Availability

<table>
<thead>
<tr>
<th>Group Availability - Last Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Availability - Last Month</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group Availability - This Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Availability - This Month</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group Availability - This Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Availability - This Year</td>
</tr>
</tbody>
</table>
Groups: Group Availability (with members)

Group Availability (with members) - Last Month
  Group Availability (with members) - Last Month

Group Availability (with members) - This Month
  Group Availability (with members) - This Month

Group Availability (with members) - This Year
  Group Availability (with members) - This Year
Historical CPU and Memory Reports

Orion provides a **CPU Load - Last Month** report that displays the vendor icon and average and peak CPU load percentages for all monitored nodes with CPUs over the previous calendar month.
Groups: Historical Groups Status

Historical Status of each Group - Last 7 Days
  Historical Status of each Group - Last 7 Days

Historical Status of each Group - Last Month
  Historical Status of each Group - Last Month

Historical Status of each Group - This Month
  Historical Status of each Group - This Month
Historical Response Time Reports

**Response Time - Last Month**
Displays average and peak response times for all monitored nodes over the previous calendar month.

**Response Time - Top 10 Last Month**
Displays the average and peak response times for the top ten monitored nodes over the previous calendar month.
Historical VMware ESX Server Reports

Network Traffic by VM for Last 7 Days
For each monitored VMware ESX Server, this report displays the average daily network traffic on the ESX Server per hosted VM for the last seven days.

Network Traffic by VM for Last Month
For each monitored VMware ESX Server, this report displays the average daily network traffic on the ESX Server per hosted VM for the last month.

Percent of CPU by VM for Last 7 Days
For each monitored VMware ESX Server, this report displays the average daily CPU load on the ESX Server due to each hosted VM for the last seven days.

Percent of CPU by VM for Last Month
For each monitored VMware ESX Server, this report displays the average daily CPU load on the ESX Server due to each hosted VM for the last month.

Percent of Memory by VM for Last 7 Days
For each monitored VMware ESX Server, this report displays the average daily memory load on the ESX Server due to each hosted VM for the last seven days.

Percent of Memory by VM for Last Month
For each monitored VMware ESX Server, this report displays the average daily memory load on the ESX Server due to each hosted VM for the last month.

Percent of Time Running vs. Stopped
For each monitored VMware ESX Server, this report displays both the percentage of time that each hosted VM has been running and the percentage of time that each hosted VM has been stopped.
Historical Volume Usage Reports

Orion provides an **Average Disk Space Used - Last 12 Months** report that displays the volume type and size, percentage of the volume space that is currently available, amount of the available space that is currently used, and the amount of volume space that is currently available for all monitored volumes. Volumes are listed beneath their respective parent nodes.
Inventory

All Disk Volumes
For all monitored volumes, this report displays the volume type and size, available space on the volume, amount of the available space that is currently used, and the peak amount of the available space that has been used on the volume, with the month in which peak usage occurred, over the last 12 months. Volumes are listed beneath their respective parent nodes.

Device Types
Displays a list of monitored machine types and the number of each type that are currently monitored.

IOS Versions of Cisco Devices
For all monitored Cisco devices, this report displays the device name, machine type, and Cisco IOS Version and Image.
NCM Audit

Config Transfer Audit
Displays information on config transfers.

Real Time Change Detection Audit
Displays change notification messages on nodes within the network.

User Activity Tracking Report
Displays relevant information on node activity within the network.

Vulnerability State Change Audit
Displays information about vulnerability state changes.
NCM Reports: Cisco Inventory

Cisco 3750 Stack - Physical Entity
Displays information about physical entities within each device.

Cisco Card Data
Displays information about Cisco card data within each device.

Cisco Catalyst Cards
Displays the card in each Catalyst switch.

Cisco Chassis IDs
Displays the chassis ID and serial number for Cisco devices.

Cisco Discovery Protocol
Displays the CDP discovered from each device.

Cisco Flash File System
Displays the list of files in the flash memory of Cisco devices.

Cisco Flash Memory
Displays the amount of flash memory in Cisco devices.

Cisco IOS Image Details
Displays details of IOS in each Cisco device.

Cisco Memory Pools
Displays memory pools in Cisco devices.

Cisco VLANs
Displays the VLANs to which devices belong.

Memory in Cisco Devices
Displays memory pools in Cisco devices.

Old Cisco Cards
Displays the cards in Cisco devices.

ROM Bootstrap for Cisco Devices
Displays the ROM bootstrap version for selected devices.
**NCM Reports: Inventory**

**ARP Tables**
- Displays ARP tables from each device.

**Interfaces**
- Displays details about each interface.

**IP Addresses on Each Interface**
- Displays the IP addresses assigned to each device.

**Juniper Physical Entities**
- Displays information about Juniper physical entities within each device.

**Last Status Change for Each Interface**
- Displays the time the status last changed on each interface.

**Logical Entities**
- Displays the logical entities within each device.

**Physical Entities (Serial Number)**
- Displays information about physical entities within each device.

**Physical Entities (Serial Number) v2**
- Displays information about physical entities within each device.

**Switch Ports**
- Displays spanning tree and VLAN information on each switch port.

**TCP Services**
- Displays the TCP services on each device.

**UDP Services**
- Displays the UDP services on each device.
NCM Reports: Node Details

All Nodes
Displays all nodes managed by NCM.

Backup Status of Running Config
Displays the timestamp for when the current Running config was backed-up or an indication that it has never been backed up.

Backup Status of Startup Config
Displays the timestamp for when the current Startup config was backed-up or an indication that it has never been backed up.

Connection Profiles
Displays the Connection Profile used by each device.

Current IOS Image and Version
Displays the current IOS image and version.

End of Support Devices
Displays devices that are at the end of their support.

Last Boot Time for Each Device
Displays timestamp for when the device was last booted.

Last Inventory of Each Device
Displays timestamp for when the device was last inventoried.

Overall Baseline Vs. Running Config Conflicts
Displays where the Running config differs from the Baseline config.

Overall Configuration Changes Snapshot
Displays all changes to the Running, Baseline, and Startup configs.

Overall Devices Backed Up Vs. Not Backed Up
Displays whether nodes have been backed up.

Overall Devices Inventoried Vs. Not Inventoried
Displays whether nodes have been inventoried.

Overall Running Vs. Startup Config Conflicts
Displays where the Running config differs from the Startup config.
System Information of Each Device

Displays the System Description, Location and Contact Information discovered from each device.
Chapter 16: Creating and Managing Reports

NCM Reports: Polling Status

Devices that do not respond to SNMP
  Displays information on Brocade agent config modules running in chassis.

Down Nodes
  Displays serial number for Brocade chassis.
NCM Reports: Route Tables Inventory

**Route Tables**

Displays route tables for relevant devices.
NCM Reports: Security

Community Strings for Each Node
Displays the SNMP community string used by each device.

Login Failure Report
Displays the devices that cannot be logged into and the error information.

Login Information for Each Device
Displays the username, enable level, and community strings for each device.

Login Status
Displays any error messages relating to login information for each device.

Nodes for Each Vulnerability
Displays nodes by vulnerability.

Vulnerabilities for Each Node
Lists vulnerabilities for each device.

Vulnerabilities for Each Node - Confirmed
Lists confirmed vulnerabilities for each device.

Vulnerabilities for Each Node - Not Applicable
Lists not applicable vulnerabilities for each device.

Vulnerabilities for Each Node - Potential
Lists potential vulnerabilities for each device.

Vulnerabilities for Each Node - Remediated
Lists remediated vulnerabilities for each device.

Vulnerabilities for Each Node - Remediation Planned
Lists remediation planned vulnerabilities for each device.

Vulnerabilities for Each Node - Waiver
Lists waiver vulnerabilities for each device.
NCM Reports: Windows Server Inventory

**Installed Services**
- Displays installed services for Windows nodes.

**Installed Software**
- Displays installed software for Windows nodes.

**Windows Accounts**
- Displays Windows accounts for relevant nodes.
Adding Content to a Web-Based Report Column

You can include any web console resource in your new report, as described below.

**Note:** The following procedure assumes you are already creating or editing a report in the web console report Layout Builder. For more information, see [Creating a New Web-Based Report](#).

**To add content to a web-based report column:**

1. On the Layout Builder view, click **Add Content** in the column to which you want to add a new report resource.
2. Select a criterion in the **Group by:** field.
   
   **Note:** The **Classic category** grouping provides the most comprehensive list of available resources.
3. Select the resource group from the list in the left pane.
4. Select the resource from the list in the main pane.
5. Click **Select and Continue**.
6. **If the resource is designated to work only with a specific object or objects:**
   
   a. Select the required object(s) from the left pane.
   
   b. To give a specific name to this data source, rather than accepting the default, enter it in the **Selection Name** field.
   
   c. Click **Add to Layout**.
7. **If you are an advanced user and want to add a Custom Chart or Table,** see [Adding a Custom Chart or Table to a Web-Based Report Column](#).
8. Once you have added content to a column, it is displayed with an **Edit Resource** button. Depending on the selected resource, clicking this button will enable you to change the title, subtitle and various other fields and settings.

**Note:** For resources and charts that report on a specific object or objects, you can select the object(s) from a drop-down list.
9. If you want to add a further row to your report, click **Add section**. You can now add content to this row as described above.

   **Note:** Resources can be dragged between columns and sections.

10. Click **Next** to preview the report.
Chapter 16: Creating and Managing Reports

Adding a Custom Chart or Table to a Web-Based Report Column

Advanced users can create custom charts or tables for inclusion in their web-based reports, as described in the following procedure. Because the Orion platform generates such a wealth of data, you need to ensure that you know exactly what data you are using, from which instances it originates from, and what you do with them to ensure that your custom charts and tables show meaningful results.

To add a custom chart or table to a web-based report column:

1. Click Add Content in the column to which you want to add a custom chart.
2. Select Type in the Group by: field.
3. Select Reports from the list in the left pane.
4. Select Custom Chart or Custom Table as required from the list in the main pane, and click Select and Continue.
5. Select:
   - **Specific Objects (static selection)** if you know precisely which objects you want to include in your chart or table.
     
     **Note**: This is the most straightforward selection method, and recommended for new users. It is also the preferred method for relatively permanent network objects.
   
   - **Dynamic Query Builder** to select objects based on object properties.
     
     **Note**: This is the preferred selection method for groups of objects of a specified type that may change over time. "All Cisco nodes in Austin" is an example of a group best defined using the Dynamic Query Builder.
   
   - **Advanced DataBase Query (SQL, SWQL)** only if you are comfortable querying your SolarWinds database directly, using SQL or SWQL.
6. **If you selected the Specific Objects (static selection) method**, select objects as shown in the following steps:

   a. Select the object type to chart from the *Show* drop-down.
   b. Select the grouping criterion from the *Group by* drop-down.
   c. Expand the groups displayed, if necessary, then check the object(s) to use.

7. **If you selected the Dynamic Query Builder method**, define objects as shown in the following steps:

   a. Select the type of selector query you want to use (*Basic* or *Advanced*).

      **Note:** Though the *Advanced Selector* provides access to all network object characteristics, the *Basic Selector* provides access to a smaller subset of the most frequently used network object characteristics.

   b. **To use the Basic selector:**

      i. Select the type of objects to report on from the *I want to report on* drop-down.
      ii. Select whether *All child conditions must be satisfied* (AND) or if only *At least one child condition must be satisfied* (OR).
      iii. Select a property of the monitored object, a conditional relation, and provide a value.
      iv. Click *Add Simple Condition* if you want to add another condition.

   c. **To use the Advanced Selector:**

      i. Select the type of objects to report on from the *I want to report on* drop-down.
      ii. Select whether *All child conditions must be satisfied* (AND) or if only *At least one child condition must be satisfied* (OR).
iii. For each condition you want to add, select the condition type by clicking on the green plus symbol (+). You can add a **Simple Condition** where you specify a monitored object property, a conditional relationship and a value, an **Advanced Condition** where you select two monitored object properties and a conditional relationship, or a nested **And/Or block**.

8. **If you selected the Advanced Database Query (SQL. SWQL),** provide a selection query, as follows:

   a. Select the **Query Type** (SWQL or SQL).

      **Note:** For more information about SWQL and SQL queries, click **How to use SWQL / SQL**.

   b. Enter a query, and then click **Preview Results** to confirm that your query provides expected results.

9. In each case enter a name for this selection in the **Selection Name** field if you don't want to use the default name and click **Add to Layout**.

10. You now need to edit the chart or table to specify the data series or columns you want to use and other settings. This is covered in **Editing a custom chart** and **Editing a custom table**.

**To add additional custom charts or tables:**

1. If you add further custom charts or tables, you will be asked if you want to use objects you selected previously or make a new object selection.
   
   - Click **Use previously specified objects** and select the objects from the drop-down to use the previously selected objects.
   
   - Click **Create new object selection** and continue from Step 5 above to specify new objects.

**To edit a custom chart:**

Once you have specified the objects to be reported on for a chart, you need to select the data series to be used.

1. For the custom chart you want to edit, select the time period to be reported on from the **From** drop-down.
2. Click **Edit Chart**.
3. Enter a **Title** and **Subtitle** as required.
4. Click **Add Data Series**.
5. Select the **Object** to report on, then how you to group data pertaining to this object. 
   
   **Note:** The groups available and the data series within these groups will depend on the object selected.
6. Select the **Data Series Name** from the list in the right pane, and click **Add Data Series**.
7. For additional settings for each data series, click **More**. Here you can:
   
   - Edit the **Display name** for this data series
   - Select a custom **Color** for this data series
   - **Show the 95th percentile line** for this data series
   - **Show Trend** for this data series
8. Repeat steps 4 to 7 to add further data series.
9. Enter a **Custom label** for the Left axis.
10. Select the **Units displayed**, and **Chart** type, and check the **Show the sum of all data series**, if required.
11. Select the **Sample Interval**. This can be from once a minute to once a week. Data within each sample interval is summarized so that a single point or bar is plotted for each of these periods. **Note:** It is possible to select a sample interval that is longer than the reporting period.
12. **To filter the data used in the chart:**
   
   a. Either:
      
      - Select **Show only limited number of top records** and enter how many of the top records to be used.
      - Select **Show only limited % of top records** and enter the top percentage of the top records to be used.
   
   b. Select how you want to sort this selection of records from the **Sort records by** drop-down. The choices shown here will depend on the data series selected.
c. Select either **Ascending** or **Descending** from the **Sort order** drop-down.

d. Select the **Data aggregation** method required.

e. Click **Advanced** if you want to sort records using a secondary field.

13. You can set up additional data series using the right axis. This allows you to superimpose two charts using different labels, units, and chart type.  

   **Note:** You cannot use a separate time period or filter results settings for the right axis series.

14. Click **Submit** to return to the Add Report page.

**To edit a custom table:**

Once you have specified the objects to be reported on for a table, you need to select the data series to be used.

1. For the custom table you want to edit, select the time period to be reported on from the **From** drop-down.

2. Click **Edit Table**.

3. Enter a **Title** and **Subtitle** as required.

4. Click **Add Column**.

5. Select the **Object** to report on, then how you want to group data pertaining to this object.

   **Note:** The groups available and the data series within these groups will depend on the object selected.

6. Select the **Database column names** from the list in the right pane, and click **Add Column**.

7. For additional settings for a column, click **Advanced**. Here you can:

   - Edit the **Display name** for this column.
   
   - Check **Hide this column in the resulting table**, if you want to use this column when querying the database but do not want to show it. For example, you may want to use this column's data in the time-based settings but not show the data in the table.
Adding a Custom Chart or Table to a Web-Based Report Column

- Check **Allow HTML tags**, if you want to use any HTML tags retrieved from the database for this column.
- Select the **Display settings** to be used for this column. This applies the selected formatting to the data in this column. The applicability of the formatting depends on the data. For example, if the column is Last Boot, you can show the date of the last boot or how many days ago it was. Similarly, if the column is Vendor and the display setting is Vendor icon, the vendor name will be replaced by the vendor logo, if available.
- Select the **Data aggregation** method to use for this column, if you want to summarize your data by time period.
- Select the **Alignment** for this data. This can be left, right or center.

8. To add further columns, click on the green plus sign in the table layout section, and repeat steps 5 to 7.

9. **To restrict data in your table to a specific time period**, select **Yes** from the **Time-based settings** drop-down.

   **Note:** You can only do this if your table contains a column with historical data.
   
   a. Select the column to use to specify the time period from the **Date/Time column in this table is** drop-down.
   
   b. Select the **Sample Interval**. This is used to summarize your data by time period.

10. To sort results in your table:

    a. Select the column you want to sort by from the **Sort results by** drop-down.

    b. Select how you want to sort the column. This can be **Ascending** or **Descending**.

   **Note:** You can sort further, using the remaining columns in the same way.
11. To group results in your table:
   a. Select the column you want to sort by from the **Group results by** drop-down.

   **Note:** You can group further, using the remaining columns in the same way.

12. To filter the results in your table, either:

13. Select **Show only the top ___ records** and enter the number of records to show

14. Select **Show only the top ___ % of records** and add the percentage of records to show

15. Click **Submit** to return to the Add Report page.
Chapter 17: Configuring TFTP, Secure Copy /SFTP, SMTP Server

The following topics describe how to configure the SolarWinds TFTP Server and Secure Copy SFTP Server.

- Using the SolarWinds TFTP Server
- Using Secure Copy /SFTP Server
- Using a Third-Party SCP Server
- Configuring the SMTP Server for Email Notifications
Chapter 17: Configuring TFTP, Secure Copy /SFTP, SMTP Server

Using the SolarWinds TFTP Server

SolarWinds NCM uses TFTP for file transfers.

**Note:** If you have NCM and NPM integrated but installed on separate servers, then follow these steps on the NPM server. The settings will automatically apply to NCM.

1. From the web console, click **Settings > NCM Settings**.
2. Under Network, click **TFTP Server**.
3. Enter the TFTP Server settings, and then click **Validate**.
4. Click **Submit**.

Using Secure Copy /SFTP Server

The SFTP/SCP server runs as a service, but some basic configuration may be necessary to ensure the SFTP/SCP server behaves in a way that works best in your environment.

1. Start the **SolarWinds SFTP & SCP Server** in the SolarWinds SFTP & SCP Server program folder.
2. Click **File > Configure**.
3. Type or browse to a **Root Directory**.
4. Select the protocols you want the server to support from the **Allowed Protocols** list.
5. Select options in the Permitted File Transfer Operations section.
6. Click the TCP/IP Settings tab, and then type the **TCP Port**.
7. **If you want to specify the IP address configuration**, select **Use custom IP address binding**, and then select the IP address you want to use.
8. **If you want to enable user authentication on the server**, complete the following:
   a. Click the Users tab.
   b. Click **New User**.
   c. Type the user name and password, and then click **Apply Changes**.
   d. If you want to remove a user, select the user, and then click **Remove**.
9. Click the Startup & System Tray tab, and then select the desired options.
10. Click **OK**.

### Using a Third-Party SCP Server

1. From the web console, click **Settings > NCM Settings**.
2. Under Network, click **SCP Server**.
3. Select **Use third-party SCP Server**.
4. Select **Allow me to specify the IP address of the SCP server** to prevent NCM from resolving the SCP server based on its own host and disabling other entries.
5. Enter a valid user name and password.
6. Specify a config transfer directory, and then click **Validate** to verify that the SCP Root Directory is set to be the same as the third-party server.
7. Click **Submit**.

**Note:** The user must have Receive/Transmit permissions configured in the third-party SCP server.

### Configuring the SMTP Server for Email Notifications

The settings you enter in the SMTP Server resource are used to send notifications regarding real-time config changes (RTCD), config change approvals, and running jobs.

1. From the web console, click **Settings > NCM Settings**.
2. Under Manage Notifications, click **SMTP Server**.
3. Enter the fully qualified domain name (FQDN) of the server in **Email Server Address**.
4. Enter the **Port Number** on which the server handles messages.
5. Select an **Authentication** type.
6. If you selected Password as your Authentication type, enter a user name and password that the server accepts.
7. Click **Submit**.
Chapter 17: Configuring TFTP, Secure Copy /SFTP, SMTP Server

For information on config change approvals, Setting Up the Config Change Approval System. See also Email Notification Settings

Email Notification Settings

These settings determine the sender, reply address, and subject included in the header of notifications received upon completion of an NCM job.

1. From the web console, click Settings > NCM Settings.
2. Under Manage Notifications, click Email Notification.
3. Enter in Sender Name the name you want to appear with a job completion notification.
4. Enter a Reply Address if desired.
5. Enter the Subject to be used to send a job completion notification.
6. Click Submit.
Chapter 18: Managing EnergyWise Entities

The following topics explore how you can use SolarWinds Network Configuration Manager in conjunction with SolarWinds Network Performance Manager to enable and manage your Cisco EnergyWise entities.

Managing and Enabling EnergyWise Nodes
Managing Your PoE Ports
Chapter 18: Managing EnergyWise Entities

What is EnergyWise?

EnergyWise is Cisco’s response to the call to cut energy costs, address environmental concerns, and adhere to government directives around green technologies. By purchasing EnergyWise capable devices and enabling their energy-saving features, you can retain business critical systems in a fully powered state while allowing less critical power over ethernet (PoE) devices to power down or drop into standby during off hours.

EnergyWise gives you the ability to control your energy cost. SolarWinds NCM gives you the ability to remotely apply recurrence policies and schedule power usage, helping you use less power. And, SolarWinds NPM allows you to monitor your energy use and power levels. SolarWinds perfectly partners with Cisco and the EnergyWise technologies to help you save more and monitor your savings.

Managing and Enabling EnergyWise Nodes

Cisco devices that support the EnergyWise technology can be enabled and their EnergyWise settings managed through the SolarWinds NCM integration with SolarWinds NPM.

Before completing the following procedure, EnergyWise nodes must be managed in both SolarWinds NCM and SolarWinds NPM.

For details on adding nodes, see Adding Nodes with Network Discovery.

1. From the web console, click Settings.
2. Under Node & Group Management, click Manage Nodes.
3. Select the Cisco node for which you want EnergyWise enabled, and then click More Actions > Manage EnergyWise.
4. Click Enable EnergyWise on these nodes.
5. Specify the appropriate values on the Manage EnergyWise Node page.
6. Click Execute Config Actions.
Managing Your PoE Ports

Power over ethernet (PoE) devices are connected to your devices on an interface and are managed at the interface level. Before completing the following procedure, you must have installed the SolarWinds NCM Integration for SolarWinds NPM on your SolarWinds NPM server and added your EnergyWise capable nodes to both SolarWinds NCM and SolarWinds NPM. For more information about adding nodes to SolarWinds NCM, see Managing NCM Nodes.

The following procedure guides you through enabling and configuring your EnergyWise interfaces. For more information about recurrence policies or the interaction between recurrence importance and entity importance, see the Help.

To enable or manage EnergyWise on an SolarWinds NPM interface:

1. Navigate to your SolarWinds NPM Web Console. For example, type http://NameOfOrionServer in the address bar of your web browser.
2. Log in to SolarWinds NPM.
3. Click Settings in the Views menu bar.
4. Click Manage Nodes.
5. Expand the Cisco node containing the interface you want to configure.
6. Select the interface you want to EnergyWise enable, and then click More Actions > Manage EnergyWise.
7. Click enable EnergyWise on these nodes.
8. Specify the appropriate values on the Manage EnergyWise Interface page. For more information about a field, click Help.
9. Click Execute Config Actions.

Note: To manage or modify interface-level EnergyWise settings, repeat this procedure omitting Step 7.
Chapter 19: Common Tasks

The following topics present example scenarios to help demonstrate how you can use SolarWinds Network Configuration Manager in different network environments:

- Configuring Automated Nightly Backups
- Changing the Community String on Multiple Nodes
- Changing an Interface Description
- Upgrading IOS and Firmware
- Blocking All Private Addresses with an Access List
- Blocking a MAC Address on a Wireless Access Point
- Customizing the Login Banner of a Device
Configuring Automated Nightly Backups

A powerful feature of SolarWinds Network Configuration Manager is the ability to schedule daily configuration file backups. SolarWinds NCM installs an example job that downloads the configuration files nightly for all nodes in the database. You can modify the example for your specific needs, or you can create a new job. The following procedure creates a new nightly configuration backup job. For more information on creating jobs, see Creating or Editing a Job.

1. From the web console, click **CONFIGS > Jobs**.
2. Click **Create New Job**
3. Name the job, and then select **Download Configs from Devices** from **Job Type**.
4. Select the **Schedule Type**.
   - *If you are creating a Basic schedule*, select the frequency of the job: once, daily, weekly, or monthly.
   - *If you are creating an Advanced schedule*, use the five fields to create an appropriate cron expression.
5. Add a comment if desired, and then click **Next**.
6. Select the nodes to target with this job, and then click **Next**.
7. Select an email notification option, and then click **Next**.
8. Select the configuration types you want to download, select the send config change notifications, and then click **Next**.
9. Review the settings for the job, and then click **Finish**.
Changing the Community String on Multiple Nodes

The following procedure replaces the public read-only community string with a new read-only community string on several network nodes at the same time. The procedure references other sections of the guide:

- Downloading Configuration Files
- Comparing Configurations
- Executing Command Scripts

1. From the web console, click CONFIGS > Jobs.
2. Click Create New Job
3. Name the job, and then select Execute Command Script on Devices from Job Type.
4. Select the Schedule Type.
   - If you are creating a Basic schedule, select the frequency of the job: once, daily, weekly, or monthly.
   - If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if desired, and then click Next.
6. Select the nodes to target with this job, and then click Next.
7. Select an email notification option, and then click Next.
8. Add the script to execute.
   - If you want to load a saved script, click Load Saved Script, and then select a script.
   - If you want to load an existing script from disk, click Load Script from File, browse to the file, and then click Open.
   - If you want to create a new script, enter your script in the text box. For example:
     
     ```
     config t
     no snmp-server community public RO
     snmp-server community 123@dm1n RO
     exit
     wr mem
     ```
     Where 123@dm1n is the new community string.

9. If you want to save a script, click Save Script to File, specify a location, and then click Save.

10. Select Filter results that match a pattern if you want to see in the script output only those lines that match a specific regex pattern.

11. Select Show commands in output to view what NCM sent to the targeted devices.

12. Click Next.

13. Review the settings for the job, and then click Finish.

**Verifying Successful Execution by Comparing Configurations**

1. Click CONFIGS > Configuration Management.
2. Select one or more nodes, and then click Compare node(s) configs.
3. Select a config from each list.
4. Click Compare Selected. Changes to are highlighted in red, green, and yellow.
Changing an Interface Description

Updating interface descriptions with SolarWinds Network Configuration Manager saves time because you do not have to remember IP addresses or logon credentials for the device you are updating. The procedure references other sections of the guide:

- Downloading Configuration Files
- Comparing Configurations
- Executing Command Scripts

Back Up the Running Configuration

1. From the web console, click CONFIGS > Configuration Management.
2. Select one or more nodes.
3. Click Download > Running.

Update Interface Descriptions

1. From the web console, click CONFIGS > Jobs.
2. Click Create New Job.
3. Name the job, and then select Execute Command Script on Devices from Job Type.
4. Select the Schedule Type.
   - If you are creating a Basic schedule, select the frequency of the job: once, daily, weekly, or monthly.
   - If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if desired, and then click Next.
6. Select the nodes to target with this job, and then click Next.
7. Select an email notification option, and then click Next.
Chapter 19: Common Tasks

8. Add the script to execute.
   - **If you want to load a saved script**, click **Load Saved Script**, and then select a script.
   - **If you want to load an existing script from disk**, click **Load Script from File**, browse to the file, and then click **Open**.
   - **If you want to create a new script**, enter your script in the text box. For example:
     ```
     config t
     interface Ethernet0
     no description
     description Link to Upstairs LabB
     exit
     exit
     wr mem
     ```
     Where *Link to Upstairs Lab* is the new description.

9. **If you want to save a script**, click **Save Script to File**, specify a location, and then click **Save**.

10. Select **Filter results** that match a pattern if you want to see in the script output only those lines that match a specific **regex pattern**.

11. Select **Show commands** in output to view what NCM sent to the targeted devices.

12. Click **Next**.

13. Review the settings for the job, and then click **Finish**.

**Verifying Successful Execution by Checking the Interface Description**

1. Click **CONFIGS > Config Summary**.
2. Click the updated node in the list.
3. Click the Configs tab.
4. Under Config List, select the running config, and then click **Edit Config**.
5. Locate the interface definitions.
6. Verify that the new description has been applied to the interface you modified.
Chapter 19: Common Tasks

Upgrading IOS and Firmware

You can upload IOS images uploaded using the SolarWinds Network Configuration Manager scripting engine. You can transfer these image files using TFTP, FTP (third party), SCP (third party), HTTP, or any other transfer protocol.

The following example uses the SolarWinds TFTP Server, included with SolarWinds NCM, to transfer an IOS image to the router. The TFTP Server must be running and configured to send and receive files. Also, the IOS image file must reside in the TFTP Root Directory.

IOS image management can be very complex. SolarWinds recommends you follow the upgrade guidelines outlined by your hardware manufacturer.

The following procedure references other sections of the guide:

- Downloading Configuration Files
- Comparing Configurations
- Executing Command Scripts

Backing Up the Running Configuration

1. From the web console, click CONFIGS > Configuration Management.
2. Select one or more nodes.
3. Click Download > Running.

Pushing an IOS Image to a Network Device

1. From the web console, click CONFIGS > Jobs.
2. Click Create New Job
3. Name the job, and then select Execute Command Script on Devices from Job Type.
4. Select the Schedule Type.
   - If you are creating a Basic schedule, select the frequency of the job: once, daily, weekly, or monthly.
   - If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if desired, and then click Next.
6. Select the nodes to target with this job, and then click **Next**.
7. Select an email notification option, and then click **Next**.
8. Add the script to execute.
   - **If you want to load a saved script**, click **Load Saved Script**, and then select a script.
   - **If you want to load an existing script from disk**, click **Load Script from File**, browse to the file, and then click **Open**.
   - **If you want to create a new script**, enter your script in the text box. For example:
     
     ```
     copy tftp flash
     10.10.2.17
     c2500-i-1.123-9a.bin
     y
     ```
     
     Where 10.10.2.17 is the location of the IOS image to copy using TFTP.
9. **If you want to save a script**, click **Save Script to File**, specify a location, and then click **Save**.
10. Select **Filter results** that match a pattern if you want to see in the script output only those lines that match a specific regex pattern.
11. Select **Show commands** in output to view what NCM sent to the targeted devices.
12. Click **Next**.
13. Review the settings for the job, and then click **Finish**.
Blocking All Private Addresses with an Access List

Routers connected to the Internet are normally configured to discard any traffic using private IP addresses. This isolation gives your private network a basic form of security as it is not usually possible for the outside world to establish a connection directly to one of your network devices using these addresses. The following procedure updates the Access Control List (ACL) to block all private IP addresses on several devices at the same time. The procedure references other sections of the guide:

- Downloading Configuration Files
- Comparing Configurations
- Executing Command Scripts

Backing Up the Running Configuration

1. From the web console, click CONFIGS > Configuration Management.
2. Select one or more nodes.
3. Click Download > Running.

Updating the ACL for a Group of Nodes

1. From the web console, click CONFIGS > Jobs.
2. Click Create New Job.
3. Name the job, and then select Execute Command Script on Devices from Job Type.
4. Select the Schedule Type.
   - If you are creating a Basic schedule, select the frequency of the job: once, daily, weekly, or monthly.
   - If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if desired, and then click Next.
6. Select the nodes to target with this job, and then click Next.
7. Select an email notification option, and then click Next.
8. Add the script to execute.
   - If you want to load a saved script, click Load Saved Script, and then select a script.
   - If you want to load an existing script from disk, click Load Script from File, browse to the file, and then click Open.
   - If you want to create a new script, enter your script in the text box. For example:
     
     ```
     ${EnterConfigMode}
     access-list 102 deny ip 10.0.0.0 0.255.255.255 any log
     access-list 102 deny ip 172.16.1.0 0.15.255.255 any log
     access-list 102 deny ip 192.168.0.0 0.0.255.255 any log
     exit
     write memory
     
     Where 102 is the name of the ACL. `${EnterConfigMode}` is a variable that is equivalent to config terminal on Cisco devices.
     ```

9. If you want to save a script, click Save Script, specify a location, and then click Save.

10. Select Filter results that match a pattern if you want to see in the script output only those lines that match a specific regex pattern.

11. Select Show commands in output to view what NCM sent to the targeted devices.

12. Click Next.

13. Review the settings for the job, and then click Finish.

**Verifying Successful Execution by Comparing Configurations**

1. Click CONFIGS > Configuration Management.
2. Select one or more nodes, and then click Compare node(s) configs.
3. Select a config from each list.
4. Click **Compare Selected**. Changes are highlighted in red, green, and yellow.
Blocking a MAC Address on a Wireless Access Point

If you discover a device utilizing unauthorized access through your wireless network, you can block the MAC address to prevent future access. The following procedure uses an Access Control List (ACL) on a wireless access point to block a specific MAC address. The procedure references other sections of the guide:

- Downloading Configuration Files
- Comparing Configurations
- Executing Command Scripts

Backing Up the Running Configuration

1. From the web console, click **CONFIGS > Configuration Management**.
2. Select one or more nodes.
3. Click **Download > Running**.

Blocking a MAC Address on a Wireless Access Point

1. From the web console, click **CONFIGS > Jobs**.
2. Click **Create New Job**.
3. Name the job, and then select **Execute Command Script on Devices** from **Job Type**.
4. Select the **Schedule Type**.
   - **If you are creating a Basic schedule**, select the frequency of the job: once, daily, weekly, or monthly.
   - **If you are creating an Advanced schedule**, use the five fields to create an appropriate cron expression.
5. Add a comment if desired, and then click **Next**.
6. Select the nodes to target with this job, and then click **Next**.
7. Select an email notification option, and then click **Next**.
8. Add the script to execute.
   - **If you want to load a saved script**, click Load Saved Script, and then select a script.
   - **If you want to load an existing script from disk**, click Load Script from File, browse to the file, and then click Open.
   - **If you want to create a new script**, enter your script in the text box. For example:
     ```
     ${EnterConfigMode}
     access-list 724 deny 000e.0ca1.a2b4 0000.0000.0000
     exit
     wr mem
     ```
     Where 724 is the name of the ACL, and 000E.0CA1.A2B4 is the MAC address to block. `${EnterConfigMode}` is a variable that is equivalent to `config terminal` on Cisco devices.

9. **If you want to save a script**, click Save Script, specify a location, and then click Save.

10. Select **Filter results** that match a pattern if you want to see in the script output only those lines that match a specific regex pattern.

11. Select **Show commands** in output to view what NCM sent to the targeted devices.

12. Click Next.

13. Review the settings for the job, and then click Finish.

**Verifying Successful Execution by Comparing Configurations**

1. Click **CONFGS > Configuration Management**.

2. Select one or more nodes, and then click **Compare node(s) configs**.

3. Select a config from each list.

4. Click **Compare Selected**. Changes to are highlighted in red, green, and yellow.
Customizing the Login Banner of a Device

You can easily change the login banner for a router, switch, or firewall using SolarWinds Network Configuration Manager. This customization can be rolled out to a single or multiple devices. The following procedure references other sections of the guide:

- Downloading Configuration Files
- Comparing Configurations
- Executing Command Scripts

Modifying the Login Banner

1. From the web console, click **CONFI GS > Jobs**.
2. Click **Create New Job**.
3. Name the job, and then select **Execute Command Script on Devices** from **Job Type**.
4. Select the **Schedule Type**.
   - **If you are creating a Basic schedule**, select the frequency of the job: once, daily, weekly, or monthly.
   - **If you are creating an Advanced schedule**, use the five fields to create an appropriate cron expression.
5. Add a comment if desired, and then click **Next**.
6. Select the nodes to target with this job, and then click **Next**.
7. Select an email notification option, and then click **Next**.
Chapter 19: Common Tasks

8. Add the script to execute.

   - *If you want to load a saved script*, click Load Saved Script, and then select a script.
   
   - *If you want to load an existing script from disk*, click Load Script from File, browse to the file, and then click Open.
   
   - *If you want to create a new script*, enter your script in the text box. For example:

     ```
     config t
     no banner login
     banner login ^Unauthorized use of these systems is punishable by law^ exit
     wr mem
     ```

     Where *Unauthorized use of these systems is punishable by law* is the new banner.

9. *If you want to save a script*, click Save Script, specify a location, and then click Save.

10. Select Filter results that match a pattern if you want to see in the script output only those lines that match a specific regex pattern.

11. Select Show commands in output to view what NCM sent to the targeted devices.

12. Click Next.

13. Review the settings for the job, and then click Finish.

Verifying Successful Execution by Comparing Configurations

1. Click CONFIGS > Configuration Management.

2. Select one or more nodes, and then click Compare node(s) configs.

3. Select a config from each list.

4. Click Compare Selected. Changes to the login banner are highlighted in yellow if the banner is different from a previous login banner. If no login banner was previously specified, changes are highlighted in red and green.
Appendix A: Node and Archive Variables

SolarWinds Network Configuration Manager uses a variable system that is similar to that of SolarWinds Network Performance Monitor. Variables always begin with a dollar sign and a curly brace (${ }), and always end with a curly brace (}). Variables may be used in most custom properties. They may also be used in any of the user editable system properties.

Variables can also be nested and recursive. That is, a single variable can refer to a node property that contains more variables that then contain even more variables. The following example demonstrates nested variables:

<table>
<thead>
<tr>
<th>Node Property</th>
<th>Value of Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Rack ${Rack} on ${Floor} floor of ${Building} - ${SysLocation}</td>
</tr>
<tr>
<td>Building</td>
<td>Building C</td>
</tr>
<tr>
<td>SysLocation</td>
<td>Data Center A</td>
</tr>
<tr>
<td>Rack</td>
<td>15</td>
</tr>
<tr>
<td>Floor</td>
<td>Second</td>
</tr>
</tbody>
</table>

The database value of Location is Rack ${Rack} on ${Floor} floor of ${Building} - ${SysLocation}. The displayed value of Location is Rack 15 on Second floor of Building C - Data Center A.

For more information about Syslog, Trap, and Template variables:

- [Command Template Commands](#)
- [Pre-Command and Command Template Variables](#)
- [Trap Alert Variables](#)
- [Syslog Alert Variables](#)
Appendix A: Node and Archive Variables

For more information: on node, configuration, and archive variables:

- Node Variables
- Command Template Commands
Node Variables

All fields in the nodes table may be used as variables, including any custom properties added to your nodes.

<table>
<thead>
<tr>
<th>Nodes Table Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NodeID</td>
<td>Unique ID assigned to each Network Node</td>
</tr>
<tr>
<td>NodeCaption</td>
<td>Displayed name for the node. The default for NodeCaption is a variable. <code>${SysName}</code></td>
</tr>
<tr>
<td>NodeGroup</td>
<td>Group to which this node belongs. Some group examples include <strong>Routers</strong>, <strong>Accounting</strong>, or simply <code>${Building}</code>. The last example refers to a custom property named <strong>Building</strong>.</td>
</tr>
<tr>
<td>AgentIP</td>
<td>The IP address used when communicating with the node. A router or server may have many IP addresses. This IP address is the one used when SolarWinds Network Configuration Manager makes SNMP requests or transfers configuration files.</td>
</tr>
<tr>
<td>AgentIPSort</td>
<td>Numeric equivalent of the AgentIP. Used for sorting by IP address in reports.</td>
</tr>
<tr>
<td>ReverseDNS</td>
<td>Reverse lookup of the AgentIP</td>
</tr>
<tr>
<td>ResponseTime</td>
<td>Current response time of the node in milliseconds</td>
</tr>
<tr>
<td>ResponseError</td>
<td>OK if the node is responding. Returns an error message if the node is not responding.</td>
</tr>
</tbody>
</table>
| Status            | Numeric status of the node.  
1 = Up  
2 = Down |
| Community         | SNMP community string |
| SNMPLevel         | The version of SNMP supported by the Node.  
0 = SNMP not supported |
### Appendix A: Node and Archive Variables

<table>
<thead>
<tr>
<th>Nodes Table Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SNMP V1</td>
</tr>
<tr>
<td>2</td>
<td>SNMP V2</td>
</tr>
<tr>
<td>3</td>
<td>SNMP V3</td>
</tr>
<tr>
<td>SysName</td>
<td>System name of the node.</td>
</tr>
<tr>
<td>SysDescr</td>
<td>System description of the node.</td>
</tr>
<tr>
<td>SysContact</td>
<td>System contact information collected from the node.</td>
</tr>
<tr>
<td>SysLocation</td>
<td>System location information collected from the node.</td>
</tr>
<tr>
<td>SystemOID</td>
<td>System OID discovered from the node.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Hardware vendor of this network node.</td>
</tr>
<tr>
<td>VendorIcon</td>
<td>Name of the vendor icon used.</td>
</tr>
<tr>
<td>MachineType</td>
<td>Type of hardware. This information is discovered by SolarWinds Discovery Engine.</td>
</tr>
<tr>
<td>LastBoot</td>
<td>Last time the node rebooted.</td>
</tr>
<tr>
<td>OSImage</td>
<td>Operating system running on the node</td>
</tr>
<tr>
<td>OSVersion</td>
<td>Version of the operating system running on the node</td>
</tr>
<tr>
<td>ConfigTypes</td>
<td>Types of configuration files supported by this node</td>
</tr>
<tr>
<td>NodeComments</td>
<td>Any comments about this node entered by the user.</td>
</tr>
<tr>
<td>NextDiscovery</td>
<td>Time for next complete discovery of this node</td>
</tr>
<tr>
<td>NextPoll</td>
<td>Time for next poll (up/down and response time)</td>
</tr>
<tr>
<td>Username</td>
<td>Login username</td>
</tr>
<tr>
<td>Password</td>
<td>Login password</td>
</tr>
</tbody>
</table>
## Configuration Archive Variables

SolarWinds Network Configuration Manager stores all downloaded configurations in a database. It can also store a copy of them in the configuration archive directory. The directory structure can be specified using any of the previous variables.

Additional variables may also be used when specifying the configuration archive directory. Many of these variables use the localization settings for the current language and region.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DateTime</td>
<td>Local date and time in short date and local time format</td>
</tr>
<tr>
<td>Date</td>
<td>Date in short date format</td>
</tr>
<tr>
<td>LongDate</td>
<td>Date in long date format</td>
</tr>
<tr>
<td>MediumDate</td>
<td>Date in medium date format</td>
</tr>
<tr>
<td>Time</td>
<td>Time in short time format</td>
</tr>
<tr>
<td>LongTime</td>
<td>Time in long time format</td>
</tr>
<tr>
<td>MediumTime</td>
<td>Time in medium time format</td>
</tr>
<tr>
<td>ShortTime</td>
<td>Time in short time format</td>
</tr>
</tbody>
</table>
## Appendix A: Node and Archive Variables

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOW</td>
<td>Day of the week, spelled out</td>
</tr>
<tr>
<td>D</td>
<td>Day of the month</td>
</tr>
<tr>
<td>DD</td>
<td>Day of the month, with leading zero, if needed</td>
</tr>
<tr>
<td>ABREVIATEDDOW</td>
<td>Day of the week in abbreviated format</td>
</tr>
<tr>
<td>LocalDow</td>
<td>Day of the week in the local language</td>
</tr>
<tr>
<td>Month</td>
<td>Number of the current month</td>
</tr>
<tr>
<td>M</td>
<td>Number of the current month</td>
</tr>
<tr>
<td>MM</td>
<td>Number of the current month, with leading zeros, if needed</td>
</tr>
<tr>
<td>MMM</td>
<td>Abbreviated name of the month</td>
</tr>
<tr>
<td>MMMM</td>
<td>Name of the month</td>
</tr>
<tr>
<td>LocalMonthName</td>
<td>Name of the month in the local language</td>
</tr>
<tr>
<td>DAYOFYEAR</td>
<td>Day number of the year</td>
</tr>
<tr>
<td>YYYY</td>
<td>4 digit year</td>
</tr>
<tr>
<td>YY</td>
<td>2 digit year</td>
</tr>
<tr>
<td>YEAR2</td>
<td>2 digit year</td>
</tr>
<tr>
<td>YEAR4</td>
<td>4 digit year</td>
</tr>
<tr>
<td>H</td>
<td>Hour</td>
</tr>
<tr>
<td>HH</td>
<td>2 digit hour, with leading zero, if needed</td>
</tr>
<tr>
<td>N</td>
<td>Minute</td>
</tr>
<tr>
<td>NN</td>
<td>2 digit minute, with leading zero, if needed</td>
</tr>
</tbody>
</table>
### Configuration Archive Variables

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>Seconds</td>
</tr>
<tr>
<td>SS</td>
<td>2 digit seconds, with leading zero, if needed</td>
</tr>
<tr>
<td>AMPM</td>
<td>AM or PM</td>
</tr>
<tr>
<td>CRLF</td>
<td>Carriage return - linefeed combination</td>
</tr>
<tr>
<td>ConfigType</td>
<td>Type of configuration: running, startup, etc.</td>
</tr>
<tr>
<td>Caption</td>
<td>Caption of the node, NodeCaption</td>
</tr>
</tbody>
</table>
Appendix B: Regular Expression Pattern Matching

When editing comparison criteria, the following regular expressions can be used for pattern matching. Examples are provided at the end of this section; however, the examples are not and do not intend to be comprehensive. In general, SolarWinds does not offer support in constructing regular expressions and instead expects users of NCM to create expressions valid for their own intended purposes.

Consulted these topics as needed:

Characters
Character Classes or Character Sets [abc]
Dot
Anchors
Word Boundaries
Alternation
Quantifiers
Regular Expression Pattern Matching Examples
Character Classes or Character Sets [abc]
NCM supports the following regular expression character classes and sets.
<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ (opening square bracket)</td>
<td>Starts a character class. A character class matches a single character out of all of the possibilities offered by the character class. Inside a character class, different rules apply. The rules in this section are only valid inside character classes. The rules outside this section are not valid in character classes, except \n, \r, \t and \xFF</td>
<td></td>
</tr>
<tr>
<td>Any character except ^,-,,\ add that character to the possible matches for the character class.</td>
<td>All characters except the listed special characters.</td>
<td>[abc] matches a, b or c</td>
</tr>
<tr>
<td>\ (backslash) followed by any of ^,-,\</td>
<td>A backslash escapes special characters to suppress their special meaning.</td>
<td>[^] matches ^ or ]</td>
</tr>
<tr>
<td>- (hyphen) except immediately after the opening [</td>
<td>Specifies a range of characters. (Specifies a hyphen if placed immediately after the opening [)</td>
<td>[a-zA-Z0-9] matches any letter or digit</td>
</tr>
<tr>
<td>^ (caret) immediately after the opening [</td>
<td>Negates the character class, causing it to match a single character not listed in the character class. (Specifies a caret if placed anywhere except after the opening [)</td>
<td>[^a-d] matches x (any character except a, b, c or d)</td>
</tr>
</tbody>
</table>
Appendix B: Regular Expression Pattern Matching

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>\d, \w and \s</td>
<td>Shorthand character classes matching digits 0-9, word characters (letters and digits) and whitespace respectively. Can be used inside and outside character classes</td>
<td>[\d\s] matches a character that is a digit or whitespace</td>
</tr>
</tbody>
</table>

**Dot**

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>. (dot)</td>
<td>Matches any single character except line break characters \r and \n.</td>
<td>. matches x or most any other character</td>
</tr>
</tbody>
</table>

**Anchors**

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>^ (caret)</td>
<td>Matches at the start of the string to which the regular expression pattern is applied. Matches a position rather than a character. Most regular expression flavors have an option to make the caret match after line breaks (i.e. at the start of a line in a file) as well.</td>
<td>^ matches a in abc\ndef. Also matches d in &quot;multi-line&quot; mode.</td>
</tr>
</tbody>
</table>
### Anchors

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>$ (dollar)</td>
<td>Matches at the end of the string to which the regular expression pattern is applied. Matches a position rather than a character. Most regular expression flavors have an option to make the dollar match before line breaks (i.e. at the end of a line in a file) as well. Also matches before the very last line break if the string ends with a line break. Note: If there are some special non-printable characters at the end of the lines in a downloaded config, the $ operator might not match the line end. A test would be to copy lines from a config to a plain text file (in Notepad, for example); if you see extra, empty lines that are not in the pasted content then there are mostly likely non-printable characters in them.</td>
<td>$. matches f in abc\ndef. Also matches c in &quot;multi-line&quot; mode.</td>
</tr>
<tr>
<td>\A</td>
<td>Matches at the start of the string to which the regular expression pattern is applied. Matches a position rather than a character. Never matches after line breaks.</td>
<td>\A. matches a in abc</td>
</tr>
<tr>
<td>\Z</td>
<td>Matches at the end of the string to which the regular expression pattern is applied. Matches a position rather than a character. Never matches before line breaks, except for the very last line break if the string ends with a line break.</td>
<td>.\Z matches f in abc\ndef</td>
</tr>
<tr>
<td>\z</td>
<td>Matches at the end of the string to which the regular expression pattern is applied. Matches a position rather than a character. Never matches before line breaks.</td>
<td>.\z matches f in abc\ndef</td>
</tr>
</tbody>
</table>
## Appendix B: Regular Expression Pattern Matching

### Word Boundaries

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>\b</td>
<td>Matches at the position between a word character (anything matched by \w) and a non-word character (anything matched by [^\w] or \W) as well as at the start and/or end of the string if the first and/or last characters in the string are word characters.</td>
<td>.\b matches c in abc</td>
</tr>
<tr>
<td>\B</td>
<td>Matches at the position between two word characters (i.e the position between \w\w) as well as at the position between two non-word characters (i.e. \W\W).</td>
<td>\B.\B matches b in abc</td>
</tr>
</tbody>
</table>

### Alternation

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(vertical bar or “pipe”)</td>
<td>Causes the regular expression engine to match either the part on the left side or the part on the right side. Can be strung together into a series of options.</td>
</tr>
<tr>
<td></td>
<td>(vertical bar or “pipe”)</td>
<td>The vertical bar has the lowest precedence of all operators. Use grouping to alternate only part of the regular expression.</td>
</tr>
</tbody>
</table>

### Quantifiers

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>(question mark)</td>
<td>Makes the preceding item optional. The optional item is included in the match, if possible.</td>
</tr>
<tr>
<td>Character</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>??</td>
<td>Makes the preceding item optional. The optional item is excluded in the match, if possible. This construct is often excluded from documentation because of its limited use.</td>
<td>abc?? matches ab or abc</td>
</tr>
<tr>
<td>* (star)</td>
<td>Repeats the previous item zero or more times. As many items as possible will be matched before trying permutations with fewer matches of the preceding item, up to the point where the preceding item is not matched at all.</td>
<td>.* matches &quot;def&quot; &quot;ghi&quot; in abc &quot;def&quot; &quot;ghi&quot; jkl</td>
</tr>
<tr>
<td>*? (lazy star)</td>
<td>Repeats the previous item zero or more times. The engine first attempts to skip the previous item before trying permutations with ever increasing matches of the preceding item.</td>
<td>.*? matches &quot;def&quot; in abc &quot;def&quot; &quot;ghi&quot; jkl</td>
</tr>
<tr>
<td>+ (plus)</td>
<td>Repeats the previous item once or more. As many items as possible will be matched before trying permutations with fewer matches of the preceding item, up to the point where the preceding item is matched only once.</td>
<td>.+ matches &quot;def&quot; &quot;ghi&quot; in abc &quot;def&quot; &quot;ghi&quot; jkl</td>
</tr>
<tr>
<td>+? (lazy plus)</td>
<td>Repeats the previous item once or more. The engine first matches the previous item only once, before trying permutations with ever increasing matches of the preceding item.</td>
<td>.+? matches &quot;def&quot; in abc &quot;def&quot; &quot;ghi&quot; jkl</td>
</tr>
<tr>
<td>{n} where n is an integer &gt;= 1</td>
<td>Repeats the previous item exactly n times.</td>
<td>a{3} matches aaa</td>
</tr>
</tbody>
</table>
### Appendix B: Regular Expression Pattern Matching

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>{n,m} where n &gt;= 1 and m &gt;= n</td>
<td>Repeats the previous item between n and m times. Will try to repeat m times before reducing the repetition to n times.</td>
<td>a{2,4} matches aa, aaa or aaaa</td>
</tr>
<tr>
<td>{n,m}? where n &gt;= 1 and m &gt;= n</td>
<td>Repeats the previous item between n and m times. Will try to repeat n times before increasing the repetition to m times.</td>
<td>a{2,4}? matches aaaa, aaa or aa</td>
</tr>
<tr>
<td>{n,} where n &gt;= 1</td>
<td>Repeats the previous item at least n times. Will try to match as many items as possible before trying permutations with fewer matches of the preceding item, up to the point where the preceding item is matched only m times.</td>
<td>a{2,} matches aaaaa in aaaaa</td>
</tr>
<tr>
<td>{n,}? where n &gt;= 1</td>
<td>Repeats the previous item between n and m times. The engine first matches the previous item n times before trying permutations with ever increasing matches of the preceding item.</td>
<td>a{2,}? matches aa in aaaaa</td>
</tr>
</tbody>
</table>

### Regular Expression Pattern Matching Examples

The following examples illustrate some of the uses of Regular Expression pattern matching.

**snmp-server community public**

Finds any line that includes the text `snmp-server community public`. There can be text before and/or after the string on the same line.

**access-list 105 deny.*tcp any any eq 139 log**

Finds the line with `access-list 105 deny.*tcp any any eq 139 Login on` the same line. The regular expression string `.*` finds any character, and any number of characters on the same line. So, this could be used to find spaces, tabs, numbers, letters, or special characters.

**ntp clock-period \d**
Finds any line that includes `ntp clock-period` followed by any number. The regular expression string `\d*` will find any number at any length, such as 3, 48, or 2394887.

**user \x2a**

Finds any line that includes `user *`. The regular expression string `\x` followed by a hexadecimal value specifies an individual character. In this example, `\x2a` represents the asterisk character, which has a hexadecimal value of 2a.
Appendix C: Using the Database Management Tools

The SolarWinds Database Manager can be used to perform queries, view database and table details.

For other database management tasks, including back-up and restoring a database for SolarWinds NCM and other Orion Platform products, you need to use an appropriate Microsoft utility such as SQL Server Management Studio.

Starting SolarWinds Database Manager
Adding a Server to SolarWinds Database Manager
Viewing Database Details
Viewing Table Details
Moving a Database with SQL Server Management Studio
Restoring Backup Files to SQL Server 2008 and 2012
Updating SolarWinds NCM to Use the New Database Server
Appendix C: Using the Database Management Tools

Starting SolarWinds Database Manager

To perform any maintenance on your database, the Database Manager must be used. Complete the following procedure to start the Database Manager.

To open Database Manager, click **Start > All Programs > SolarWinds Orion > Advanced Features > SolarWinds Database Manager**.

Adding a Server to SolarWinds Database Manager

The following procedure adds a SQL server to the SolarWinds Database Manager.

To add a SQL server:

1. Start Database Manager (**SolarWinds Orion > Advanced Features > Database Manager**).
2. Click **Add Server**.
3. Select the SQL server from the list or enter the IP address of the SQL Server machine.
4. Provide the appropriate login type:
   - Windows Integrated Security automatically passes Windows account credentials to the SQL server
   - SQL Server user ID and password
5. Click **Connect to Database Server**. The left pane navigation tree populates with your database server information.

Viewing Database Details

Details about your database can be viewed in Database Manager. To maintain peak performance, monitor the value in the **Total Space Used** field. SolarWinds recommends you compact your database as it approaches capacity. If you are using SQL Express, the maximum database size is 4GB.

The **Last Backup** field should also be noted to ensure you are adhering to a regular database maintenance plan. If this field is blank, you do not have a backup of your database.
To view database details:

1. Start Database Manager.
2. Click **Add server** and enter relevant information if your Orion Platform database server is not already listed in the left pane.
3. Expand the list under your Orion Platform database server.
4. Right-click the Orion Platform database, and then select **Database Details**.
5. Review the Properties tab.

**Viewing Table Details**

Details about a table in a selected database can be viewed in Database Manager. The Properties tab includes general statistics pertaining to table size and creation date. The Columns tab describes table columns, keys, and field types. The Indexes tab provides a list of indexes used within the table.

**To view table details:**

1. Start Database Manager.
2. Click **Add server** and enter relevant information if your Orion Platform database server is not already listed in the left pane.
3. Expand the list under your Orion Platform database server.
4. Expand the list of tables under the Orion Platform database.
5. Right-click a table, and then select **Table Details**.
6. Click the Properties, Columns, or Indexes tabs to view details about respective aspects of your table.
Appendix C: Using the Database Management Tools

Moving a Database with SQL Server Management Studio

The following topics walk you through the creation of a backup of your current SolarWinds database(s) and restoring the, if needed, as part of the process of moving the database to a different SQL Server host.

**Note:** Shutdown the SolarWinds services with the Orion Service Manager (SolarWinds Orion > Advanced Features) service before you begin backing up your database.

**Creating a Database Backup File with SQL 2000 Enterprise Manager**

**Creating a Database Backup File with SQL Server Management Studio**

Complete the following procedure if your new database server uses SQL Server 2008.

To backup your Orion database using SQL Server Management Studio:

1. Log on to the new database server using an administrator account.

2. Click Start > All Programs > Microsoft SQL Server 200X > SQL Server Management Studio.

3. Specify the server name of the current SolarWinds Orion Platform database server on the Connect to Server window.

4. If you are using SQL Server Authentication, click SQL Server Authentication in the Authentication field, and then specify your credentials in the User name and Password fields.

5. Click Connect.

6. In the pane on the left, expand the name of the server hosting the SQL instance you are using for SolarWinds NCM, and then expand Databases.

7. Right-click the name of your SolarWinds Orion Platform database (for example, right-click NCM_database), and then click Tasks > Back Up.

8. In the Source area, select Full as the Backup type.

9. In the Backup set area, provide an appropriate Name and Description for your database backup.
10. If there is not already an appropriate backup location listed in the Destination area, click Add, and then specify and remember the destination path and file name you provide. This is the location where your backup is stored.

   **Note:** Remember, if your database is on a remote server, as recommended, this backup file is also created on the remote database server. It is not created locally.

11. Click **Options** in Select a page pane on the left.
12. In the Reliability area, check **Verify backup when finished**.
13. Click **OK**.
14. Copy the .bak file from your current SolarWinds Orion Platform database server to your new database server.
Appendix C: Using the Database Management Tools

**Restoring Backup Files to SQL Server 2008 and 2012**

The following procedures walk you through the restoration of your SolarWinds database backup file on your new database server.

*Restoring a Database Backup File for SQL Server 2008*

*Restoring a Database Backup File for SQL Server 2012*

**Restoring a Database Backup File for SQL Server 2008**

Complete the following procedure if you are restoring your SolarWinds database backup file to a database server running SQL Server 2008.

To restore your database backup file on a server running SQL Server 2008:

1. Log on to the new database server using an administrator account.
2. Click **Start > All Programs > Microsoft SQL Server 2008 > SQL Server Management Studio**.
3. Click **File > Connect Object Explorer**.
4. Specify the name of the new SolarWinds database server on the Connect to Server window.
5. If you are using SQL Server Authentication, click **SQL Server Authentication** in the Authentication field, and then specify your credentials in the User name and Password fields.
6. Click **Connect**.
7. Click the name of your server to view an expanded list of objects associated with your server, and then right-click Databases.
8. Click **Restore Database**.
9. Leave **To database** blank.
10. Select **From device**, and then click **Browse (...)**.
11. Confirm that **File** is selected as the Backup media.
12. Click **Add**.
13. Navigate to the .bak file, select it, and then click **OK**.
14. Click **OK** on the Specify Backup window.
15. In the Destination for restore area, select the name of your database from the To database field.

   **Note:** The **To database** is now populated with the correct name. For example, select NCM_database.

16. Check **Restore** next to the database backup you are restoring.

17. Click **Options** in the left **Select a page** pane.

18. Check **Overwrite the existing database** (WITH REPLACE).

19. For each Original File Name listed, complete the following steps to ensure a successful restoration:

   a. Click **Browse (…)**.
   
   b. Select a directory that already exists.
   
   c. Provide a name for the Restore As file that matches the Original File Name, and then click **OK**.

20. Select **Leave the database ready to use by rolling uncommitted transactions**(RESTORE WITH RECOVERY), and then click **OK**.


22. Select **Database** and follow the prompts.

   **Note:** Due to the nature of security identifiers (SIDs) assigned to SQL Server 2008 database accounts, SolarWinds recommends that you create and use a new account for accessing your restored Orion database on the Database Account window of the Orion Configuration Wizard.

---

**Restoring a Database Backup File for SQL Server 2012**

Microsoft has fully documented the process and requirements for restoring a database backup file to SQL Server 2012. Due to the number of potential database sources and the fact that the database upgrade itself is automatic, consult the Microsoft article, "[Restore a Database backup (SQL Server Management Studio)](https://docs.microsoft.com/en-us/sql-server/the-sql-server-management-studio-desktop-application/restore-a-database-backup)" for fully detailed requirements and instructions.
Appendix C: Using the Database Management Tools

**Updating SolarWinds NCM to Use the New Database Server**

After you have restored your SolarWinds database backup file, you must update your SolarWinds NCM server to recognize the restored database on the new database server, as shown in the following procedure.

**Note:** In general, SolarWinds recommends that you use SQL Server Authentication with the **SA** login and password to ensure that SolarWinds NCM can always access your SQL Server database, even when it is hosted remotely on a separate server.

**To update SolarWinds NCM to use a new database:**

1. Log in to your NCM server.
2. Start the SolarWinds Configuration Wizard.
3. Select **Database**, and then click **Next**.
4. Specify your new database server in the SQL Server field.
5. **If you want to use SQL authentication**, check **Use SQL Server Authentication**, and then provide the appropriate credentials.
   
   **Note:** SolarWinds recommends that you use the SA login and password for your database server to ensure that you are able to properly configure the Orion database user account.

6. Click **Next**.
7. Select Use an existing database, select or type the Existing Database name, and then click **Next**.
8. If you are prompted to use the existing database, click **Yes**.
9. Select **Create a new account**, and then provide a New Account name.

**Notes:**

- Creating a new account ensures that SolarWinds NCM has required access to your database.
- The New Account must be a member of the securityadmin server role.
- The sysadmin role and the SA user account are always members of securityadm.
10. Provide and confirm an account Password.

11. Click **Next** to start database configuration, and then click Finish to exit the Configuration Wizard.
Appendix D: Monitoring SNMP Traps

SNMP traps signal the occurrence of significant events by sending unsolicited SNMP messages to a monitoring device. The SolarWinds Trap Server listens for incoming trap messages on UDP port 161 and then decodes, displays, and stores the messages in the SolarWinds Orion Platform database. The SolarWinds Trap Service allows SolarWinds NCM to receive and process SNMP traps from any type of monitored network device, and, because the SolarWinds Trap Service is multi-threaded, it can handle large numbers of simultaneously incoming traps.

You can view SNMP traps in the Trap Viewer application. The Trap Viewer application allows you to configure trap-specific alerts, to view and search traps, and to apply powerful trap filtering.

**Note:** When configuring devices to send SNMP traps, confirm that traps are sent to the IP address assigned to the SolarWinds NCM server. To ensure proper configuration, refer to the documentation supplied by the vendor of your devices.

- [The SNMP Trap Protocol](#)
- [Configuring the Trap Viewer](#)
- [Configuring Trap Viewer Filters and Alerts](#)
- [Available Trap Alert Actions](#)
- [Working with Traps](#)
The SNMP Trap Protocol

SNMPv1 (Simple Network Management Protocol) and SNMPv2c, along with the associated Management Information Base (MIB), allow you to take advantage of trap-directed notification. When monitoring a large number of devices, where each device may have a large number of its own connected objects, it can become impractical to request information from every object on every device. Consider having each managed device notify the SolarWinds NCM SNMP Trap Server of any issues without solicitation. In this configuration, a problem device notifies the server by sending a message. This message is known as a trap of the event. After receiving the event, the Trap Viewer displays it, allowing you to choose to take action or automatically trigger an action based on the nature of the event.

Configuring the Trap Viewer

Before you can monitor SNMP traps, the Microsoft SNMP Trap service must be installed and devices must be configure to send traps to the SolarWinds NCM SNMP Trap Server. To ensure proper configuration, refer to the documentation supplied by the vendor of your network devices.

If you want to use the Trap Viewer tool or trigger Real-time configuration change alerts based on traps, ensure the SNMP Trap Service is running. If the SNMP Trap Service is not listed as a running service in the service control manager (services.msc), you can enable Simple Network Management Protocol in the Management and Monitoring Tools through Add/Remove Windows Components in the Add/Remove Programs application.

**Note:** The SNMP port used to monitor traps is UDP port 162.

**Trap Viewer Settings**

Use the following procedure to start and configure the Trap Viewer.

**To start and configure the Trap Viewer:**

1. Click **Start > All Programs > SolarWinds > SolarWinds SNMP Trap Server**.
2. Click **File > Settings**.
3. Select the General tab on the Trap Server Settings window.
4. Adjust the Maximum number of traps to display in Current Traps view to the number you want.

5. If you want to automatically refresh the Current Traps view, select the appropriate option, and then adjust the refresh rate.

6. Adjust the Retain Trap messages for how many days? to set the length of time traps remain in the database.

7. Select the Displayed Columns tab.

8. Use the arrow keys to select and order the columns of information that you want to see in the Current Traps view.

9. Click the Message Parsing tab.

10. If you do not need the domain name from your trap messages, select **Remove Domain Name from DNS Lookups**.

    **Note**: Selecting this option will remove the domain name from your trap messages, and this will help to reduce the size of the database.

---

**Configuring Trap Viewer Filters and Alerts**

The Trap Viewer can be configured to trigger alert actions when trap messages match defined rules. The following steps establish rules to filter trap messages and initiate alert actions as you determine.

**To configure Trap Viewer filters and alerts:**

1. Click **Start > All Programs > SolarWinds SolarWinds Network Configuration Manager > SolarWinds NCM SNMP Trap Server**.

2. Click **View > Alerts / Filter Rules**.

3. If you are creating a new rule, click **Add Rule**.

4. If you are editing an existing rule, select the rule, and then click **Edit Rule**.

5. Select the General tab, and then type a Rule Name.

6. Select **Enabled** to enable the rule.

7. Select appropriate servers from the Apply this Rule to list.

8. Enter the IP addresses or subnets to which this rule applies.

    **Note**: Use the examples listed on this tab to format the list properly.
9. If you want the rule to be limited to messages from specific hosts, domains, or hostname patterns, click DNS Hostname, and then enter a DNS Hostname Pattern.

   **Note:** When Use Regular Expressions in this Rule is selected, regular expressions can be used in place of “like” statements. For more information about regular expressions, see [Regular Expression Pattern Matching](#).

10. If you want the rule to be limited to specific community strings or text within a trap message, click Message, and then enter rules Community String Pattern.

   **Notes:**
   Use the examples listed on this tab to format the list properly.
   When Use Regular Expressions in this Rule is selected, regular expressions can be used in place of “like” statements. For more information about regular expressions, see [Regular Expression Pattern Matching](#).

11. Select the Conditions tab, and then generate trigger conditions for rule application in the text field as follows:

   a. Select appropriate object identifiers and comparison functions from the linked context menus.

   b. Click **Browse (...)** to insert an or condition, to insert an and condition, or to delete a condition.

   c. For more information about how to configure conditions, see [Configuring Real Time Configuration Change Detection](#).

12. If you want to limit rule application to within a specific period of time, select the Time of Day tab, select **Enable Time of Day checking**, enter the time period, and then select days of the week on which to apply the rule.

   **Notes:**
   Enabling time of day checking creates more overhead for the CPU.
   Messages received outside the specified timeframe will not trigger alerts.

13. If you want to suppress alert actions until a specified number of traps arrive that match the rule, select the Trigger Threshold tab, select **Define a**
**Trigger Threshold for this Rule**, and then enter option values as appropriate.

**Note:** When Suspend further Alert Actions for is selected, alert actions are not sent until the specified amount of time has expired. After the time period has expired, only new alerts are sent. All alerts that are suppressed during the time period are discarded.

14. Select the Alert Actions tab.

15. If you are associating a new action to the rule, click **Add New Action**, and then select an action from the list to configure. For more information about alert actions, see **Available Trap Alert Actions**.

16. If you are editing an existing action for the rule, select an action from the list, click **Edit Action**, and then configure the action. For more information about alert actions, see **Available Trap Alert Actions**.

17. Use the arrow buttons to arrange the order in which actions are performed.

   **Note:** Actions are processed in the order that they appear in this list, from top to bottom.

18. If you need to delete an action, select the action, and then click **Delete Action**.

19. Click **OK** to save all changes and return to Trap Viewer Settings.

20. Use the arrow buttons to arrange the order in which the rules are applied.

   **Note:** Rules are processed in the order they appear, from top to bottom.

**Available Trap Alert Actions**

The following list provides definitions of the actions available for each trap alert type. For more information about how to assign alert actions, see **Configuring Trap Viewer Filters and Alerts**.

**Discard the Trap**

   Allows you to delete unwanted traps sent to the SNMP Trap server.

**Tag the Trap**

   Allows you to add a custom tag to received traps. Ensure you include the Tag column in the viewer when assigning a tag.
Flag the Trap with a specific color
   Allows you to assign a specific color to flag traps matching the rule.

Log the Trap to a file
   Allows you to specify a file and a series of variables with which to tag traps sent to the file. Ensure you have already created the log file you want to use. The alert cannot create a file.

Windows Event Log
   Allows you to write a message to the local Windows Event Log or to a remote Windows Event Log.

Forward the Trap
   Allows you to specify the IP address or hostname and the port on which to forward the trap.

Play a sound
   Allows you to play a sound when a matching SNMP trap is received.

Text to Speech output
   Allows you to define a specific speech engine, the speed, pitch, volume, and message to read.

Execute an external program
   Allows you to specify an external program to launch. This action is used when creating Real-time change notifications in SolarWinds NCM.

Execute an external VB Script
   Allows you to launch a VB Script using the selected script interpreter engine and a saved script file.

Send a Windows Net Message
   Allows you to send a net message to a specific computer or an entire domain or workgroup.

Send an E-mail / Page
   Allows you to send an email from a specified account to a specified address, using a specific SMTP server, and containing a customizable subject and message.

Stop Processing Trap Rules
   Stops the processing of SNMP trap rules for the matching trap.
Working with Traps

Trap Viewer collects traps from your network and presents them in a readily reviewable and searchable list so that you can easily monitor network health. The following topics provide a guide to working with trap messages within the Trap Viewer.

Searching for Traps

For information on Orion Platform trap variables, see Appendix A: References in the Orion Common Components Administrator's Guide

Viewing Current Traps

To view current trap messages:

1. Click Start > All Programs > SolarWinds Orion > Trap Viewer.
2. Click View > Current Traps.

Searching for Traps

Collected trap messages may be searched within Trap Viewer. The following steps search for trap messages and format the search results list.

To search the trap message list:

1. Click Start > All Programs > SolarWinds > SolarWinds Network Configuration Manager > SolarWinds NCM SNMP Trap Server.
2. Click View > Search Traps.
3. Enter appropriate search criteria, and then click Search Database.
4. If you want to group messages for easier navigation, select the type of grouping from the Grouping list.
5. If you want to limit the number of messages that are shown, enter or select a number in the Maximum number of messages to display field.
6. If you want to view messages that meet your search criteria as they arrive, select a number for the Auto Refresh every number seconds field.

Note: Auto Refresh is only available when you are viewing current messages. The Date/Time Range must be set to Today, Last 24 Hours, Last 2 Hours, or Last Hour.
Appendix D: Monitoring SNMP Traps

**Trap Alert Variables**

The following variables can be used in trap alert messages within Orion Platform products.

**General Trap Variables**

**Trap Date/Time Variables**

<table>
<thead>
<tr>
<th>Trap Date/Time Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${AbbreviatedDOW}</td>
<td>Current day of the week. Three character abbreviation.</td>
</tr>
<tr>
<td>${AbbreviatedMonth}</td>
<td>Current month of the year. Three character abbreviation.</td>
</tr>
<tr>
<td>${AMPM}</td>
<td>AM or PM corresponding to current time (before or after noon)</td>
</tr>
<tr>
<td>${D}</td>
<td>Current day of the month</td>
</tr>
<tr>
<td>${DD}</td>
<td>Current day of the month (two digit number, zero padded)</td>
</tr>
<tr>
<td>${Date}</td>
<td>Current date. (MM/DD/YYYY format)</td>
</tr>
<tr>
<td>${DateTime}</td>
<td>Current date and time. (MM/DD/YYYY HH:MM format)</td>
</tr>
<tr>
<td>${Day}</td>
<td>Current day of the month</td>
</tr>
<tr>
<td>${DayOfWeek}</td>
<td>Current day of the week.</td>
</tr>
<tr>
<td>${DayOfYear}</td>
<td>Numeric day of the year</td>
</tr>
<tr>
<td>${H}</td>
<td>Current hour</td>
</tr>
<tr>
<td>${HH}</td>
<td>Current hour. Two digit format, zero padded.</td>
</tr>
<tr>
<td>${Hour}</td>
<td>Current hour. 24-hour format</td>
</tr>
</tbody>
</table>
### General Trap Variables

<table>
<thead>
<tr>
<th>Trap Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${LocalDOW}</td>
<td>Current day of the week. Localized language format.</td>
</tr>
<tr>
<td>${LongDate}</td>
<td>Current date. (DAY NAME, MONTH DAY, YEAR format)</td>
</tr>
<tr>
<td>${LongTime}</td>
<td>Current Time. (HH:MM:SS AM/PM format)</td>
</tr>
<tr>
<td>${M}</td>
<td>Current numeric month</td>
</tr>
<tr>
<td>${MM}</td>
<td>Current month. Two digit number, zero padded.</td>
</tr>
<tr>
<td>${MMM}</td>
<td>Current month. Three character abbreviation.</td>
</tr>
<tr>
<td>${MMMM}</td>
<td>Full name of the current month</td>
</tr>
<tr>
<td>${MediumDate}</td>
<td>Current date. (DD-MMM-YY format)</td>
</tr>
<tr>
<td>${MediumTime}</td>
<td>Current time. (HH:MM AM/PM format)</td>
</tr>
<tr>
<td>${Minute}</td>
<td>Current minute. Two digit format, zero padded.</td>
</tr>
<tr>
<td>${MonthName}</td>
<td>Full name of the current month</td>
</tr>
<tr>
<td>${S}</td>
<td>Current second.</td>
</tr>
<tr>
<td>${Second}</td>
<td>Current second. Two digit format, zero padded.</td>
</tr>
<tr>
<td>${Time}</td>
<td>Current Time. (HH:MM format)</td>
</tr>
<tr>
<td>${Year}</td>
<td>Four digit year</td>
</tr>
<tr>
<td>${Year2}</td>
<td>Two digit year</td>
</tr>
</tbody>
</table>

**${Application}**

SolarWinds application information
### Appendix D: Monitoring SNMP Traps

<table>
<thead>
<tr>
<th>Trap Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${Community}</code></td>
<td>Node community string</td>
</tr>
<tr>
<td><code>${Copyright}</code></td>
<td>Copyright information</td>
</tr>
<tr>
<td><code>${DNS}</code></td>
<td>Fully qualified node name</td>
</tr>
<tr>
<td><code>${Hostname}</code></td>
<td>Host name of the device triggering the trap</td>
</tr>
<tr>
<td><code>${IP}</code></td>
<td>IP address of device triggering alert</td>
</tr>
<tr>
<td><code>${IP_Address}</code></td>
<td>IP address of device triggering alert</td>
</tr>
<tr>
<td><code>${Message}</code></td>
<td>Message sent with triggered trap and displayed in Trap Details field of Trap Viewer</td>
</tr>
<tr>
<td><code>${MessageType}</code></td>
<td>Name or type of trap triggered</td>
</tr>
<tr>
<td><code>${Raw}</code></td>
<td>Raw numerical values for properties sent in the corresponding incoming trap</td>
</tr>
<tr>
<td><code>${RawValue}</code></td>
<td>Raw numerical values for properties sent in the corresponding incoming trap. The same as <code>${Raw}</code></td>
</tr>
</tbody>
</table>
Appendix E: Monitoring Syslog Messages

Syslog messages are Real-time messages network devices generate to notify you about specific device events. The SolarWinds Syslog Service allows you to receive and process Syslog messages from any type of network device. Because the SolarWinds Syslog Service has the ability to open multiple connections, it can handle large numbers of simultaneously incoming Syslog messages.

The Syslog Server allows you to view, acknowledge, and alert on Syslog messages you receive. By utilizing the built-in flexible message filtering, you can easily create message-specific alerts.

**Note:** When configuring network devices to send Syslog messages, confirm that messages are sent to the IP address assigned on which the Syslog Server is installed. To ensure proper configuration, refer to the documentation supplied by the vendor for each network device.

- Understanding the Syslog Protocol
- Configuring Syslog Server
- Using Syslog Server
- Syslog Alert Variables
Appendix E: Monitoring Syslog Messages

Understanding the Syslog Protocol

The Syslog service listens for incoming Syslog messages on UDP port 514 and then decodes, displays, and stores the message in a database. Many network devices can be configured to generate Syslog messages, allowing you to receive and process the messages generated by these network devices. For details on enabling Syslog message on a particular device, refer to the vendor's documentation.

Syslog Priorities

Syslog Priorities

Included at the beginning of each Syslog message is a priority value. The priority value range spans between 0 and 191 and is enclosed in angle bracket (< and >) delimiters. The priority value is calculated using the following formula:

Priority = Facility * 8 + Severity

Syslog Facilities

The facility value is used to determine which process of the machine created the message. Since the Syslog protocol was originally written on BSD Unix, the Facilities reflect the names of UNIX processes and daemons. The following tables list Syslog facilities and levels.

<table>
<thead>
<tr>
<th>Number</th>
<th>Source</th>
<th>Number</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>kernel messages</td>
<td>12</td>
<td>NTP subsystem</td>
</tr>
<tr>
<td>1</td>
<td>user-level messages</td>
<td>13</td>
<td>log audit</td>
</tr>
<tr>
<td>2</td>
<td>mail system</td>
<td>14</td>
<td>log alert</td>
</tr>
<tr>
<td>3</td>
<td>system daemons</td>
<td>15</td>
<td>clock daemon</td>
</tr>
<tr>
<td>4</td>
<td>security/authorization messages</td>
<td>16</td>
<td>local use 0 (local0)</td>
</tr>
<tr>
<td>5</td>
<td>messages generated internally by Syslog</td>
<td>17</td>
<td>local use 1 (local1)</td>
</tr>
</tbody>
</table>
Note: If you are receiving messages from a UNIX system, consider using the User Facility as your first choice. Local0 through Local7 are not used by UNIX and are traditionally used by networking equipment. Cisco routers, for example, use Local6 or Local7.

Syslog Severities

The following table provides a list of Syslog severity levels with descriptions and suggested actions for each.

<table>
<thead>
<tr>
<th>Number</th>
<th>Severity</th>
<th>Suggested Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Emergency</td>
<td>A &quot;panic&quot; condition affecting multiple applications, servers, or sites. System is unusable. Notify all technical staff on call.</td>
</tr>
<tr>
<td>1</td>
<td>Alert</td>
<td>A condition requiring immediate correction, for example, the loss of a backup ISP connection. Notify staff who can fix the problem.</td>
</tr>
</tbody>
</table>
Appendix E: Monitoring Syslog Messages

<table>
<thead>
<tr>
<th>Number</th>
<th>Severity</th>
<th>Suggested Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Critical</td>
<td>A condition requiring immediate correction or indicating a failure in a primary system, for example, a loss of a primary ISP connection. Fix CRITICAL problems before ALERT-level problems.</td>
</tr>
<tr>
<td>3</td>
<td>Error</td>
<td>Non-urgent failures. Relay errors to developers or administrators. Each item must be resolved within a given time.</td>
</tr>
<tr>
<td>4</td>
<td>Warning</td>
<td>Warning messages are not errors, but they indicate that an error will occur if required action is not taken. An example is a file system that is 85% full. Each item must be resolved within a given time.</td>
</tr>
<tr>
<td>5</td>
<td>Notice</td>
<td>Events that are unusual but are not error conditions. These items might be summarized in an email to developers or administrators to spot potential problems. No immediate action is required.</td>
</tr>
<tr>
<td>6</td>
<td>Informational</td>
<td>Normal operational messages. These may be harvested for network maintenance functions like reporting and throughput measurement. No action is required.</td>
</tr>
<tr>
<td>7</td>
<td>Debug</td>
<td>Information useful to developers for debugging an application. This information is not useful during operations.</td>
</tr>
</tbody>
</table>

Configuring Syslog Server

You can use the Syslog Server application for viewing, acknowledging, and triggering alerts in response to Syslog messages on your network.

Syslog Server Settings

Configuring Syslog Viewer Filters and Alerts

Available Syslog Alert Actions
Syslog Server Settings

Use the following procedure as a guide to starting and configuring the Syslog Server.

To start and configure the Syslog Server:

1. Click Start > All Programs > SolarWinds SolarWinds Network Configuration Manager > Syslog Viewer.
2. Click File > Settings.
4. Adjust the Maximum number of messages to display in Current Messages view to show the number of messages you want.
5. If you want to Automatically Refresh the Current Messages View, select the option accordingly, and then position the middle slider to set the refresh rate.
6. Adjust Retain Syslog messages for how many days? to set the length of time Syslog messages should stay in the database.
7. Select the Displayed Columns tab, and then use the arrow keys to select and order the fields of information that you want to see in the Current Messages view.
   
   **Note:** You can make it easier to acknowledge Syslog messages by selecting the Acknowledged column to add to your view. For more information, see Viewing and Acknowledging Current Messages.

   8. If you want to wrap Syslog messages text in the Current Messages view, select **Word wrap long messages**.
   9. If you do not expect to use Syslog Server as your primary viewer for Syslog messages, select the Message Parsing tab, and then complete the following steps:
      
      **Note:** The following data points are saved within the Syslog tables in your SolarWinds database, removing the added data from each record helps you proactively reduce the size of your database.

   10. Select **Remove embedded Date/Time from Syslog Messages**.
   11. Select **Remove Message Type from Syslog Messages**.
   12. Select **Remove Domain Name from DNS Lookups**.
Appendix E: Monitoring Syslog Messages

Configuring Syslog Viewer Filters and Alerts

The Syslog Viewer can be configured to signal Orion N alert actions when Syslog messages that are received from network devices match defined rules. The steps in the following procedure establish rules that filter Syslog messages and initiate alert actions as you determine.

To configure Syslog Viewer filters and alerts:

1. Click Start > All Programs > SolarWinds SolarWinds Network Configuration Manager > Syslog Viewer.
2. Click File > Settings.
3. Click View > Alerts/Filter Rules.
4. If you are creating a new rule, click Add New Rule.
5. If you are editing an existing rule, select the rule, and then click Edit Rule.
6. Select the General tab.
7. Type a Rule Name, and then select Enabled to enable the rule.
8. Select appropriate servers from the Apply this Rule to list.
9. Enter the IP addresses or subnets to which this rule applies.
   
   **Note:** Use the examples listed on this tab to properly format the list.
10. If you want to limit the rule to only messages from specific hosts, domains, or hostname patterns, select the DNS Hostname tab, and then enter a DNS Hostname Pattern.
   
   **Note:** When Use Regular Expressions in this Rule is selected, regular expressions can be used in place of "like" statements. For more information about regular expressions, see Regular Expression Pattern Matching.
11. If you want to limit the rule to only specific message types or text within a Syslog message, select the Message tab, and then enter rules for one or both of Message Type Pattern and Syslog Message Pattern.

**Notes:**

Use the examples listed on this tab to format the list properly.

When Use Regular Expressions in this Rule is selected, regular expressions can be used in place of “like” statements. For more information about regular expressions, see Regular Expression Pattern Matching.
12. Select the Severity / Facility tab, and then select the severity and facility types you want to apply.

   **Note:** By default, all message severities and facilities are selected.

13. If you want to limit rule application to within a specific period of time, select the Time of Day tab, select **Enable Time of Day checking**, enter the time period, and then select days of the week on which to apply the rule.

   **Notes:**
   Enabling Time of Day checking creates more overhead for the CPU.
   Messages received outside the specified timeframe will not trigger alerts.

14. If you want to suppress alert actions until a specified number of messages arrive that match the rule, complete the following procedure:
   a. Select the Trigger Threshold tab.
   b. Select **Define a Trigger Threshold for this Rule**.
   c. Enter option values as appropriate.

   **Note:** When Suspend further Alert Actions for is selected, alert actions are not sent until the specified amount of time has expired. After the time period has expired, only new alerts are sent. All alerts suppressed during the time period are discarded.

15. Select the Alert Actions tab.

16. If you are associating a new action to the rule, click **Add New Action**, and then select an action from the list to configure. For more information about available actions, see [Available Syslog Alert Actions](#).

   **Note:** Syslog alerts use a unique set of variables. For more information about available Syslog variables, see [Syslog Alert Variables](#).

17. If you are editing an existing action for the rule, complete the following steps:
   a. Select an action from the list.
   b. Click **Edit Selected Action**.
   c. Configure the action as appropriate. For more information about available actions, see [Available Syslog Alert Actions](#).
Appendix E: Monitoring Syslog Messages

Note: Syslog alerts use a unique set of variables. For more information about available Syslog variables, see Syslog Alert Variables.

18. If you need to delete an action, select the action, and then click Delete Action.
19. Use the arrow buttons to arrange the order in which actions are performed.
   
   Note: Actions are processed in the order that they appear in this list, from top to bottom.

20. Click OK to save all changes and return to Syslog Viewer Settings.
21. Use the arrow buttons to arrange the order in which the rules are applied.
   
   Note: Rules are processed in the order they appear, from top to bottom.

Available Syslog Alert Actions

The following list provides definitions of the actions available for each Syslog alert type. For more information about how to assign alert actions, see Adding Alert Actions

Discard the Syslog Message
   
   Allows you to delete unwanted Syslog messages sent to the Syslog server.

Tag the Syslog Message
   
   Allows you to add a custom tag to received Syslog messages. Ensure you include the Tag column in the viewer when assigning a tag.

Modify the Syslog Message
   
   Allows you to modify severity, facility, type and contents of a Syslog message.

Log the Message to a file
   
   Allows you to specify a file and a series of variables with which to tag Syslog messages sent to the file. Ensure you have already created the log file you want to use. The alert cannot create a file.

Windows Event Log
   
   Allows you to write a message to the local Windows Event Log or to a remote Windows Event Log.
Available Syslog Alert Actions

**Forward the Syslog message**
Allows you to specify the IP address or hostname and the port on which to forward the Syslog event.

**Send a new Syslog message**
Allow you to trigger a new Syslog message to a specific IP address or hostname, on a specific port, with a customizable severity, facility, and message.

**Send an SNMP Trap**
Allows you to send a trap to an IP address following a specific trap template and using a specific SNMP community string.

**Play a sound**
Allows you to play a sound when a matching Syslog message is received.

**Text to Speech output**
Allows you to define a specific speech engine, the speed, pitch, volume, and message to read.

**Execute an external program**
Allows you to specify an external program to launch. This action is used when creating Real-time change notifications in SolarWinds NCM.

**Execute an external VB Script**
Allows you to launch a VB Script using the selected script interpreter engine and a saved script file.

**Send a Windows Net Message**
Allows you to send a net message to a specific computer or an entire domain or workgroup.

**Send an E-mail / Page**
Allows you to send an email from a specified account to a specified address, using a specific SMTP server, and containing a customizable subject and message.

**Stop Processing Syslog Rules**
Stops the processing of Syslog rules for the matching Syslog message.
Appendix E: Monitoring Syslog Messages

Using Syslog Server

Syslog Server collects Syslog messages from your network and presents them in a readily reviewable and searchable list so that you can easily monitor your network. The following topics provide a guide to working with Syslog messages within the Syslog Server application.

Viewing and Acknowledging Current Messages

Searching for Syslog Messages

Viewing and Acknowledging Current Messages

The main Syslog Server window, Syslog Viewer, makes it easy to view and acknowledge messages. The following procedure views and then acknowledges current Syslog messages.

To view and acknowledge current Syslog messages:

1. Click View > Current Messages.
2. Acknowledge current messages by either of the following methods:
   - Right-click any message, and then select Acknowledge Selected.
   - Add an Acknowledged column to the Syslog Viewer, and then select each message that you want to acknowledge. For more information, see Syslog Server Settings.

Searching for Syslog Messages

Collected Syslog messages may be searched within Syslog Viewer. The following steps both search for Syslog messages and format search results.

To search the Syslog message list:

1. Click View > Search Messages.
2. Enter appropriate search criteria, and then click Search Database.
3. If you want to group messages for easier navigation, select the type of grouping from the Grouping list.

   Note: Messages can be acknowledged in the search results just as they can be acknowledged in the Current Messages view. For more information, see Viewing and Acknowledging Current Messages.
4. If you want to limit the number of messages that are shown, enter or select a number in the Maximum number of messages to display field.

5. If you want to view messages that meet your search criteria as they arrive, select a number for the Auto Refresh every number seconds field.

**Note:** Auto Refresh is only available when you are viewing current messages. The Date/Time Range must be set to Today, Last 24 Hours, Last 2 Hours, or Last Hour.

**Syslog Alert Variables**

The following variables can be used in Syslog alert messages within SolarWinds Network Configuration Manager applications. You must begin each variable with a dollar sign and enclose each variable identifier in curly braces as, for example, `$ObjectName`.

**Syslog Date/Time Variables**

**Other Syslog Variables**

**Syslog Date/Time Variables**

<table>
<thead>
<tr>
<th>Syslog Date/Time Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${AbreviatedDOW}</td>
<td>Current day of the week. Three character abbreviation.</td>
</tr>
<tr>
<td>${AMPM}</td>
<td>AM or PM corresponding to current time (before or after noon)</td>
</tr>
<tr>
<td>${D}</td>
<td>Current day of the month</td>
</tr>
<tr>
<td>${DD}</td>
<td>Current day of the month (two digit number, zero padded)</td>
</tr>
<tr>
<td>${Date}</td>
<td>Current date. (Short Date format)</td>
</tr>
<tr>
<td>${DateTime}</td>
<td>Current date and time. (Windows control panel defined “Short Date” and “Short Time” format)</td>
</tr>
<tr>
<td>${DayOfWeek}</td>
<td>Current day of the week.</td>
</tr>
</tbody>
</table>
### Appendix E: Monitoring Syslog Messages

<table>
<thead>
<tr>
<th>Syslog Date/Time Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${DayOfYear}</td>
<td>Numeric day of the year</td>
</tr>
<tr>
<td>${H}</td>
<td>Current hour</td>
</tr>
<tr>
<td>${HH}</td>
<td>Current hour. Two digit format, zero padded.</td>
</tr>
<tr>
<td>${Hour}</td>
<td>Current hour. 24-hour format</td>
</tr>
<tr>
<td>${LocalDOW}</td>
<td>Current day of the week. Localized language format.</td>
</tr>
<tr>
<td>${LongDate}</td>
<td>Current date. (Long Date format)</td>
</tr>
<tr>
<td>${LocalMonthName}</td>
<td>Current month name in the local language.</td>
</tr>
<tr>
<td>${LongTime}</td>
<td>Current Time. (Long Time format)</td>
</tr>
<tr>
<td>${M}</td>
<td>Current numeric month</td>
</tr>
<tr>
<td>${MM}</td>
<td>Current month. Two digit number, zero padded.</td>
</tr>
<tr>
<td>${MMM}</td>
<td>Current month. Three character abbreviation.</td>
</tr>
<tr>
<td>${MediumDate}</td>
<td>Current date. (Medium Date format)</td>
</tr>
<tr>
<td>${Minute}</td>
<td>Current minute. Two digit format, zero padded.</td>
</tr>
<tr>
<td>${Month}</td>
<td>Full name of the current month</td>
</tr>
<tr>
<td>${N}</td>
<td>Current month and day</td>
</tr>
<tr>
<td>${S}</td>
<td>Current second.</td>
</tr>
<tr>
<td>${Second}</td>
<td>Current second. Two digit format, zero padded.</td>
</tr>
<tr>
<td>${Time}</td>
<td>Current Time. (Short Time format)</td>
</tr>
<tr>
<td>${Year2}</td>
<td>Two digit year</td>
</tr>
<tr>
<td>${Year}</td>
<td>Four digit year</td>
</tr>
</tbody>
</table>
### Other Syslog Variables

<table>
<thead>
<tr>
<th>Syslog Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${Application}</code></td>
<td>SolarWinds application information</td>
</tr>
<tr>
<td><code>${Copyright}</code></td>
<td>Copyright information</td>
</tr>
<tr>
<td><code>${DNS}</code></td>
<td>Fully qualified node name</td>
</tr>
<tr>
<td><code>${Hostname}</code></td>
<td>Host name of the device triggering the alert</td>
</tr>
<tr>
<td><code>${IP_Address}</code></td>
<td>IP address of device triggering alert</td>
</tr>
<tr>
<td><code>${Message}</code></td>
<td>Status of device triggering alert</td>
</tr>
<tr>
<td><code>${MessageType}</code></td>
<td>Assigned alert name</td>
</tr>
<tr>
<td><code>${Release}</code></td>
<td>Release information</td>
</tr>
<tr>
<td><code>${Severity}</code></td>
<td>A network health score providing 1 point for an interface in a warning state, 1000 points for a down interface, and 1 million points for a down node.</td>
</tr>
<tr>
<td><code>${Version}</code></td>
<td>Version of the SolarWinds software package</td>
</tr>
</tbody>
</table>
Appendix F: Creating Custom Properties

Along with all other SolarWinds Orion Platform products, SolarWinds NCM now uses a web-based version of the Custom Property Editor. NCM only supports custom properties written in English.

The following sections provide steps required to manage custom properties:

- Creating a Custom Property
- Assigning Values to a Custom Property
- Importing Custom Property Data
- Removing Custom Properties
- Exporting a Custom Property

Notes:

- Older versions of SolarWinds Orion Core Services used the Custom Property Editor application to create and manage custom properties. The Custom Property Editor is no longer available NCM version 7.1.1 and higher.

- Custom properties are stored in the SolarWinds database. SQL Server treats NULL and 0 differently, so, if you are creating a custom property to trigger an alert, confirm that the alert trigger conditions account for this difference. For more information, see the SolarWinds Knowledge Base article, “Unexpected results when you use advanced alerts on custom properties with NULL values”.

480
Creating a Custom Property

The following procedure provides steps required to create a custom property.

To create a custom property:

1. Log on to the Orion Web Console as an administrator.
2. Click **Settings** in the top right corner of the web console, and then click **Manage Custom Properties** in the Node & Group Management grouping.
3. Click **Add Custom Property**.
4. Select the object type for the property you are creating, and then click **Next**.
   
   **Note:** Available object types will vary depending on the SolarWinds Orion products you have installed, but all installations will allow you to create both Node and Volume custom properties.

5. If you want to create a property based on a predefined template, click the appropriate **Property Template**.
   
   **Note:** Property templates provide generic suggestions in the Property Name and Description fields and an appropriate custom property Format.

6. Enter or Edit the Property Name and Description fields, as appropriate.

   **Notes:**
   
   - To ensure full custom property functionality, do not leave the Property Name field empty.
   - Only English custom property names are supported.
   - Although most non-alphanumeric characters used in custom property names are replaced by underscores (\_) when names are stored in the Orion database, SolarWinds recommends against using non-alphanumeric characters in custom property names. Hash characters (#) are not allowed in any property name.

   NCM ignores custom properties that use words from the list of reserved words. For details, see see [Reserved Words](#).
7. Select a custom property Format, as appropriate.

8. If you want to restrict the possible values that other, non-administrative users can use for the selected property, check Restrict values, and then provide values, as follows:
   a. Enter an appropriate value for Value X.
   b. Click Add Value.
   c. If you need to delete a provided property value, click X next to the property to delete.
   d. Repeat, as needed, until you have supplied all valid property values.

9. Select how the property will be used in NCM. Contexts include Alerts, Filtering, Grouping, Reports, Object Details Views.

10. Click Next.

11. Click Select Objects, and then, using either of the following methods, sort the objects to which you can apply the selected property:
    Select an appropriate Group by: criterion, and then click the appropriate group including the objects to which you want the selected property to apply.
    Use the search tool to search your SolarWinds database for the objects to which you want the selected property to apply.

12. Check all monitored objects to which you want the selected custom property to apply.
    **Note:** Click > to expand listed objects to view available child objects.

13. Click Add to add checked objects to the Selected Objects list.

14. In the Selected Objects list, check all objects to which you want the selected property to apply.

15. If you have selected all objects to which you want the selected property to apply, click Select Objects.

16. For each selected object, select or enter an appropriate property value.

17. If you are editing a property with defined values, you are an administrator, and you want to add a new property value, select Add new value in the dropdown menu, and then provide the New value.
Appendix F: Creating Custom Properties

18. If you want to apply the selected property to a different group of objects, click **Add more**, and then select objects as indicated above.

19. If you have selected values for all objects to which you want the selected property to apply, click **Submit**.

**Assigning Values to a Custom Property**

The following procedure provides steps required to assign new values to an existing custom property.

**To assign custom property values:**

1. Log on to the Orion Web Console as an administrator.

2. Click **Settings** in the top right corner of the web console, and then click **Manage Custom Properties** in the Node & Group Management grouping.

3. Select the custom property for which you want to assign values, and then click **Assign values**.

4. Click **Select Objects**, and then, using either of the following methods, sort the objects to which you can apply the selected property:

   Select an appropriate Group by: criterion, and then click the appropriate group including the objects to which you want the selected property to apply.

   Use the search tool to search your SolarWinds database for the objects to which you want the selected property to apply.

5. Check all monitored objects to which you want the selected custom property to apply.

   **Note:** Click > to expand listed objects to view available child objects.

6. Click **Add** to add checked objects to the Selected Objects list.

7. In the Selected Objects list, check all objects to which you want the selected property to apply.

8. If you have selected all objects to which you want the selected property to apply, click **Select Objects**.

9. For each selected object, select or enter an appropriate property value.
10. If you are editing a property with defined values, you are an administrator, and you want to add a new property value, select Add new value in the drop-down menu, and then provide the New value.

11. If you want to apply the selected property to a different group of objects, click Add more, and then select objects as indicated above.

12. If you have selected values for all objects to which you want the selected property to apply, click Submit.

**Importing Custom Property Data**

After you have defined custom properties, it is possible to import corresponding values from an external document, if it is correctly formatted. For example, you may already possess a spreadsheet listing the asset tags of all your network nodes, and you would like to have this information available for reporting and publication in the web console. In this scenario, Asset Tag is added as a custom property, and then the import wizard is used to populate the asset tag values from the spreadsheet. The following steps outline the process for importing custom properties data.

To import custom property data:

1. Log on to the Orion Web Console as an administrator.
2. Click **Settings** in the top right corner of the web console, and then click **Manage Custom Properties** in the Node & Group Management grouping.
3. Click **Import**.
4. Click **Browse**, and then navigate to your custom property data file.
5. Select the type of object for which you are importing values.

   **Note:** For best results, format your data as tables and provide titles in your data file that match the existing custom properties you are populating.

6. Click **Next**.
7. For each detected Spreadsheet Column, select the corresponding Orion Database Column, and then select the appropriate Relationship between the indicated columns.

   **Notes:**
Appendix F: Creating Custom Properties

At least one column must match, for corresponding entries, between your spreadsheet and the Orion database column. Select the matches Relationship option for this key data.

The imports to Relationship option overwrites any existing data in the corresponding Orion Database Column.

8. Click Import.

Removing Custom Properties

Custom properties are easily removed, as shown in the following procedure.

To remove a custom property:

1. Log on to the Orion Web Console as an administrator.
2. Click Settings in the top right corner of the web console, and then click Manage Custom Properties in the Node & Group Management grouping.
3. Check each property you want to remove, and then click Delete.
4. Confirm your selection by clicking Delete when prompted.

Exporting a Custom Property

With the Export Custom Properties feature, you can download a spreadsheet of any selected custom property, as it is stored in your SolarWinds database.

To export a custom property:

1. Log on to the Orion Web Console as an administrator.
2. Click Settings in the top right corner of the web console, and then click Manage Custom Properties in the Node & Group Management grouping.
3. Check the property you want to export, and then click Export.
4. If you want to select values for only a subset of all monitored objects for which the selected custom property is defined, click Select Objects, select the objects for which you want property values, and then click Select Objects.
5. Select the columns you would like to export.
6. Choose a file type for the exported file, and then click Export.
7. The exported file is saved with the filename exportCP in the locally designated downloaded files folder for your web console browser.
Appendix G: Configuring Automatic Login

The SolarWinds NCM Web Console allows you to log in using any of the following methods:

- Windows Pass-through Security. If you choose to employ Windows Pass-through Security, SolarWinds NCM users can be authenticated through Windows Security, with no need to log in using a separate SolarWinds NCM Account or User Name and Password. For more information, see Using Windows Pass-through Security
- DirectLink. If a DirectLink account is activated, any URL referring directly to an Orion Web Console page will bypass the Orion Web Console login page by logging the user into the DirectLink account. For more information, see Using the DirectLink Account.
- URL Pass-through. For more information, see Passing Login Information Using URL Parameters.

SolarWinds NCM prioritizes user login in the following manner:

1. Windows Active Directory Authentication is enabled. To enable Windows Active Directory Authentication, select the Windows Authentication option when configuring the Orion Web Console in the Configuration Wizard.
2. The Account or User ID and Password passed on the URL.
3. The Account or User ID and Password entered on the login.aspx page.
4. The Windows User if IIS NT Security is enabled, logging the user in using NT Security.
5. The Windows Domain to which the User belongs, for example, Development\Everyone.
6. The presence of a DirectLink Account.
Appendix G: Configuring Automatic Login

Using Windows Pass-through Security

On all Orion Platform products released before SolarWinds NPM version 10.1, you may take advantage of the Windows Pass-through Security functionality when IIS NT Security is enabled. SolarWinds NCM users can be authenticated through Windows Security, with no need to log in using a separate SolarWinds NCM account or User Id and Password. Pass-through Security can be configured to employ either Domain or Local computer security. Both may also be used at the same time. The SolarWinds Network Configuration Manager Account or User ID and Passwords must then be set up to match the Account or User ID and Passwords that are used for the Domain and/or Local computer security. Use the following procedure to enable IIS NT Security for logging in to the Orion Web Console with Windows Pass-through Security.

Notes:

- With the release of SolarWinds NPM 10.1, Orion Web Console users may be authenticated using Active Directory.

- When authenticating users with Windows Security, ensure your Orion server uses the NetBIOS domain name, instead of the fully qualified domain name.

To enable IIS NT security for Windows Pass-through Security:

1. If you are using NT Domain Authentication Format for pass-through accounts, create these pass-through accounts in the Orion Web Console Account Manager using Domain\UserID as the User Name, as follows:
   - Washington\Edward
   - StLouis\Bill

   Note: For more information about creating accounts using the Orion Web Console Account Manager, see Creating a New Account.
2. If you are using Local Computer Authentication Format for pass-through accounts, create these accounts in the Orion Web Console Account Manager using Computer\UserID as the User Name, as follows:

SolarWindsS2\Edward
Server3\JonesR

**Note:** For more information about creating accounts using the Orion Web Console Account Manager, see [Creating a New Account](#).

3. Click **Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager.**

4. If you are using Windows Server 2003, complete the following steps:
   a. Expand **Internet Information Services > Local Computer > Web Sites** in the left pane.
   b. Select **SolarWinds NetPerfMon.**
   c. Click **Action > Properties.**
   d. Click the Directory Security tab.
   e. Click **Edit** within the Authentication and access control area.
   f. Clear **Enable anonymous access.**
   g. Select **Integrated Windows authentication** in the Authenticated access group.
   h. Click **OK** to close the Authentication Methods window.
   i. Click **Apply**, if available, and then click **OK** to close the SolarWinds NetPerfMon Properties window.
   j. Collapse Internet Information Services > Local Computer > Web Sites.
   k. Collapse Internet Information Services > Local Computer in the left pane.
   l. Click **Action > All Tasks > Restart IIS.**
   m. Confirm that **Restart Internet Services on Local Computer** is selected, and then click **OK.**
   n. Close the IIS Manager.
5. If you are using Windows Server 2008, complete the following steps:
   a. Click Start > Administrative Tools > Server Manager.
   b. Expand Roles.
   c. Click Web Server (IIS).
   d. In the Role Services area, confirm that Web Server > Security > Windows Authentication is installed.
   e. If Windows Authentication is not installed, click Add Role Services, select Web Server > Security > Windows Authentication, click Next, and then complete the service installation.
   f. Click Start > Administrative Tools > Internet Information Services (IIS) Manager.
   g. Select your Orion server in the left pane.
   h. Click Authentication in the IIS group of the main pane.
   i. Right-click Anonymous Authentication, and then click Disable.
   j. Right-click Windows Authentication, and then click Enable.
   k. Click your Orion server, and then click Restart in the Actions pane.

6. Close the IIS Manager.

7. Log in to the Orion Web Console using the Windows account credentials you have already established.

Passing Login Information Using URL Parameters

The user ID and password can be passed as parameters within the URL. This allows you to create a favorite or bookmark within a browser, or on your desktop. Create a favorite with a link in the following form to pass the login information:


Provide the hostname or IP address of your Orion server as the DOMAIN. Provide your Orion User ID as the USER, and then provide your Orion user account password as the PASSWORD.

Warning: HTTP requests are not encrypted, so User IDs and Passwords sent in HTTP requests are not secure. For more information about enabling HTTPS on your Orion server, consult www.microsoft.com.
Using the DirectLink Account

Enabling a DirectLink account allows you to make direct hyperlinks to specific web console views available to individuals who do not already have Orion Web Console user accounts. Any URL referring directly to an SolarWinds NCM web page bypasses the login screen, logging the user into the DirectLink account. The DirectLink account is created like any other account, and it can include custom views and account limitations. For more information web console accounts, see Creating a New Account.

To enable a DirectLink account for the Orion Web Console:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings in the top right of the web console, and then click Manage Accounts in the Accounts grouping.
3. Click Add.
4. Type DirectLink as the new User Name.
5. Type a Password, confirm it, and then click Submit.
6. Edit DirectLink account options, as necessary, for your installation of SolarWinds Network Performance Monitor. For more information about editing account options, see Editing an Orion User Account.
7. Create a custom view to be used as the home page of the DirectLink account.
8. Specify the new DirectLink view as a default view in Account Manager. For more information, see Editing an Orion User Account.