Copyright © 2016 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 7.5, revised 8/29/2016
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.

Contact SolarWinds

<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>
# Table of Contents

**Introduction to SolarWinds NCM** ................................................................. 26
  - Why should I install SolarWinds NCM? ......................................................... 26
  - Key features of SolarWinds NCM ................................................................. 27
  - How does SolarWinds NCM work? ............................................................... 29

**Installation** .................................................................................................. 30
  - Single server standalone: installation or upgrade ........................................ 30
  - Single server integrated: upgrade only ....................................................... 30
  - Requirements ............................................................................................... 30
    - Additional information ............................................................................... 35
  - Scalability ..................................................................................................... 35
  - Server sizing ............................................................................................... 36

**Install SolarWinds NCM** ............................................................................ 36
  - Orion platform products: integration support ............................................. 37
  - About the Orion platform database ............................................................ 37

**License your product with Internet access** .................................................. 38
  - License your product without Internet access ............................................ 39

**Upgrade SolarWinds NCM** ....................................................................... 39
  - Stop SolarWinds NCM Jobs .......................................................................... 39
  - Stop jobs that are running before upgrading ............................................ 39
  - Stop the SCP Server tray application before upgrading .......................... 40

**Launch the SolarWinds NCM installer** ....................................................... 40
  - Additional polling engine and web console ............................................... 41
Install or upgrade an additional poller .......................................................... 41
Install or upgrade an additional web console .................................................. 42
Set node communication defaults .................................................................. 43
Set node communication default parameters .................................................. 44
Override default settings for a specific node ................................................... 44
Define and apply global device logins .............................................................. 44
Set communication limits ............................................................................. 45
Log events for a detailed record of SolarWinds NCM functions ....................... 45
Enable SSL communication with SolarWinds NCM ........................................ 45
Repair SolarWinds NCM .............................................................................. 46
Move SolarWinds NCM to another computer .................................................. 47
Uninstall SolarWinds NCM ........................................................................... 48
About the SolarWinds Orion database ............................................................. 48
SNMP communication .................................................................................. 49
SolarWinds NCM licensing ............................................................................ 49
  Activate your SolarWinds license ................................................................. 49
    Activate licenses with Internet access ......................................................... 50
    Activate licenses offline .......................................................................... 51
License keys .................................................................................................. 51
Review your NCM license ............................................................................. 52
Maintain licenses ......................................................................................... 52
License Manager requirements ....................................................................... 53
Install License Manager ................................................................................ 54
Activate licenses with the License Manager .................................................. 54
Deactivate and reactive licenses .................................................................... 56
Upgrade and synchronize licenses ................................................................. 58

Get started with NCM .................................................................................. 59

SNMP communication ................................................................................ 59

Add nodes to NCM ........................................................................................ 59

Add an individual node ................................................................................ 59

Add nodes via Network Discovery ............................................................... 60

Select network devices for monitoring in NCM ........................................... 63

Select the results of a network discovery ..................................................... 63

Common tasks ............................................................................................... 65

Schedule daily backups of config files ....................................................... 65

Change the community string on multiple nodes ...................................... 65

Verify success by comparing configs ......................................................... 66

Block a MAC address on a wireless access point ...................................... 66

Back up the running configuration ............................................................. 67

Block a MAC address on a wireless access point ...................................... 67

Verify success by comparing configs ......................................................... 68

Change an interface description ............................................................... 68

Back up the running configuration ............................................................. 68

Update the interface descriptions ............................................................. 68

Verify success by checking the interface description ............................... 69

Upgrade IOS and firmware ......................................................................... 70

Back up the running configuration ............................................................. 70

Push an IOS image to a network device .................................................... 70

Block all private addresses with an access control list ............................. 71

Back up the running configuration ............................................................. 71
Update the access control list for a group of nodes .......................................................... 72
Verify success by comparing configs ................................................................................. 73
Customize the login banner of a device .............................................................................. 73
Modify the login banner ....................................................................................................... 73
Verify success by comparing configs ................................................................................. 74

**Node management** ........................................................................................................ 75

Manage SolarWinds NCM nodes ......................................................................................... 75
Find a specific node .............................................................................................................. 75
Add or edit a node ................................................................................................................ 75
View node interface details ................................................................................................. 76
View the interface details of a specific node ....................................................................... 76

**Firmware vulnerability data** .......................................................................................... 76

View firmware vulnerability reports ................................................................................... 77
Troubleshoot firmware vulnerability reports ....................................................................... 79
Vulnerability summary ......................................................................................................... 79
Access firmware vulnerability settings ................................................................................. 80
Add firmware vulnerability files ........................................................................................ 80
Save an XML source to your SolarWinds NCM server ..................................................... 80
Access firmware vulnerability settings ................................................................................. 81
Change the vulnerability announcements folder .............................................................. 81
Add direct URLs .................................................................................................................. 81
Download firmware vulnerability data and import into SolarWinds NCM ......................... 81
Verify the vulnerability announcements folder ................................................................... 81
Download firmware vulnerability data and import into SolarWinds NCM ......................... 82
Manage end of support and end of sales (EOS) ................................................................ 82
Refresh EOS dates ........................................................................................................................................... 82
Assign EOS dates .................................................................................................................................................. 83
Ignoring Devices in EOS Management .................................................................................................................. 83
Export EOS information ........................................................................................................................................ 84
Filter EOS data ....................................................................................................................................................... 84
Delete EOS data ...................................................................................................................................................... 85
Search for network addresses ............................................................................................................................... 85
  Find IP addresses .................................................................................................................................................. 85
  Find MAC addresses .............................................................................................................................................. 85
  Find hostnames ................................................................................................................................................... 85
  How does SolarWinds NCM find addresses? ........................................................................................................ 86
SolarWinds NCM macros ......................................................................................................................................... 87
  Supported macro types .......................................................................................................................................... 87
Custom macros ......................................................................................................................................................... 88
  Access custom macros .......................................................................................................................................... 88
  Create a custom macro ....................................................................................................................................... 88
  Edit a custom macro ............................................................................................................................................ 88
  Delete a custom macro ....................................................................................................................................... 89
Find connected port for a host: SolarWinds NPM integration .................................................................................. 89
  Search for connected ports ................................................................................................................................ 89
Unmanage and remanage nodes ............................................................................................................................. 91
  Access the management page ............................................................................................................................ 91
  Unmanage nodes ................................................................................................................................................ 91
  Remanage nodes ................................................................................................................................................ 91

Manage Orion Web Console user accounts ......................................................................................................... 92
Create users ........................................................................................................................................92
Create users based on existing Active Directory or local domain accounts ..........................94
Set user account access ..................................................................................................................96
Limit users to specific network areas .............................................................................................98
Set user level login credentials ......................................................................................................99
Restrict user access to network areas by applying limitations .....................................................99
Using the Account Limitation Builder ..........................................................................................100
Create limitations based on custom properties ..........................................................................100
Delete account limitations .............................................................................................................101
Patterns for limitations ..................................................................................................................101
Set default menu bars and views for users ....................................................................................102
Configuring audible web alerts .......................................................................................................103
Change account passwords ............................................................................................................104

**Configuration files** .....................................................................................................................106
Setup required for Binary Configs ....................................................................................................106
Download configuration files in NCM ............................................................................................107
  Downloading from a single node ....................................................................................................107
  Downloading from multiple nodes ..................................................................................................108
Enable a new config type ..................................................................................................................108
  Enable a new config type for a device ..........................................................................................109
Enable the config and policy caches ...............................................................................................109
Edit config files ...............................................................................................................................109
  Upload the edited config file ........................................................................................................110
Troubleshooting: Confine recognition of the command prompt during download ....................110
Compare configs ...............................................................................................................................110
<table>
<thead>
<tr>
<th>Feature</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define comparison criteria</td>
<td>111</td>
</tr>
<tr>
<td>Create a new regular expression</td>
<td>112</td>
</tr>
<tr>
<td>Edit a regular expression</td>
<td>112</td>
</tr>
<tr>
<td>Enable or disable a regular expression</td>
<td>112</td>
</tr>
<tr>
<td>Delete a regular expression</td>
<td>112</td>
</tr>
<tr>
<td>Comparison criteria: exclusion examples</td>
<td>112</td>
</tr>
<tr>
<td>Comparison results overview</td>
<td>113</td>
</tr>
<tr>
<td>Execute a script on a node</td>
<td>113</td>
</tr>
<tr>
<td>View the results</td>
<td>114</td>
</tr>
<tr>
<td>Upload a config</td>
<td>114</td>
</tr>
<tr>
<td>Upload a config to one or more nodes</td>
<td>115</td>
</tr>
<tr>
<td>Import config files</td>
<td>115</td>
</tr>
<tr>
<td>Import a config file</td>
<td>115</td>
</tr>
<tr>
<td>What is a baseline?</td>
<td>115</td>
</tr>
<tr>
<td>Set a baseline</td>
<td>116</td>
</tr>
<tr>
<td>Remove a config file as a baseline</td>
<td>116</td>
</tr>
<tr>
<td>Baseline your entire network</td>
<td>116</td>
</tr>
<tr>
<td>Clear all baselines to reset the comparison point for config changes</td>
<td>117</td>
</tr>
<tr>
<td>Upload configuration changes</td>
<td>118</td>
</tr>
<tr>
<td>Upload an entire configuration</td>
<td>118</td>
</tr>
<tr>
<td>Create a config archive for local or network storage</td>
<td>118</td>
</tr>
<tr>
<td>Create a config archive for local storage</td>
<td>118</td>
</tr>
<tr>
<td>Create a config archive for network storage</td>
<td>119</td>
</tr>
<tr>
<td>Real time change detection</td>
<td>120</td>
</tr>
<tr>
<td>Real time change detection requirements</td>
<td>120</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Configure real time change detection</td>
<td>121</td>
</tr>
<tr>
<td>Access real-time change detection settings</td>
<td>121</td>
</tr>
<tr>
<td>Step 1: Manually configure your devices to send syslog or trap messages</td>
<td>121</td>
</tr>
<tr>
<td>Step 2: Configure alerts and filters triggered by syslog and trap messages</td>
<td>122</td>
</tr>
<tr>
<td>Step 3: Config changes</td>
<td>127</td>
</tr>
<tr>
<td>Step 4: Config downloads and notifications</td>
<td>127</td>
</tr>
<tr>
<td>Step 5: Enter NCM SMTP server details</td>
<td>127</td>
</tr>
<tr>
<td>Step 6: Enable real time config change notifications</td>
<td>128</td>
</tr>
<tr>
<td>Limit real time notification download operations</td>
<td>128</td>
</tr>
<tr>
<td>Run syslog and trap services as administrator</td>
<td>128</td>
</tr>
<tr>
<td>Search for config files in the web console</td>
<td>128</td>
</tr>
<tr>
<td>Delete config files from the database</td>
<td>129</td>
</tr>
<tr>
<td>Automate config file purges</td>
<td>129</td>
</tr>
<tr>
<td><strong>Device templates</strong></td>
<td>131</td>
</tr>
<tr>
<td>Gather the information you need</td>
<td>131</td>
</tr>
<tr>
<td>Best practices for device command templates</td>
<td>134</td>
</tr>
<tr>
<td>Communication process diagrams</td>
<td>137</td>
</tr>
<tr>
<td>Create Device Templates in NCM</td>
<td>138</td>
</tr>
<tr>
<td>Create a device template with the interactive wizard</td>
<td>139</td>
</tr>
<tr>
<td>Create a device template with the XML editor</td>
<td>139</td>
</tr>
<tr>
<td>Edit a device template</td>
<td>140</td>
</tr>
<tr>
<td>Edit a device template with the interactive wizard</td>
<td>140</td>
</tr>
<tr>
<td>Edit a device template with the XML editor</td>
<td>140</td>
</tr>
<tr>
<td>Confirm the device template is working</td>
<td>141</td>
</tr>
<tr>
<td>Sample CLI device command templates</td>
<td>141</td>
</tr>
</tbody>
</table>
Cisco IOS example ..................................................................................................................142
Nortel BayStack 380 example ..............................................................................................142
SCP example of config upload and download ........................................................................143
Create a menu-based command template ...........................................................................144
Command template commands ............................................................................................148
Pre-command and command template variables ...................................................................151
  Pre-command device template entry example ....................................................................153
  Preclude pseudoterminal setup with command template variables ....................................153
  Declare a special command prompt with command template variables ............................154
  Switch user context with command template variables ......................................................154
  Respond to post-login interaction requests with command template variables .................154
Troubleshoot device connections ..........................................................................................155
F5 device template behavior ..................................................................................................155
  Device setup prerequisites ..................................................................................................155
  Template details ................................................................................................................156

Command scripts ..................................................................................................................157
  Creating an executable command script .............................................................................157
  Use variables in scripts ......................................................................................................157
  Example variable script .....................................................................................................158
    Define script variables ......................................................................................................158
    Reference variables with variables ..................................................................................158
    Troubleshoot script execution ..........................................................................................159

Managing Inventory ..............................................................................................................160
  Run an inventory scan .........................................................................................................160
  Run a complete inventory scan ..........................................................................................160
Run an inventory scan on a single node ................................................................. 160
Schedule an inventory scan ................................................................................... 161
Adjust inventory settings ....................................................................................... 161
View inventory status ............................................................................................. 162

Policy reports .......................................................................................................... 163
Create a policy report in SolarWinds NCM ............................................................. 163
Schedule a policy report ......................................................................................... 164
Remediating a policy violation ................................................................................ 164
Export a policy report to thwack .......................................................................... 165
Export a policy report as a file ............................................................................... 165
Edit a policy report ................................................................................................. 165
Delete a policy report .............................................................................................. 165
Configuring DISA STIG reports ............................................................................. 166
Creating a DISA STIG Dashboard .......................................................................... 166
Rules ........................................................................................................................ 166
Customize Policy Violation Levels ....................................................................... 167
Create a policy rule ................................................................................................. 168
Basic string matching ............................................................................................. 168
Advanced string matching ....................................................................................... 169
Edit a policy rule ..................................................................................................... 171
Delete a policy rule ................................................................................................ 171
Policies ..................................................................................................................... 172
Create a policy ........................................................................................................ 172
Edit a policy ............................................................................................................ 172
Delete a policy ........................................................................................................ 172
Enable the config and policy caches ...............................................................173
Manually refresh the policy cache ...............................................................173

Jobs ..................................................................................................................174
Create or edit a job ..........................................................................................174
Enable a Job ......................................................................................................175
Disable a job ......................................................................................................175
Start a job .........................................................................................................175
Stopping a Job ..................................................................................................176
View job logs ....................................................................................................176
Delete a job ........................................................................................................176

Approval system for device configuration changes ........................................177
Set up config change approval ........................................................................177
Turn on approval system ..................................................................................178
    Enable config change approval ...................................................................178
    Disable config change approval ..................................................................179
View, approve, and decline approval requests ..................................................179
Create, edit, and delete NCM accounts ............................................................179
    Access account settings ..............................................................................179
    Create a new account ..................................................................................179
    Edit an existing account .............................................................................180
    Delete an account .......................................................................................180
Device access information ................................................................................180
    Third Party Authentication ...........................................................................181

Orion Web Console ..........................................................................................182
Access and log in to the Orion Web Console ....................................................182
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the conditions that must exist to reset an alert</td>
<td>200</td>
</tr>
<tr>
<td>Alert Suppression Example</td>
<td>202</td>
</tr>
<tr>
<td>Build complex conditions</td>
<td>202</td>
</tr>
<tr>
<td>Manage alert actions</td>
<td>203</td>
</tr>
<tr>
<td>Enable and Disable Alerts</td>
<td>203</td>
</tr>
<tr>
<td>Schedule when an alert monitors your environment</td>
<td>204</td>
</tr>
<tr>
<td>Define what happens when an alert is triggered</td>
<td>206</td>
</tr>
<tr>
<td>Add actions to alerts</td>
<td>206</td>
</tr>
<tr>
<td>Add what happens when an alert is not acknowledged</td>
<td>207</td>
</tr>
<tr>
<td>Test alert triggers and actions</td>
<td>208</td>
</tr>
<tr>
<td>Test trigger conditions</td>
<td>208</td>
</tr>
<tr>
<td>Test alert actions while creating or editing an alert</td>
<td>208</td>
</tr>
<tr>
<td>Test alert actions in the Action Manager</td>
<td>209</td>
</tr>
<tr>
<td>Define what happens when the alert is reset</td>
<td>209</td>
</tr>
<tr>
<td>Escalating Alerts</td>
<td>210</td>
</tr>
<tr>
<td>Add an SMTP server</td>
<td>211</td>
</tr>
<tr>
<td>Available alert actions</td>
<td>212</td>
</tr>
<tr>
<td>Change a custom property</td>
<td>213</td>
</tr>
<tr>
<td>Create a ServiceNow incident</td>
<td>213</td>
</tr>
<tr>
<td>Use reference fields</td>
<td>214</td>
</tr>
<tr>
<td>Filter expression examples</td>
<td>214</td>
</tr>
<tr>
<td>Configure a ServiceNow incident</td>
<td>215</td>
</tr>
<tr>
<td>Send an email or page</td>
<td>216</td>
</tr>
<tr>
<td>Play a sound when an alert is triggered</td>
<td>217</td>
</tr>
<tr>
<td>Log the alert message to a file</td>
<td>219</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Log an alert to the Windows Event Log on a specific server</td>
<td>219</td>
</tr>
<tr>
<td>Log the alert to the NPM event log</td>
<td>220</td>
</tr>
<tr>
<td>Change the resource allocation of a virtual machine</td>
<td>221</td>
</tr>
<tr>
<td>Send a syslog message</td>
<td>222</td>
</tr>
<tr>
<td>Execute an external batch file</td>
<td>223</td>
</tr>
<tr>
<td>Execute an external Visual Basic script</td>
<td>223</td>
</tr>
<tr>
<td>Email a web page to users</td>
<td>224</td>
</tr>
<tr>
<td>Create a dynamic URL</td>
<td>225</td>
</tr>
<tr>
<td>Use the speech synthesizer to read alerts</td>
<td>225</td>
</tr>
<tr>
<td>Send a Windows Net message</td>
<td>226</td>
</tr>
<tr>
<td>Send an SNMP trap</td>
<td>227</td>
</tr>
<tr>
<td>Send a GET or POST request</td>
<td>228</td>
</tr>
<tr>
<td>Dial a paging or SMS service</td>
<td>229</td>
</tr>
<tr>
<td>Alert me when a server goes down</td>
<td>229</td>
</tr>
<tr>
<td>Take a snapshot of a virtual machine</td>
<td>231</td>
</tr>
<tr>
<td>Viewing Alerts in the Orion Web Console</td>
<td>232</td>
</tr>
<tr>
<td>Remove alerts from the Active Alerts list</td>
<td>233</td>
</tr>
<tr>
<td>Escalating Alerts</td>
<td>233</td>
</tr>
<tr>
<td>Escalated Alert Example</td>
<td>234</td>
</tr>
<tr>
<td>Viewing Alerts from Mobile Devices</td>
<td>235</td>
</tr>
<tr>
<td>Syslog alert variables</td>
<td>236</td>
</tr>
<tr>
<td>Syslog date/time variables</td>
<td>236</td>
</tr>
<tr>
<td>Other Syslog Variables</td>
<td>237</td>
</tr>
<tr>
<td>Reports</td>
<td>239</td>
</tr>
<tr>
<td>Predefined NCM reports</td>
<td>239</td>
</tr>
</tbody>
</table>
NCM Audit ............................................................................................................. 240
Brocade Inventory ............................................................................................... 240
Cisco Inventory ................................................................................................... 240
F5 Inventory ......................................................................................................... 242
NCM Inventory ................................................................................................... 242
Node Details Report ........................................................................................... 243
Polling Status ...................................................................................................... 244
Route Tables Inventory ....................................................................................... 245
Security ................................................................................................................ 245
Windows Server Inventory ................................................................................... 246
Predefined Orion reports ..................................................................................... 246
Current Node Status ........................................................................................... 246
Current Volume Status ......................................................................................... 247
Daily Node Availability ......................................................................................... 247
Events .................................................................................................................. 247
Historical CPU and Memory Reports ................................................................. 249
Historical Response Time Reports ...................................................................... 249
Historical VMware ESX Server Reports .............................................................. 249
Historical Volume Usage Reports ....................................................................... 250
Groups: Current Groups and Groups Members Status ....................................... 250
Groups: Daily Group Availability ........................................................................ 250
Groups: Group Availability (with members) ......................................................... 251
Groups: Historical Groups Status ........................................................................ 251
Inventory .............................................................................................................. 251
Create a new web-based report ......................................................................... 252
Run a config change report once ................................................................. 255
Schedule a recurring config change report ............................................... 256
Schedule a report to run automatically while creating or editing a report .... 257
Create and assign report schedules in Report Manager ............................ 258
   Create a report schedule ....................................................................... 258
   Assign a report to a schedule or multiple schedules ......................... 259
Exporting and Importing Reports .............................................................. 259
Add content to a web-based report ........................................................... 260
Add a custom chart or table to a web-based report .................................... 261
   Add a data series and customize a chart .............................................. 262
   Add a data series and customize a table .............................................. 263
   Build conditions .............................................................................. 264

**Servers for file transfers and email notifications** ..................................... 266
Use the SolarWinds TFTP server .............................................................. 266
Use the SFTP & SCP server .................................................................... 266
Use a third-party SCP server ................................................................... 267
Configure email notifications ................................................................... 267
   SMTP server credentials used to send notifications for config change approvals, real time change detection, and running jobs ................................................................. 267
   Email notification defaults used in new scheduled jobs ...................... 268

**Config change templates** ..................................................................... 269
The basics of config change templates ...................................................... 269
Config Change Templates ........................................................................ 269
Preparation and use of a template ............................................................. 270
Parts of a config change template ............................................................. 271
Config change template details ................................................................. 271
Delete a config change template ................................................................. 293

SolarWinds Information Service data entities ................................................. 293

NCM.ArpTables ......................................................................................... 294

NCM.ARPTables entity relationships ............................................................. 295

NCM.BridgePorts ....................................................................................... 296

NCM.BridgePorts entity relationships ........................................................... 298

NCM.CatalystCards ..................................................................................... 299

NCM.CatalystCards entity relationships ....................................................... 303

NCM.CiscoCards ......................................................................................... 303

NCM.CiscoCards entity relationships ........................................................... 305

NCM.CiscoCdp .......................................................................................... 305

NCM.CiscoCdp entity relationships ............................................................... 308

NCM.CiscoChassis ....................................................................................... 308

NCM.CiscoChassis entity relationships ......................................................... 310

NCM.CiscoFlash ......................................................................................... 310

NCM.CiscoFlash entity relationships ............................................................ 318

NCM.CiscoFlashFiles .................................................................................. 318

NCM.CiscoFlashFiles entity relationships .................................................... 320

NCM.CiscoImageMIB ................................................................................... 320

NCM.CiscoImageMIB entity relationships .................................................... 321

NCM.CiscoMemoryPools .............................................................................. 321

NCM.CiscoMemoryPools entity relationships ............................................... 322

NCM.EntityLogical ...................................................................................... 322

NCM.EntityLogical entity relationships ....................................................... 324

NCM.EntityPhysical .................................................................................... 325
<table>
<thead>
<tr>
<th>Entity/Relationship</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCM.EntityPhysical entity relationships</td>
<td>330</td>
</tr>
<tr>
<td>NCM. Interfaces</td>
<td>331</td>
</tr>
<tr>
<td>NCM.Interfaces entity relationships</td>
<td>338</td>
</tr>
<tr>
<td>NCM.IpAddresses</td>
<td>338</td>
</tr>
<tr>
<td>NCM.IpAddresses entity relationships</td>
<td>339</td>
</tr>
<tr>
<td>NCM.MacForwarding</td>
<td>339</td>
</tr>
<tr>
<td>NCM.MacForwarding entity relationships</td>
<td>340</td>
</tr>
<tr>
<td>NCM.Nodes</td>
<td>341</td>
</tr>
<tr>
<td>NCM.Nodes entity relationships</td>
<td>343</td>
</tr>
<tr>
<td>NCM.PortsTcp</td>
<td>345</td>
</tr>
<tr>
<td>NCM.PortsTcp entity relationships</td>
<td>346</td>
</tr>
<tr>
<td>NCM.PortsUdp</td>
<td>346</td>
</tr>
<tr>
<td>NCM.PortsUdp entity relationships</td>
<td>347</td>
</tr>
<tr>
<td>NCM.RouteTable</td>
<td>347</td>
</tr>
<tr>
<td>NCM.RouteTable entity relationships</td>
<td>352</td>
</tr>
<tr>
<td>NCM.VLANs</td>
<td>352</td>
</tr>
<tr>
<td>NCM.VLANs entity relationships</td>
<td>354</td>
</tr>
<tr>
<td><strong>EnergyWise devices</strong></td>
<td><strong>355</strong></td>
</tr>
<tr>
<td>What is EnergyWise?</td>
<td>355</td>
</tr>
<tr>
<td>Manage and enable EnergyWise nodes</td>
<td>355</td>
</tr>
<tr>
<td>Manage Power over Ethernet ports</td>
<td>356</td>
</tr>
<tr>
<td><strong>References</strong></td>
<td><strong>357</strong></td>
</tr>
<tr>
<td>Node and configuration archive variables</td>
<td>357</td>
</tr>
<tr>
<td>Node variables</td>
<td>357</td>
</tr>
<tr>
<td>Status Variables</td>
<td>366</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>General alert variables</td>
<td>368</td>
</tr>
<tr>
<td>Configuration archive variables</td>
<td>369</td>
</tr>
<tr>
<td>Regular Expression Pattern Matching</td>
<td>371</td>
</tr>
<tr>
<td>Characters</td>
<td>371</td>
</tr>
<tr>
<td>Character Classes or Character Sets [abc]</td>
<td>372</td>
</tr>
<tr>
<td>Anchors</td>
<td>373</td>
</tr>
<tr>
<td>Quantifiers</td>
<td>374</td>
</tr>
<tr>
<td>Dot</td>
<td>376</td>
</tr>
<tr>
<td>Word Boundaries</td>
<td>376</td>
</tr>
<tr>
<td>Alternation</td>
<td>377</td>
</tr>
<tr>
<td>View database details and data in the Database Manager</td>
<td>377</td>
</tr>
<tr>
<td>Add a server to Database Manager</td>
<td>378</td>
</tr>
<tr>
<td>View database details</td>
<td>378</td>
</tr>
<tr>
<td>View table details</td>
<td>379</td>
</tr>
<tr>
<td>Database backups and restorations</td>
<td>379</td>
</tr>
<tr>
<td>Update NCM to use a new database server</td>
<td>380</td>
</tr>
<tr>
<td>Monitor SNMP traps</td>
<td>380</td>
</tr>
<tr>
<td>Before you begin</td>
<td>381</td>
</tr>
<tr>
<td>What is a Trap Template?</td>
<td>381</td>
</tr>
<tr>
<td>Define how many traps to display, if you want to refresh the traps view, trap retention, and the information displayed in the Trap Viewer</td>
<td>382</td>
</tr>
<tr>
<td>Configure Trap Viewer filters and alerts</td>
<td>383</td>
</tr>
<tr>
<td>Available trap alert actions</td>
<td>384</td>
</tr>
<tr>
<td>Search for traps in the Trap Viewer</td>
<td>386</td>
</tr>
<tr>
<td>View current traps in the Trap Viewer</td>
<td>387</td>
</tr>
<tr>
<td>Trap alert variables</td>
<td>387</td>
</tr>
</tbody>
</table>
View Syslog messages in the Orion Web Console ............................................................410
Search for Syslog messages in the Syslog Viewer ..........................................................412
Custom properties ........................................................................................................412
  Create a custom property ..........................................................................................413
  Assigning values to a custom property ....................................................................416
  Change custom properties values ..........................................................................417
    Edit values for custom properties .........................................................................417
  Import custom property values ..............................................................................418
  Exporting custom properties ..................................................................................419
  Remove a custom property .....................................................................................419
Configure automatic login ..........................................................................................420
  Log in with Windows pass-through security ..........................................................421
  Automatically login by passing your credentials through the URL .......................422
Share views with non-Orion Web Console users .........................................................422
Enable Windows Authentication with Active Directory ..........................................423
  Authenticate users through MSAPI .........................................................................423
Enable users to authenticate through LDAP .............................................................424
Define what users can access and do .......................................................................424
Introduction to SolarWinds NCM

SolarWinds Network Configuration Manager is a comprehensive, intuitive solution designed to streamline and automate network configuration management. SolarWinds NCM increases availability, saves time, improves security, and ensures policy adherence. SolarWinds NCM 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 should I install SolarWinds NCM?

SolarWinds Network Configuration Manager allows you to easily manage configurations on heterogeneous, multi-vendor networks. SolarWinds NCM provides a single point of management for routers, switches, firewalls, load balancers, and wireless access points. Supported vendors include Cisco, Cisco ASA, Dell, Adtran, Arris, Aruba, Nortel, Nortel Alteon, Nortel BayStack, Extreme, Marconi, Radware, Netscreen, Motorola, HP, Netscalar, Juniper, Foundry, and F5. Additional capabilities include:

- Control access based on user roles.
- Schedule device configuration backups.
- Implement configuration changes in bulk, such as IOS and firmware updates.
- Manage configuration changes to multiple devices from different vendors.
- Generate detailed configuration reports for inventory, change, and policy management.
- Receive notification of device configuration changes.
- Identify configuration violations through policy management reporting.
- Receive results of SolarWinds NCM actions with Orion alerts.
- View detailed change history and side-by-side comparison of configurations.
- Perform detailed device inventory for managed devices.
- Track and view configuration changes made by users.
- Access your device configurations and configuration changes.
- Map the port connections for a specific network switch.
Key features of SolarWinds NCM

Scheduled configuration backups

Scheduled configuration downloads, configuration uploads, device reboots, command script 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 includes policy reports such as SOX, HIPAA, CISP, and Cisco Security.

Role-based access control

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

Multiple vendor support

Monitor network devices from multiple hardware vendors in a hybrid network environment.

Bulk changes

Make changes to community strings, passwords, and black lists across many devices. 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 a custom property.

Configuration change history

Receive reports on what devices have had configuration changes over a specified time period. Configuration change reports can also compare current configurations with a baseline configuration, alerting you whenever a change is discovered.
Configuration viewing, tracking, and comparing

Use SolarWinds NCM to remotely view, track and make changes, and compare network device configurations without logging in to the physical SolarWinds NCM server. The Orion Web Console offers these 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 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 commands for relevant devices for which you need to make a specific configuration change.

Device configuration change management

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

Device end of support and end of sales tacking

Track the end of support and sales statuses of your SolarWinds NCM nodes.
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.
Installation

SolarWinds NCM 7.5 builds on the major rearchitecture that merged all Orion platform and SolarWinds NCM data into a single database.

**Single server standalone: installation or 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 SolarWinds 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 SolarWinds NCM involves these processes:

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

Whether you are installing or upgrading SolarWinds 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
C:\Windows\System32\msmq\storage
```

SolarWinds NCM 7.5 installation software is in your customer portal.

**Requirements**

Requirements vary based on:
### Installation

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

<table>
<thead>
<tr>
<th>TYPE</th>
<th>REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Installing SolarWinds Orion on Windows Server 2012 R2 Essentials is not supported.</strong></td>
</tr>
<tr>
<td>Operating System Language</td>
<td>- English  &lt;br&gt;- German  &lt;br&gt;- Japanese  &lt;br&gt;- Simplified Chinese.  &lt;br&gt;<strong>NCM does not support using locales outside the group of supported operating system languages.</strong></td>
</tr>
<tr>
<td>SolarWinds NCM Server Hardware</td>
<td>- <strong>CPU Speed</strong> 3 GHz dual core dual processor&lt;br&gt;- <strong>Memory</strong> 4GB  &lt;br&gt;- <strong>Hard Drive Space</strong> 30GB  &lt;br&gt;This version of SolarWinds NCM holds a searchable config index on local disk that adds 6-10GB additional disk space to the previous requirement.</td>
</tr>
<tr>
<td>TYPE</td>
<td>REQUIREMENTS</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</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 and write access to the Orion Platform database.</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 and write access to the Orion Platform database.</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.</td>
</tr>
<tr>
<td>Microsoft IIS</td>
<td>Version 7.5 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.</td>
</tr>
<tr>
<td>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>
<td></td>
</tr>
<tr>
<td>Microsoft ASP .NET 2.0 Ajax Extension</td>
<td>Version 1 or later</td>
</tr>
<tr>
<td></td>
<td>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 4.5 (and compatible with 4.6.1)</td>
</tr>
</tbody>
</table>
## Installation

### Type

<table>
<thead>
<tr>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the required version is not found on the target computer, the setup program downloads and installs it. Ensure that .NET is turned on in Windows Features.</td>
</tr>
</tbody>
</table>

### Database

You must create the SolarWinds Orion database with the SolarWinds Configuration Wizard. Creating the database another way is not supported.

SolarWinds supports using NCM with database servers set up in these languages: English, German, Japanese, and Chinese, but only supports storing characters in the UTF-8 set.

The following database servers are supported:
- SQL Server 2014 and SQL Server 2014 with SP1, and with Always On Availability Groups
- SQL Server 2012, with or without SP1 and SP2, Standard or Enterprise
- SQL 2008 R2 without SP, 2008 R2 SP1, 2008 R2 SP2
- SQL 2008 without SP, 2008 SP1, 2008 SP2, 2008 SP3

Note: NCM local SQL database uses SQL 2014 Express.

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

```
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
## Requirements

<table>
<thead>
<tr>
<th>Type</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Your database server must support mixed-mode authentication or SQL authentication and have the following protocols enabled:</td>
</tr>
<tr>
<td></td>
<td>■ Shared memory</td>
</tr>
<tr>
<td></td>
<td>■ TCP/IP</td>
</tr>
<tr>
<td></td>
<td>■ Named Pipes</td>
</tr>
<tr>
<td></td>
<td>SQL Server 2008 Express Edition does not enable these protocols.</td>
</tr>
<tr>
<td></td>
<td>The following x86 components must be installed:</td>
</tr>
<tr>
<td></td>
<td>■ SQL Server System Common Language Runtime (CLR) Types</td>
</tr>
<tr>
<td></td>
<td>■ Microsoft SQL Server Native Client</td>
</tr>
<tr>
<td></td>
<td>■ Microsoft SQL Server Management Objects</td>
</tr>
<tr>
<td></td>
<td>If the components are not found on the target computer, the setup program downloads and installs the components.</td>
</tr>
<tr>
<td></td>
<td>Ports The following ports may be needed for Orion Web Console, depending on how SolarWinds NCM is set up to download and upload configurations:</td>
</tr>
<tr>
<td></td>
<td>■ 22: SSH/SCP default for NCM to transfer configs</td>
</tr>
<tr>
<td></td>
<td>■ 23: TELNET default for NCM to transfer configs</td>
</tr>
<tr>
<td></td>
<td>■ 25: SMTP email default that NCM uses for notification (If SSL/TLS encryption is set up on SMTP server, default port is 465)</td>
</tr>
<tr>
<td></td>
<td>■ 69: TFTP server listens on it</td>
</tr>
<tr>
<td></td>
<td>■ 80: HTTP default for Orion Web Console</td>
</tr>
<tr>
<td></td>
<td>■ 161: SNMP statistics collection, the default for polling in NCM</td>
</tr>
<tr>
<td></td>
<td>■ 162: UDP trap messages listened for and received by Trap Server</td>
</tr>
<tr>
<td></td>
<td>■ 443: TCP default port for https binding.</td>
</tr>
<tr>
<td></td>
<td>■ 465: TCP port used for SSL-enabled email alert actions</td>
</tr>
<tr>
<td></td>
<td>■ 514: UDP Syslog messages arrive for Orion Syslog Service</td>
</tr>
<tr>
<td></td>
<td>■ 587: Port used for TLS-enabled email alert actions.</td>
</tr>
<tr>
<td></td>
<td>■ 1801: TCP used for MSMQ WCF binding.</td>
</tr>
</tbody>
</table>
### Installation

<table>
<thead>
<tr>
<th>TYPE</th>
<th>REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5671: TCP for SSL-encrypted RabbitMQ messaging from the additional polling engines to the main polling engine</td>
</tr>
<tr>
<td></td>
<td>17777: SolarWinds Information Service for Orion Web Console</td>
</tr>
<tr>
<td></td>
<td>17778: SolarWinds Information Service for Orion Web Console</td>
</tr>
<tr>
<td></td>
<td>17779: SolarWinds Information Service for Orion Web Console</td>
</tr>
</tbody>
</table>

Ports 4369, 5672, and 25672 are opened by default. These ports can be blocked by the firewall.

### Additional information

- The SolarWinds NCM Information Service requires that the Net.TCP Port Sharing service be enabled and port 17777 open for TCP traffic to the SolarWinds NCM server. By default, this service is disabled. The setup program sets the service to manual. Resetting the service setting to disabled is not recommended.

- To take advantage of the numerous integration points in SolarWinds NCM, 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

SolarWinds NCM 7.5 was tested for scalability in a standalone deployment of three servers: one server hosts the main server and the other two servers each host an additional polling engine. The main server manages up to 10,000 nodes, as does each additional 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 server, polling for node status at the default rate. This deployment supports two SolarWinds NCM operations, inventory update and configuration download, performed per day on all 30,000 nodes.

Though the main 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 servers, consider consolidating your views of multiple servers with the Orion Enterprise Operations Console.

**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, and 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.

**Install SolarWinds NCM**

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

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

Because they share a single database, you cannot integrate SolarWinds NCM with an Orion platform product installed on a different host. For the same reason, you cannot separate SolarWinds NCM from another Orion platform product once they are integrated.

**Orion platform products: integration support**

If you are integrating SolarWinds NCM with another Orion platform product, the other product must be installed first on the host. SolarWinds NCM version 7.5 integrates with the following Orion platform products and versions:

- SolarWinds Network Performance Monitor (NPM) version 12.0
- SolarWinds Server and Application Monitor (SAM) versions 6.2.x, 6.3.x
- SolarWinds Enterprise Operations Console versions 1.6.2
- SolarWinds IP Address Manager (IPAM) versions 4.3.x
- SolarWinds User Device Tracker (UDT) versions 3.2.2, 3.3, 3.4
- SolarWinds VNQM (IPSLA) versions 4.2.x
- SolarWinds Engineer’s Toolset versions 11.0.1, 11.0.2, 11.0.3

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 2014 Express Edition is distributed with SolarWinds NCM. SQL Server 2014 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 multiprocessor server, according to information published by Microsoft.

SolarWinds recommends that you create the database on a separate SQL Server host, and not the SolarWinds 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.
Install SolarWinds NCM

1. Log in to the host server with a local administrator account. Do not install on a domain controller.
2. Launch the executable from the download location.
4. Accept the License Agreement, and click Next.
5. Accept the default target directory, or set a custom path.
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.
10. Enter the database authentication method, Windows or SQL Server Authentication, and click Next.
   - 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 account: SA.
11. Select your existing Orion platform database, and click Next.
12. Select an existing account with administrator rights on the database, and click Next. You must supply a strong password.
13. Click Next to set up the website with default settings, or adjust the settings.
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.

License your product with Internet access

1. Click Enter Licensing Information.
2. Select the I Have Internet Access and an Activation Key.
3. Enter your Activation Key, and click Next.
Installation

4. If applicable, select I Access the Internet Through a Proxy Server.
5. Enter registration information, and click Finish.
6. If licensing fails, the software enters evaluation mode for 30 days.

License your product without Internet access

1. Click Enter Licensing Information.
2. Select This Server Does Not Have Internet Access, click Next, and complete the steps provided.
3. You need a customer ID and password to install the key. For more information, see Obtain a software license key.

Upgrade SolarWinds NCM

You have two options for upgrading SolarWinds NCM software to version 7.5:

**Single Server Standalone**

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

**Single Server Integrated**

This option installs SolarWinds 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.

Stop SolarWinds NCM Jobs

You cannot upgrade the SolarWinds NCM software while jobs are still running.

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

Stop jobs that are running before upgrading

1. Open the Windows Task Manager.
2. Click Processes and highlight `configMgmtJob.exe`.
3. Click End Task.
Stop the SCP Server tray application before upgrading

1. Open the Windows Task Manager.
2. Click Processes, and then select ScpServerTray.exe.
3. Click End Task.

Launch the SolarWinds NCM installer

1. Log in to the host with a local administrator account. 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 SQL Server host of the Orion Platform database, 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.
   - 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 account: SA.
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. You must supply a strong password. For more information about strong passwords, see the Microsoft website.
Installation

14. Click Next to set up 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.

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.

Install or upgrade an additional poller
If you are upgrading to SolarWinds NCM 7.5, before you attempt to install an additional poller on another server, you must first Upgrade SolarWinds NCM.

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.
11. Enter the database authentication method, Windows or SQL Server Authentication, and then click Next.
   - 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 account: SA.

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.

Install or upgrade an additional web console

If you are upgrading to SolarWinds NCM 7.5, before you attempt to install an additional web console on another server, you must first upgrade the main server.

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.
4. Accept the end user agreement, and 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 click Next.
10. Specify the SQL Server instance where the Orion Platform database is located.
11. Enter the authentication method, Windows or SQL Server Authentication, and click Next.
   - 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 account: `SA`.
12. Click Use an Existing Database, select the Orion Platform database in the list, and 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 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 click Next.
19. Review the Database, Website, and Services to be configured, and click Next.
20. Click Launch Orion Web and Finish.

Set 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 SolarWinds 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 set to AES-256 after you have resolved the SNMP-related issue.
Set node communication default parameters

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
4. Enter the appropriate values and click Submit.

Override default settings for a specific node

1. Click Settings > Manage Nodes.
2. Use the Group By list to filter the nodes.
3. Select a node in the list, and click Edit Properties.
4. Scroll down to NCM Properties.
5. Edit login and communication information, and click Submit.

Define and apply global device logins

A connection profile is a global device login that you apply to one or more devices managed by SolarWinds NCM.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
4. To create a new connection profile, click Create New.
5. To edit an existing profile, select a profile, and click Edit.
6. Enter the appropriate values. See below for more information on the last option, Automatically Test This Profile Against Monitored Nodes That Allow It:
   - Make this profile available to SolarWinds NCM in communicating with nodes for which no profile is assigned.
   - If you have multiple connection profiles with this setting enabled, SolarWinds NCM cycles through them before performing the desired operation on a node without a specific connection profile applied. SolarWinds NCM permanently assigns the first connection profile that works to the node.
   - Though selecting this setting on your connection profiles helps SolarWinds NCM communicate with devices without assigned profiles, we recommend applying a specific connection profile to each managed node.
Installation

7. Click Submit.

Set communication limits

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

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
4. Enter timeout settings for each protocol, and click Submit.

Log events for a detailed record of SolarWinds NCM functions

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
4. Select all log types for which to keep verbose log information. This information aids in troubleshooting.
5. Select Enable Session Tracing to create a log file of each Telnet session to troubleshoot communication node by node.
6. Click Submit.

Enable 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.

1. Log in as an administrator to your main SolarWinds NCM server.
3. Expand Services and Applications > Internet Information Services (IIS) Manager > Web Sites.
5. Click the Web Site tab.
6. Confirm that SSL port is set to 443, and 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 select the IP address of the Orion Web Console.
      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 click OK.
12. Click Apply, and click OK to exit.

**Repair SolarWinds NCM**

⚠️ 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.

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

4. Select the appropriate Orion platform, and click Next.

5. Create a new database account and password or select an existing account on the database server. You must supply a strong password. For more information about strong passwords, see the Microsoft website.

6. Click Next.

7. Review the services to install, and click Next.

8. Review the configuration to change, and click Next.

9. Review the Configuration Summary, and click Finish.

**Move SolarWinds NCM to another computer**

1. Log in to the SolarWinds NCM server host with an administrator account.
2. Start Database Manager in the SolarWinds Orion program folder.
3. Select your Orion platform database in the left pane of the Database Manager window.
4. Click Database > Backup Database.
5. 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. Ensure the target location has sufficient available disk space.
6. Click OK.
7. Start SolarWinds License Manager in the SolarWinds program folder to reset your current license. This makes it available for your new implementation.
8. Log in to the new computer and install SolarWinds Network Configuration Manager.
Uninstall SolarWinds NCM

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

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

About the SolarWinds Orion database

Microsoft SQL Server 2014 Express Edition is distributed with SolarWinds NCM. SQL Server 2014 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 multiprocessor server, according to information published by Microsoft.

SolarWinds recommends that you create the database on a separate SQL Server host, and not the SolarWinds 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.

The following characters cannot be included in the database name:

- Asterisk (*)
- Closing square bracket (]
- Colon (:)
- Semicolon (;)
- Single quote (‘)
- Double quote (“)
- Backward slash (\)
- Forward slash (/)
- Less than (<)
- Greater than (>)
- Question mark (?)
Installation

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.

SolarWinds NCM licensing

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 NCM. 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)

Activate your SolarWinds license

When you install your Orion Platform product, you are prompted to provide your licensing information (software license key and customer data), and activate your product.

To postpone the activation, click Continue Evaluation. You can activate the license later, with the License Manager.
Activate licenses with Internet access

Activate licenses with Internet access

1. On the Activate Product window, select I Have Internet Access...
2. Find your activation key in the customer portal, and enter it in the Activation Key field.
   a. Browse to https://customerportal.solarwinds.com, and then log in using your Customer ID and password, or your individual user account information.
      
      If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support and submit a ticket.

   b. Under the Licensing Management section on the top bar, select License Management.
   c. Browse to the SolarWinds product, and click the plus sign next to the product to display your activation key.
   d. Copy your unregistered activation key for the SolarWinds product to the clipboard, and paste it into the Activation Key field in the Activate window.
3. If you are using a proxy server to access the Internet, select I Access the Internet Through a Proxy Server, and enter the proxy address and port number.
4. Click Next.
5. Provide your customer data, and complete the Activation Wizard.
Installation

Activate licenses offline

1. On the Activate Product window, select This Server Does Not Have Internet Access, and click Next.
2. To finalize your registration, click Copy Unique Machine ID.
3. Paste the data into a new document in a text editor, and save the text document.
4. Transfer the document to a computer with Internet access. For example, transfer the document to a shared location.
5. Log in to the SolarWinds customer portal and find your activation key:
   a. **Browse** to [https://customerportal.solarwinds.com](https://customerportal.solarwinds.com) from a computer with Internet access, and then log in using your Customer ID and password, or your individual user account information.

   ![Information](https://example.com/image)

   *If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support and [submit a ticket](https://customerportal.solarwinds.com).*

   b. Click License Management.
   c. **Browse** to the SolarWinds product, such as Network Performance Monitor, and click Manually Register License.
   d. Provide the Unique Machine ID you transferred earlier, and download your license key.
   e. Transfer the license key to a shared location.
6. Return to the offline computer where you have been running the activation wizard, and browse to the shared License Key File location from the Activate Product window.
7. Click Next to continue, and complete the Activation wizard.

License keys

Versions of the SolarWinds NCM software that are released during the release candidate period have a limited license. When upgrading, 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 official release.

From the appropriate server in your deployment, go to the [customer portal](https://customerportal.solarwinds.com) 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 SolarWinds NPM 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.

Review your NCM license

1. Click Settings > All Settings.
2. Under Details, click License Details.
3. View the information under NCM.

Maintain licenses

After you install an Orion Platform product or other products such as DameWare, you are prompted to activate your license. You can activate your product straight away, or later, using the SolarWinds License Manager.

SolarWinds License Manager features

- Deactivate licenses on one computer and activate them on another computer without contacting SolarWinds Customer Service.
- Upgrade from one production license level to another.
- Upgrade from evaluation licenses to production licenses.
- Synchronize licenses with the licensing server automatically or manually.

You cannot activate the license for a product that is released after the end of your maintenance period. You can activate the license for a product released before the end of your maintenance period at any time.

The following sections provide more information about the following License Manager-related topics:

- License Manager requirements
- Install License Manager
- Activate your SolarWinds license
Installation

- Activate licenses with the License Manager
- Deactivate and reactive licenses
- Upgrade and synchronize licenses

License Manager requirements

<table>
<thead>
<tr>
<th>ITEM</th>
<th>REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install location</td>
<td>SolarWinds License Manager must be installed on the same computer as your installed products. You must install License Manager on a computer with the correct time.</td>
</tr>
<tr>
<td>Connectivity</td>
<td>For instant license management, the computer must have internet connectivity. You can also manage licenses using offline activation and deactivation. You must have online access to the SolarWinds Customer Portal from another computer.</td>
</tr>
<tr>
<td>.NET Framework</td>
<td>.NET 4.5</td>
</tr>
</tbody>
</table>
| Operating system| - Windows Server 2008 R2 SP1  
                  - Windows Server 2012  
                  - Windows Server 2012 R2  
                  For evaluation purposes:  
                  - Windows 7 SP1  
                  - Windows 8 (except for Standard edition)  
                  - Windows 8.1 (except for Standard edition)  
                  - Windows 10                                                                                                                                 |
| Browser         | - Microsoft Internet Explorer 8 or later  
                  - Microsoft Edge  
                  - Firefox 44.0 or later  
                  - Chrome latest version |
Install License Manager

Install License Manager on the computer with SolarWinds products installed. The License Manager can only license products on that computer.

⚠️ You must install License Manager on a computer with the correct time.

1. Start the SolarWinds License Manager Setup in the SolarWinds program folder.

   🔹 If problems with License Manager occur, or if or the computer does not have access to the Internet, download and install the latest version of License Manager from [http://solarwinds.s3.amazonaws.com/solarwinds/Release/LicenseManager/LicenseManager.zip](http://solarwinds.s3.amazonaws.com/solarwinds/Release/LicenseManager/LicenseManager.zip)

2. Click Next to accept the SolarWinds EULA, and click Install.

Activate licenses with the License Manager

With the License Manager, you can manage licenses for multiple SolarWinds products.

1. Start the License Manager in your SolarWinds program folder.

   🔹 If the License Manager is not installed on the computer, install it first.

2. Click Activate next to the SolarWinds product, and complete the Activation Wizard.

   - **Activate licenses with Internet access**
     a. On the Activate Product window, select I Have Internet Access...
     b. Find your activation key in the customer portal, and enter it in the Activation Key field.
       a. Browse to [https://customerportal.solarwinds.com](https://customerportal.solarwinds.com), and then log in using your Customer ID and password, or your individual user account information.

         🔹 If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support and submit a ticket.

       b. Under the Licensing Management section on the top bar, select License Management.

---

54
c. Browse to the SolarWinds product, and click the plus sign next to the product to display your activation key.

d. Copy your unregistered activation key for the SolarWinds product to the clipboard, and paste it into the Activation Key field in the Activate window.

c. If you are using a proxy server to access the Internet, select I Access the Internet Through a Proxy Server, and enter the proxy address and port number.

d. Click Next.

e. Provide your customer data, and complete the Activation Wizard.
Activate licenses offline

a. On the Activate Product window, select This Server Does Not Have Internet Access, and click Next.
b. To finalize your registration, click Copy Unique Machine ID.
c. Paste the data into a new document in a text editor, and save the text document.
d. Transfer the document to a computer with Internet access. For example, transfer the document to a shared location.
e. Log in to the SolarWinds customer portal and find your activation key:
   a. Browse to https://customerportal.solarwinds.com from a computer with Internet access, and then log in using your Customer ID and password, or your individual user account information.
   
   If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support and submit a ticket.

   b. Click License Management.
   c. Browse to the SolarWinds product, such as Network Performance Monitor, and click Manually Register License.
   d. Provide the Unique Machine ID you transferred earlier, and download your license key.
   e. Transfer the license key to a shared location.
   f. Return to the offline computer where you have been running the activation wizard, and browse to the shared License Key File location from the Activate Product window.
   g. Click Next to continue, and complete the Activation wizard.

3. Provide your customer data, and complete the Activation Wizard.

Deactivate and reactive licenses

If you decide to move your SolarWinds product to another server, you must deactivate the license on the original computer, and reactivate it on the server with the new installation.
Installation

You can deactivate and reuse the licenses to install product versions that were released during your maintenance period. You cannot deactivate and reuse licenses to install products that were released after your maintenance period expired. To license these products, you must renew your maintenance or re-license your product.

Deactivate licenses online

1. Log in to the computer where the currently licensed SolarWinds product is installed.
2. Start the License Manager in the SolarWinds program folder.
3. Select the products you want to deactivate on this computer, and click Deactivate.
   You can deactivate more than one product at the same time.
   In certain products, you can deactivate licenses by using the internal licensing tool of the product.
4. Complete the deactivation wizard.
5. Log in to the computer on which to install your products, and begin installation.
6. When asked to specify your licenses, provide the information. The license you deactivated earlier is assigned to the new installation.

Deactivate licenses offline

1. Log in to the computer where the currently licensed SolarWinds product is installed.
2. Start the License Manager in the SolarWinds program folder.
3. Select the products you want to deactivate on this computer, and click Deactivate.
   You can deactivate more than one product at the same time. The deactivation file will contain information about each product.
   In certain products, you can deactivate licenses by using the internal licensing tool of the product.
4. Complete the deactivation wizard, and save the deactivation file.
5. Log in to the SolarWinds Customer Portal, and navigate to the License Management page.
6. Select your product instance, and click Deactivate License Manually.
7. In the Manage License Deactivation page, locate the deactivation file you created in License Manager, and click Upload. The deactivated licenses are now available to activate on a new computer.

8. Log in to the computer on which to install your products, and begin installation.
9. When asked to specify your licenses, provide the information. The license you deactivated earlier is assigned to the new installation.

Upgrade and synchronize licenses

If you have changed how your product is licensed, such as by increasing the number of objects you can monitor, use the License Manager to apply the change to your products.

1. Start the License Manager from the SolarWinds program group.
2. Click Upgrade in the Action column next to the products for which you want to upgrade the license on this computer.
3. Complete the Activation Wizard.

Synchronize licenses to the Customer Portal

For most Orion Platform products licenses, you can synchronize the data on your Customer Portal with the data in the License Manager.

Synchronizing can include:

- Updating the maintenance end date
- Registering the license again, if it was reset

License synchronization takes place automatically once a day. If the automatic synchronization does not occur, or you want to update your licenses immediately, you can synchronize your installed licenses with the SolarWinds Customer Portal:

1. Start the License Manager from the SolarWinds program group.
2. Select the product, and click Synchronize.
3. Click Synchronize again in the Synchronize Licenses window.

The License Manager synchronizes with the Customer Portal and any updates in the Customer Portal are reflected in the License Manager.
Get started with NCM

A significant amount of time spent managing your network devices can be decreased using SolarWinds Network Configuration Manager. Before adding or discovering nodes to manage in NCM, make sure your devices are properly set up to communicate with NCM and to export network flows.

The following sections walk you through adding nodes to monitor and other common tasks.

SolarWinds NCM uses SNMP communication to collect inventory information.

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.

Add nodes to NCM

Use any of the following methods to add nodes for configuration management in the SolarWinds Network Configuration Manager:

- add them individually
- through network discovery using SolarWinds Network Discovery.
- by importing a list of IP addresses or hostnames from a file.

For complete information about adding or discovering nodes on the Orion platform, see the SolarWinds Orion Common Components Administrator Guide.

Add an individual node

Use this option to add a single node that you want to start managing in your Network Configuration Manager installation. If adding a large number of nodes, consider using Network Discovery.

1. Click Settings > Manage Nodes.
2. Click Add Node.
3. Type the hostname or IP Address of the node you are adding. Both IPv4 and IPv6 are supported.

4. Select a Polling Method:
   a. External Node — reports no status for node itself but is useful for monitoring a hosted application.
   b. Status Only: ICMP — reports status, response time, and packet loss only.
   c. Most Devices: SNMP and ICMP — default polling method typically used for routers, switches, and Linux/Unix servers. Make sure to specify a community string if using one other than "public".

   Use the TEST option to verify that your settings are valid before continuing.

5. Select the Additional Monitoring Options, and click Next.

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

7. On the Change Properties tab, under Polling, edit the default polling settings if desired.
   - Node Status Polling: The number of seconds between status checks performed on the added node.
   - Collect Statistics Every: The period of time between updates made to displayed statistics for the added node

8. Under Custom Properties, add appropriate values if you defined custom properties for monitored nodes.
   - The Custom Properties area is empty if you did not define custom properties for monitored nodes.
   - SolarWinds NCM ignores custom properties that use words from the list of reserved words.

9. Click OK, Add Node when you have completed the properties configuration.

The added node appears in the Config Summary.

You can also use the More Actions menu on the Managed Nodes page to "Add Nodes to NCM" that you have selected.

**Add nodes via Network Discovery**

Network Discovery is particularly useful when you have multiple devices that you want to add for configuration management. At first, SolarWinds recommends scanning a small subnet or a few individual IP addresses.
1. Click Settings > Network Discovery.
2. Click Add New Discovery, and click Start.
3. To discover devices on your network within a specific range of IP addresses:
   a. In the IP Ranges section, click Add Range and provide a Start and End Address for the range. Scheduled discovery profiles should not use IP address ranges that include nodes with dynamically assigned IP addresses (DHCP).
   b. Repeat to add ranges, and then click Next when finished.
4. To discover devices connected to a specific router or on a specific subnet of your network:
   a. In the Subnets section, click Add > Subnet, and enter a Subnet IP Address. Repeat to add subnets.
   b. If you want to discover devices using a seed router, click Add > Seed Router, enter the IP address of the Router, and click Scan Router.
   - 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.
   c. When finished, click Next.
5. If you already know the IP addresses or hostnames of the devices you want to discover:
   a. In the IP Addresses section, click Add IP Address and enter the IPv4 or IPv6 addresses or hostnames of the devices. Type only one address or hostname per line.
   c. Click Validate to confirm that the provided IPv4 addresses and hostnames are assigned to SNMP-enabled devices.
   d. When finished, click Next.
6. If you want to import nodes by querying your Active Directory Domain Controllers for registered devices, click Add Active Directory Domain Controller to Query. Choose existing credentials or add the credentials to access the Active Directory server.
7. On the Agents tab, decide whether to poll for updates on these nodes, and click Next.

8. On the Virtualization tab, decide whether to poll for VMware, and click next.

9. On the Config Management tab, Add SSH or Telnet credentials, and click Next.

10. On the SNMP tab, specify SNMP credentials for discovery:
   a. If the devices on your network do not require community strings other than the default public and private strings provided by SolarWinds NCM, click Next.
   b. If any of your network devices require community strings other than public and private provided, or if you want to use an SNMPv3 credential, add the required SNMP credential for each 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.
      b. Select the SNMP Version, enter the required information, and click Add.
      c. Click Next.


12. Set polling and monitoring settings, and click Next.
13. On the Discovery Settings tab, edit the Details, Retries, and Timeouts.
   a. Name and Description: distinguishes the current discovery profile from other profiles you may use to discover other network areas. This Description displays next to the Name in the list of available network discovery configurations on the Network Sonar view.
   b. SNMP Timeout: If you are encountering numerous SNMP timeouts during Network Discovery, increase the value for this setting. A recommended value is at least more than double the time it takes a packet to travel the longest route between devices on your network.
   c. Search Timeout: The amount of time Network Sonar Discovery waits to determine if a given IP address has a network device assigned to it.
   d. SNMP Retries: The number of times Network Sonar Discovery retries a failed SNMP request, when a response is not received within the time set in SNMP Timeout.
   e. Hop Count: 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.
   f. Discovery Timeout: The amount of time, in minutes, Network Sonar Discovery is allowed to complete a network discovery. If the Discovery Timeout value is exceeded, the discovery is terminated.

14. The default Frequency for discovery is Once, which starts immediately. If you want the discovery to run on a regular schedule, select Hourly, Daily, or Advanced as the Frequency, and click Discover.

15. If you do not want to run the network discovery, select No, Don't Run Now, and click Save or Schedule, depending on the Frequency selection.

**Select network devices for monitoring in NCM**

The Network Sonar Results Wizard opens to guide you through selecting the devices from discovery results that you want to monitor. These results are available whenever a requested or scheduled SolarWinds Network Sonar Discovery operation completes, or whenever you choose to either Import All Results or Import New Results for a selected discovery profile.

The Results Wizard automatically adds non-server nodes as SolarWinds NCM nodes if there is at least one connection profile set up with Use for Auto Detect enabled.

**Select the results of a network discovery**

1. Click Settings > Network Discovery.
2. Select an existing discovery profile, and click Import New Results.
Get started with NCM

3. Select the device types you want to monitor, and click Next.
4. Select the interface types you want to monitor, and click Next.
5. Select the volume types you want to monitor, and click Next.
6. Select the AppInsight applications to use with your environment, and click Next.
7. If there are any devices on the Import Preview that you do not want to import, select the device, and click Ignore.
   Selected nodes are added to the Discovery Ignore List.
8. Confirm that the network objects you want to monitor are selected on the Import Preview tab, and click Import.
9. After the import completes, click Finish.
10. Click My Dashboards > Home > Summary to see imported devices in the All Nodes resource.
Common tasks

The following topics present example scenarios to help demonstrate how you can use SolarWinds Network Configuration Manager in different network environments.

Schedule daily backups of config files

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.

1. Click My Dashboards > Configs > Jobs.
2. Click Create New Job.
3. Name the job, and select Download Configs from Devices from Job Type.
4. Select the Schedule Type. If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if this job relates to a business rule, and click Next.
6. Select the nodes to target with this job, and click Next.
7. Select an email notification option, and click Next. If you click Email Results, the default Email Notification Settings and SMTP Server Settings and SMTP Server Settings are populated. These settings can be overridden in each job.
8. Select the configuration types you want to download, select the send config change notifications, and click Next.
9. Review the settings for the job, and click Finish.

Change the community string on multiple nodes

This procedure replaces the public read-only community string with a new read-only community string on several network nodes at the same time.

1. Click My Dashboards > Configs > Jobs.
2. Click Create New Job.
3. Name the job, and select Execute Command Script on Devices from Job Type.
4. Select the Schedule Type. If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if this job relates to a business rule, and click Next.
6. Select the nodes to target with this job, and click Next.
7. Select an email notification option, and click Next. If you click Email Results, the default Email Notification Settings and SMTP Server Settings and **SMTP Server Settings** are populated. These settings can be overridden in each job.

8. Add the script to execute.
   - If you want to load a saved script, click Load Saved Script, and select a script.
   - If you want to load an existing script from disk, click Load Script from File, browse to the file, and 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, specify a location, and 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 regular expression pattern.

11. Select Show Commands in Output to view what SolarWinds NCM sent to the targeted devices.

12. Click Next.

13. Review the settings for the job, and click Finish.

**Verify success by comparing configs**

1. Click My Dashboards > Configs > Configuration Management.
2. Select one or more nodes, and 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.

**Block 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 on a wireless access point to block a specific MAC address.
**Back up the running configuration**

1. Click My Dashboards > Configs > Configuration Management.
2. Select one or more nodes.
3. Click Download > Running.

**Block a MAC address on a wireless access point**

1. Click My Dashboards > Configs > Jobs.
2. Click Create New Job.
3. Name the job, and select Execute Command Script on Devices from Job Type.
4. Select the Schedule Type. If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if this job relates to a business rule, and click Next.
6. Select the nodes to target with this job, and click Next.
7. Select an email notification option, and click Next. If you click Email Results, the default Email Notification Settings and SMTP Server Settings and SMTP Server Settings are populated. These settings can be overridden in each job.
8. Add the script to execute.
   - If you want to load a saved script, click Load Saved Script, and select a script.
   - If you want to load an existing script from disk, click Load Script from File, browse to the file, and 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 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 regular expression pattern.
11. Select Show Commands in Output to view what SolarWinds NCM sent to the targeted devices.
12. Click Next.
13. Review the settings for the job, and click Finish.

**Verify success by comparing configs**

1. Click My Dashboards > Configs > Configuration Management.
2. Select one or more nodes, and 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.

**Change an interface description**

Updating interface descriptions with SolarWinds Network Configuration Manager saves time because you do not have to remember IP addresses or login credentials for the device you are updating.

**Back up the running configuration**

1. Click My Dashboards > Configs > Configuration Management.
2. Select one or more nodes.
3. Click Download > Running.

**Update the interface descriptions**

1. Click My Dashboards > Configs > Jobs.
2. Click Create New Job.
3. Name the job, and select Execute Command Script on Devices from Job Type.
4. Select the Schedule Type. If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if this job relates to a business rule, and click Next.
6. Select the nodes to target with this job, and click Next.
7. Select an email notification option, and click Next. If you click Email Results, the default Email Notification Settings and SMTP Server Settings and SMTP Server Settings are populated. These settings can be overridden in each job.
8. Add the script to execute.
   - If you want to load a saved script, click Load Saved Script, and select a script.
   - If you want to load an existing script from disk, click Load Script from File, browse to the file, and 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 Lab
     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 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 regular expression pattern.

11. Select Show Commands in Output to view what SolarWinds NCM sent to the targeted devices.

12. Click Next.

13. Review the settings for the job, and click Finish.

**Verify success by checking the interface description**

1. Click My Dashboards > 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 click Edit Config.
5. Locate the interface definitions.
6. Verify that the new description has been applied to the interface you modified.
Upgrade 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, third-party FTP, third-party SCP, 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.

Back up the running configuration

1. Click My Dashboards > Configs > Configuration Management.
2. Select one or more nodes.
3. Click Download > Running.

Push an IOS image to a network device

1. Click My Dashboards > Configs > Jobs.
2. Click Create New Job.
3. Name the job, and select Execute Command Script on Devices from Job Type.
4. Select the Schedule Type. If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if this job relates to a business rule, and click Next.
6. Select the nodes to target with this job, and click Next.
7. Select an email notification option, and click Next. If you click Email Results, the default Email Notification Settings and SMTP Server Settings and SMTP Server Settings are populated. These settings can be overridden in each job.
8. Add the script to execute.
   - If you want to load a saved script, click Load Saved Script, and select a script.
   - If you want to load an existing script from disk, click Load Script from File, browse to the file, and 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 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 regular expression pattern.
11. Select Show Commands in Output to view what SolarWinds NCM sent to the targeted devices.
12. Click Next.
13. Review the settings for the job, and click Finish.

**Block all private addresses with an access control list**

Routers connected 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 one of your network devices using these addresses. The following procedure updates the access control list to block all private IP addresses on several devices at the same time.

**Back up the running configuration**

1. Click My Dashboards > Configs > Configuration Management.
2. Select one or more nodes.
3. Click Download > Running.
Update the access control list for a group of nodes

1. Click My Dashboards > Configs > Jobs.
2. Click Create New Job.
3. Name the job, and select Execute Command Script on Devices from Job Type.
4. Select the Schedule Type. If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if this job relates to a business rule, and click Next.
6. Select the nodes to target with this job, and click Next.
7. Select an email notification option, and click Next. If you click Email Results, the default Email Notification Settings and SMTP Server Settings and SMTP Server Settings are populated. These settings can be overridden in each job.
8. Add the script to execute.
   - If you want to load a saved script, click Load Saved Script, and select a script.
   - If you want to load an existing script from disk, click Load Script from File, browse to the file, and 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 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 regular expression pattern.
11. Select Show Commands in Output to view what SolarWinds NCM sent to the targeted devices.
12. Click Next.
13. Review the settings for the job, and click Finish.
Verify success by comparing configs

1. Click My Dashboards > Configs > Configuration Management.
2. Select one or more nodes, and 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.

Customize 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.

Modify the login banner

1. Click My Dashboards > Configs > Jobs.
2. Click Create New Job.
3. Name the job, and select Execute Command Script on Devices from Job Type.
4. Select the Schedule Type. If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if this job relates to a business rule, and click Next.
6. Select the nodes to target with this job, and click Next.
7. Select an email notification option, and click Next. If you click Email Results, the default Email Notification Settings and SMTP Server Settings and SMTP Server Settings are populated. These settings can be overridden in each job.
8. Add the script to execute.
   - If you want to load a saved script, click Load Saved Script, and select a script.
   - If you want to load an existing script from disk, click Load Script from File, browse to the file, and 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 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 regular expression pattern.

11. Select Show Commands in Output to view what SolarWinds NCM sent to the targeted devices.

12. Click Next.

13. Review the settings for the job, and click Finish.

**Verify success by comparing configs**

1. Click My Dashboards > Configs > Configuration Management.
2. Select one or more nodes, and 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.
Node management

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.

After you Add nodes to NCM you can begin to Manage SolarWinds NCM nodes and their device configurations. If you use SolarWinds Network Sonar Discovery to add nodes, you can then Select network devices for monitoring in NCM from the discovery results.

Manage SolarWinds NCM nodes

The NCM Manage Nodes view shows the status of managed nodes and enables you to select added nodes to determine when and how the devices will be managed. You can modify the node properties, work with custom properties, and initiate polling and discovery actions.

Click Settings > Manage Nodes.

To add or change columns displayed in the view, click the double-right angle icon at the far right of the table header and choose the data you want displayed.

Find a specific node

Enter an IP address or hostname in the Search field, and click Search.

Add or edit a node

1. Use the Group By list to filter the nodes.
2. Select one or more nodes you want to license in SolarWinds NCM, and click Edit Properties.
3. Scroll down to the Manage Node(s) with NCM list, and select Yes, No, or Never.

If you remove a node from SolarWinds NCM, all data associated with the node, such as configs and inventory data, are also removed.
View node interface details

The interface details view displays the following information about interfaces being monitored on NCM nodes.

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

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 Interfaces under Node Details.
   b. Adjust the slider to the appropriate interval.
   c. Click OK.

Firmware vulnerability data

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

Click a vulnerability in the summary view to view and manage the vulnerability information. For more information about working with vulnerability data, see Add firmware vulnerability files.
**View firmware vulnerability reports**

1. Click Reports > All Reports.
2. Use the Group By list to locate a report.
3. Click the report.

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 Applicable</td>
<td>Lists nodes with their corresponding vulnerabilities with a status of Not Applicable, meaning that the vulnerability 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>


Node management

These reports list vulnerabilities discovered in the last run of the vulnerability matching logic. That logic is based on data last downloaded from sources in Firmware Vulnerability Settings.

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>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>
<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 vulnerability data.</td>
</tr>
<tr>
<td>CVSS V2 Base Score</td>
<td>The Common Vulnerability Scoring System (CVSS) uses a set of metrics to determine the severity of a determined vulnerability. The metrics analyze and assign a value to these aspects related to exploiting a vulnerability: access required, access complexity, authentication requirement, confidentiality protection, integrity or imperviousness of data to change, and availability safeguards.</td>
</tr>
<tr>
<td>Severity</td>
<td>A CVSS score determines the severity of a vulnerability as Low (0-3.9), 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-</td>
</tr>
</tbody>
</table>
Troubleshoot firmware vulnerability reports

<table>
<thead>
<tr>
<th>REPORT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>managed nodes.</td>
<td></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>

Troubleshoot 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>
</table>
| CVSS V2 Base Score | 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:  
  ▪ Access required  
  ▪ Access complexity  
  ▪ Authentication requirement  
  ▪ Confidentiality protection  
  ▪ Integrity or imperviousness of data to change  
  ▪ Availability safeguards |
| Severity | A CVSS score determines the severity of a vulnerability as:  
  ▪ Low (0-3.9)  
  ▪ Medium (4.0-6.9)  
  ▪ High (7.0-10.0) |
Node management

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td></td>
<td>- Not applicable</td>
</tr>
<tr>
<td></td>
<td>- Remediation planned</td>
</tr>
<tr>
<td></td>
<td>- Remediated, Waiver</td>
</tr>
</tbody>
</table>

Provides an option to apply selected state to some or all nodes.

Access firmware vulnerability settings

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
5. Click Submit.

Add 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.

Save an XML source to your SolarWinds NCM server

1. Log in 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
Access firmware vulnerability settings

C:\ProgramData\SolarWinds\NCM\Vuln\Xml.

3. Copy a vulnerability announcement XML file to that folder.

Access firmware vulnerability settings

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.

Change the vulnerability announcements folder

1. Under Vulnerability Data Import Settings, enter the location of the folder that includes the XML files of vulnerability announcements.
2. Click Submit.

Add direct URLs

1. Under Vulnerability Data Import Settings, click Add New.
2. Select Direct URLs to XML Vulnerability Announcements Data Files to Be Automatically Downloaded and Imported into Database.
3. Enter the URL to the vulnerability announcements XML file.
4. To test the file, paste the URL into a browser. The server should return XML data.
5. Click Submit.

Download firmware vulnerability data and import into SolarWinds NCM

Because of a change from the National Institute of Standards and Technology (NIST), SolarWinds NCM can no longer download new firmware vulnerability data. This data must be downloaded from NIST and imported into SolarWinds NCM.

Verify the vulnerability announcements folder

1. Click Settings.
2. Under Product Specific Settings, click NCM Settings.
4. Under Vulnerability Data Import Settings, verify the location of the folder with vulnerability announcements XML data.
Download firmware vulnerability data and import into SolarWinds NCM

1. Log in to your SolarWinds NCM server.
2. Download the firmware vulnerability .zip files from NIST.
3. Extract the contents of the .zip files to the location verified above. The default location is C:\ProgramData\SolarWinds\NCM\Vuln\Xml.
4. Under Vulnerability Search Settings, click Run Now.

Manage 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 SolarWinds NCM devices. You can also search for specific nodes and assign EOS dates based on information related to device models. Automatic refresh of EOS data occurs once per day.

1. Click My Dashboards > Configs > End of Support.
2. SolarWinds NCM shows the End of Support and End of Sales Lookup data currently associated with your SolarWinds NCM devices.

**SolarWinds neither verifies nor supports EOS data provided by EOS Lookup. Consult your vendor with any data-related issues or questions.**

If you want to set EOS dates for a node, select the node and click Assign Dates, wherein you can choose an optional date for vendor models or define your own dates.

Refresh EOS dates

SolarWinds 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.
1. Click My Dashboards > Configs > End of Support.
2. Select the devices for which you want updated data, if available. Use the Group By list if necessary.
3. Click Refresh Suggested Dates.

**Assign EOS dates**

1. Click My Dashboards > Configs > End of Support.
2. Select the devices for which you want updated data, if available. Use the Group By list 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 click OK.
5. Search the table for the model of your selected SolarWinds NCM nodes in the Choose Dates table. If you find it, select that row.
6. Search the table for the model of your selected SolarWinds 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 a SolarWinds NCM user.
7. If you did not find the model of your selected SolarWinds NCM nodes but want to assign dates anyway, select Option 2 and define your own dates.
8. Add comments, and click Assign.

**Ignoring Devices in EOS Management**

1. Click My Dashboards > Configs > End of Support.
2. Select the devices for which you want updated data, if available.
3. Click Ignore Devices.
Node management

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 SolarWinds 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 SolarWinds NCM nodes, but you want to assign dates anyway, select Option 2 and define your own dates.

7. Add comments as needed.

8. Click Assign.

Export EOS information

1. Click My Dashboards > Configs > End of Support.
2. Select the devices for which you want updated data, if available. Use the Group By list if necessary.
3. Click Export, and select the format.
4. Select a location, and click OK.

Filter EOS data

By default, SolarWinds NCM presents data in the End of Support and Sales table for all nodes it manages. SolarWinds 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, SolarWinds 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.
Delete EOS data

1. Click My Dashboards > Configs > End of Support.
2. Select the devices for which you want updated data, if available. Use the Group By list if necessary.
3. Click Delete EOS Data.
4. Click OK.

Search for network addresses

SolarWinds NCM 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 NCM, and always update your inventory prior to a search, especially when searching for a MAC address.

Find IP addresses

1. Click My Dashboards > Configs > Config Summary.
2. Under Search NCM, type the address pattern you want to find.
   For example, 10.199.[2-12].[10-200], searches for nodes 10-100 in the subnets 10.199.3.0 through 10.199.12.0.
3. Click Search.

Find 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. Click My Dashboards > Configs > Config Summary.
2. Under Search NCM, type the pattern you want to find.
3. Click Search.

Find hostnames

If you network supports DNS, you can search for NCM nodes by hostname.
Node management

1. Click My Dashboards > Configs > Config Summary.
2. Under Search NCM, type the pattern you want to find. SolarWinds NCM automatically searches on the string in any part of the current property value(s) in the database.
3. Click Search.

**How does SolarWinds NCM find addresses?**

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 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.
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.

**SolarWinds NCM macros**

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

All SolarWinds NCM macros are enclosed in $\{\}$. The macro for system name, for example, is $\{\text{SysName}\}$. You can concatenate any number of macros in each editable node field. For example, the macros $\{\text{SysName}\} \{\text{Vendor}\}$ 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.

**Supported macro types**

<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: ${\text{SysName}}$ 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 ${\text{GlobalCommunityString}}$, 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: ${\text{ConfigType}}$.</td>
</tr>
</tbody>
</table>
Node management

<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: ${DownArrow} simulates sending the Down Arrow key while connected to the device.</td>
</tr>
</tbody>
</table>

**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.

**Access custom macros**

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
3. Under Advanced, click Manage Macros.

**Create a custom macro**

1. Click Add New.
2. 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 10/10/2015
3. Click Submit.

**Edit a custom macro**

1. Select the macro, and then click Edit.
2. Modify the value of the macro.
3. Click Submit.
Delete a custom macro

1. Select the macro.
2. Click Delete.
3. 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

Search for connected ports

1. Click My Dashboards > Configs > Config Summary.
2. Under Find Connected Port for End Host, select the Search By filter, and enter a value in the Find field.
3. Click Edit in the resource header 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:
## Node management

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>For Wired Devices</strong></td>
<td></td>
</tr>
<tr>
<td>Node</td>
<td>Vendor and model of context node</td>
</tr>
<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>
## Unmanage and remanage 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.

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

### Access the management page

Click Settings > Manage Nodes.

### Unmanage nodes

Select the nodes you want to unmanage in the nodes list, and click Unmanage.

### Remanage nodes

Select the nodes you want to remanage in the nodes list, and click Remanage.

<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>
Manage Orion Web Console user accounts

Users need an Orion Web Console account to perform actions in your SolarWinds product, such as acknowledging alerts. Default account views and privileges are assigned in the account manager.

You may not need to grant all users accounts if they only need to review reports or access views. See Share views with non-Orion Web Console users for more information.

Add users individually, add group accounts, or use Active Directory accounts. If a user is in multiple group accounts, the permissions of the group highest on the Groups tab of the Account Manager are applied to the user. By default SolarWinds uses MSAPI to authenticate Active Directory users, but you can authenticate users with LDAP.

To prevent issues with accounts, make sure that your SQL Server does not have the no count connection option enabled.

For more information, see the following topics:

- Create users
- Define what users can access and do
- Set default menu bars and views for users
- Limit users to specific network areas

Create users

Check out this video on account permissions and limitations.

Before you begin, consider what tasks the user must perform, and what views and menu bars are most suitable.
Manage Orion Web Console user accounts

Users created using default settings can log in to the Orion Web Console and see information available in views, resources, and reports. For administration and customization tasks, users need extra rights.

<table>
<thead>
<tr>
<th>Task</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add and edit user accounts and reset passwords.</td>
<td>Allow Administrator Rights</td>
</tr>
<tr>
<td>Add, edit, and delete nodes.</td>
<td>Allow Node Management Rights</td>
</tr>
<tr>
<td>Enable/disable monitoring elements.</td>
<td>Allow Account to Unmanage Objects</td>
</tr>
<tr>
<td>Add, edit, schedule, and delete reports.</td>
<td>Allow Report Management Rights</td>
</tr>
<tr>
<td>Add, edit, and delete alerts.</td>
<td>Allow Alert Management Rights</td>
</tr>
<tr>
<td></td>
<td>To only allow some actions, keep No in Allow Alert Management rights and Allow items in the Alerts section as appropriate.</td>
</tr>
<tr>
<td>Customize views.</td>
<td>Allow Account to Customize Views</td>
</tr>
<tr>
<td>Access only a set of devices (type, location, department, and so on).</td>
<td>Click Add Limitation and define the limitation.</td>
</tr>
</tbody>
</table>
Create users based on existing Active Directory or local domain accounts

1. Log in to the Orion Web Console, and click Settings > All Settings.
2. Click Manage Accounts in the User Accounts grouping, and click Add New Account on the Individual Accounts tab.

3. Select Orion individual account, and click Next.

4. Provide the account credentials, and click Next.

5. On Define Settings, provide rights so that the user can perform assigned tasks, select default views and menu bars, and then click Submit.

The user account is listed in the Individual Accounts tab.

See Define what users can access and do for information about assigning rights to users.

Create users based on existing Active Directory or local domain accounts

Users can use their existing Active Directory credentials to log in to the Orion Web Console, so you do not need to manage an extra user account.

ℹ️ You must enable Windows Account Login in the Orion Web Console.
Manage Orion Web Console user accounts

1. Click Settings > All Settings, and in Product Specific Settings, click Web Console Settings.
2. In Windows Account Login, select Enable automatic login, and click Submit.
   - To maintain administrative privileges, individual and group Windows user accounts must be defined in the same domain as the SolarWinds server they can access.
   - Only Security AD groups are supported. Distribution Groups are not supported.

1. Log in to Orion Web Console, and click Settings > All Settings.
2. Click Manage Accounts in the User Accounts grouping, and click Add New Account.
3. Select Windows individual account or Windows group account, and click Next.

4. Provide the credentials for an account with administrative access to the Active Directory or local domain, and click Next.
5. If a system account is available, you can use it. Select Use [Account Name] account to access Active Directory or Local Domain, and click Test Active Directory.

You may need to specify the credentials manually.

6. To specify the credentials manually, select Specify credentials to access the Active Directory or Local Domain, and provide the credentials.

7. Search for the Active Directory or local domain account.

To search for all users or groups in the domain, enter domain name\* and click Search.

8. Select the appropriate users in the Add Users area, and click Next.

9. On Define Settings, provide rights so that the user can perform assigned tasks, select default views and menu bars, and then click Submit.

Users can now log in to the Orion Web Console using their local domain or Active Directory credentials.

If you use Active Directory, users can also automatically login with their Windows credentials.

**Set user account access**

1. Click Settings > All Settings.
2. Under User Accounts, click Manage Accounts.
Manage Orion Web Console user accounts

3. Select an account, and click Edit.
4. Review the description next to each option and adjust settings.
5. Review the following notes about each option, and 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>
<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>OPTION</td>
<td>NOTE</td>
</tr>
<tr>
<td>---</td>
<td>---</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 None, and your intention is to hide all NCM-related features and functions, select None for all view settings. If you do not set them to None, and you select None as the NCM role for the account, the user will still see My Dashboards &gt; Configs and all the NCM views. For details see Setting Default Account Menu Bars and Views.</td>
</tr>
</tbody>
</table>
| Network Configuration Manager Settings > NCM Role | 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 WebUploader, which enables the account user to make changes to device configurations and submit them for approval. 
Select None if you do not want this account to access NCM. A user with the NCM role None 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 My Dashboards > Home > Summary. 
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 Add Node option does not appear), and NCM properties are hidden when the user edits a node. 
If an account user with NCM role None sets up an NCM Alert Action, Orion Web Console displays an error in Alert Details. |

## Limit users to specific network areas

Account limitations ensure that Orion Web Console users only view the network objects that are relevant to their job duties.

You can use account limitations in the following ways:

- 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
Manage Orion Web Console user accounts

Predefined account limitations use built-in SolarWinds Orion properties to limit user access. For greater flexibility, you can create your own account limitations in the Account Limitation Builder, based on custom properties.

Set user level login credentials

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

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
4. Enter a valid SolarWinds NCM user name and password.
5. Select an Enable Level if you want to limit the account to a specific level of access on relevant network devices.
6. If you select an Enable Level, enter the password for it.
7. Click Submit.

Restrict user access to network areas by applying limitations

Account limitations restrict user access to specific network areas or withhold certain types of information from designated users.

To limit user access, apply a limitation on the user account, and specify the network area the user can access. Depending on the limitation, you can use logical operators and wildcards.

Pattern limitations can have a negative impact on performance and are error prone.

If the default limitations are not enough, you can create limitations based on custom properties, and apply them on user accounts.

• Group limitations are not applied until after the group availability is calculated.
• Because SolarWinds NetFlow Traffic Analyzer (NTA) initially caches account limitations, it may take up to a minute for account limitations to take effect in SolarWinds NTA.
1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the User Accounts grouping, click Manage Accounts.
4. Edit an individual or group account.
   a. Click Add Limitation in the Account Limitations section.
   b. Select the type of limitation to apply, and click Continue.
   c. Define the limitation, and click Submit.
      The limitation will be added to the Edit Account page.
5. Click Submit.

When the user logs back in, the account respects the limitations applied to it.

**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 SolarWinds Orion Web Console. For more information about custom properties, see Create a custom property. After you have defined custom properties and populated them with data, you may use the Account Limitations Builder as directed in the following procedure.

**Create limitations based on custom properties**

You can define the part of a monitored network that users can access based on custom properties, and create custom limitations. Custom limitations are added to the list of available limitation types that you can apply on individual user accounts. After you create the limitation, you must edit accounts to use the limitation, and then select how the account is restricted.

1. Click Start > All Programs > SolarWinds Orion > Grouping and Access Control > Account Limitation Builder.
2. Click Start on the splash screen.
3. Click Add Limitation.
Manage Orion Web Console user accounts

4. Select a Custom Property. The fields are populated automatically based on your selection.

5. Choose a Selection Method.

   - **Pattern matching** is the most powerful selection, but it is also the selection most prone to errors when restricting access and impacts performance.

6. Click OK.

Your account limitation is added to the top of the table view. You may now apply the limitation on user accounts to restrict user access to monitored objects in the Orion Web Console.

**Delete account limitations**

Deleting a limitation makes it unavailable for future use in the Orion Web Console. If the limitation is applied to user accounts, the accounts will remain limited.

- **This procedure requires access to the computer that hosts the SolarWinds Orion server.**

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

The limitation is now unavailable for limiting user accounts in the Orion Web Console.

**Patterns for limitations**

When restricting user access to network areas, you can specify the limitation with patterns using **OR, AND, EXCEPT, and NOT** operators with _ and * as wildcards if the limitation allows pattern matching.
Patterns are not case sensitive.

You may 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.

Set default menu bars and views for users

The items users see in My Dashboards and in Alerts & Activity are specified in their user accounts.

1. Click Settings > All Settings in the menu bar.
2. In the User Accounts grouping, click Manage Accounts.
3. Select a user, and click Edit.
4. Scroll down to Default Menu Bars and Views, and select top menu bars from the lists.

5. Select Yes for the items the user will see in the Alerts & Activity menu bar.
Manage Orion Web Console user accounts

6. Select an item and use the arrows to change the order of menu bars. Select an item from the list to specify the default Home page view.

<table>
<thead>
<tr>
<th>Tabs ordering</th>
<th>Home</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Network</td>
</tr>
<tr>
<td></td>
<td>Applications</td>
</tr>
<tr>
<td></td>
<td>Storage</td>
</tr>
<tr>
<td>Home Page View</td>
<td>New York IT Summary</td>
</tr>
</tbody>
</table>

7. Click Submit.

The user can now use the specified links in My Dashboards and Alerts & Activity menu bars.

New account settings are applied when a user next logs in.

You can set default view for feature-specific views, such as hardware health or F5, or for product-specific view, such as VSAN or Application Details.

**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 will 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. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. Click Manage Accounts in the Accounts grouping of the Orion Website Administration page.
4. Select the account you want to configure.
5. Click Edit.
6. Select the sound file you want to play when new alerts arrive from the Alert Sound list.
   Note: By default, sounds are stored in the Sounds directory, located at C:\Inetpub\SolarWinds\NetPerfMon\Sounds. Sounds in .wav format that are added to this directory become available as soon as the Edit User Account page refreshes.
7. Click Submit.

**Change account passwords**

When you log in to the Orion Web Console for the first time, SolarWinds recommends that you change the password for the Admin account.

Only users with administrator rights can change the password.

1. Log in to the Orion Web Console, and click Settings > All Settings.
2. Click Manage Accounts in the User Accounts grouping.
Manage Orion Web Console user accounts

3. Select a user, and click Change Password.

4. Enter and confirm the new password, and click Change Password.
Configuration files

When nodes are added to NCM, you can download and edit the configuration files of those devices, compare configuration changes, and create an archive of config files for backup. NCM recognizes any configuration file with a minimum of 11 lines as valid for file transfer. You can change this default value if you plan to work with configuration files that have fewer lines.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
3. In the Configs section, select Configs.
4. Under Config Transfer, use the slider bar to adjust the value for Config Min Length, or type the new value. This setting changes the default value for the minimum number of lines recognized by NCM as valid for download.

Use the Simultaneous Downloads/Uploads value to throttle the load that a big job could put on the network. By default, this value is set to 25 download/upload sessions.

| Tip | If you plan to use NCM to back up device configurations that are in binary file format, complete the Setup required for Binary Configs. Editing or running comparisons on binary configuration files are not currently an option in NCM. |

Setup required for Binary Configs

SolarWinds NCM stores binary configuration files that you download on a network share. If you will be managing device configurations that are in binary format, you must first specify the network share that you want NCM to use.

1. Click Settings > All Settings in the menu bar.
2. In the Product Specific Settings section, select NCM Settings.
3. In the Configs section, select Binary Config Storage Settings.
4. Enter the path to the network share. For example: \MYLAB-SERVERNAME-01\binarystorage.
5. Enter the credentials required to access the network share.
Configuration files

6. To validate the connection before submitting your settings, click Validate.
7. When finished, click Submit.

The NCM server must be in the same domain as the network share system.

Download configuration files in NCM

Download configuration files to view the current configuration of your managed devices, compare current and previous configurations, or archive configuration files for backup. SolarWinds NCM can transfer files using direct and indirect transfers.

If a configuration includes the command prompt character, SolarWinds NCM stops downloading. SolarWinds NCM provides the UseExactPromptMatch device template command you can use to instruct NCM to act on the command prompt only if it appears on a separate line. For more details about using this command, see Troubleshooting: Confine recognition of the command prompt during download.

Download from a single node

1. Click My Dashboards > Configs > Config Summary. Use an account that has the WebDownloader, WebUploader, Engineer, or Administrator role.
2. Under NCM Node List, click a node in the list.
3. Click Configs on the left.
4. Under Download Config, select the config type, and click Download.

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. If you receive a connection error, click Fix Connection in Device Template, and follow the Device Template wizard.
6. Follow the prompts of the Device Template wizard:

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

1. Click My Dashboards > Configs > Jobs.
2. Click Create New Job.
3. Name the job, and then select Download Configs from Devices from Job Type.

   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 an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if this job relates to a business rule, and click Next.
6. Select the nodes to target with this job, and click Next.
7. Select an email notification option, and click Next. If you click Email Results, the default Email Notification Settings and SMTP Server Settings and SMTP Server Settings are populated. These settings can be overridden in each job.
8. Select the configuration types you want to download.
9. Set your notifications preference, and click Next.
10. Review the settings for the job, and click Finish.

Enable a new config type

You can create a custom type of configuration to download from relevant devices. To do this you must enable SolarWinds 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 SolarWinds 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.
Enable a new config type for a device

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
3. Under Configs, click Configs.
4. Under Config Types, enter a name for the new config type.
5. Click Add New.
6. Click Submit.
7. See the Communication process diagrams to modify your device template with an appropriate statement.

Enable the config and policy caches

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

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
5. Click Submit.

Edit config files

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

1. Click My Dashboards > Configs > Config Summary. 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 click Edit Config.
5. Edit the Config Title if necessary.
6. Select Edit Config Text, and make changes.
7. Add comments, and click Submit. The revision is saved in the Config List with the indication that it is an Edited config of its type.

Upload the edited config file

1. Under Upload Config, select the edited config file.
2. Click Upload.

Troubleshooting: Confine recognition of the command prompt during download

By default, SolarWinds NCM stops downloading a config file that contains the device command prompt in the body of the config.

Use the UseExactPromptMatch command to prevent SolarWinds NCM from recognizing the command prompt unless it appears on a separate line:

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
4. Select a device template.
5. Click Edit > Using XML Editor.
6. Add this line to the Template XML:
   
   ```
   <Command Name="UseExactPromptMatch" Value="true"/>
   ```
7. Click Save.

Compare configs

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

When comparing files, you can select comparison criteria for excluding lines that contain a specific string pattern. See Define comparison criteria to learn how to specify the criteria to filter the comparison results.

1. Click My Dashboards > 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 a single node.
4. Click Compare Node(s) Configs.
5. Select the configs you want to compare.
6. Review the configs for changes (yellow), added lines (green), and missing lines (red).
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. If you want a PDF of the config comparison, click Export to PDF in the top right.
11. Click Close.

You can adjust the default settings for how the comparison results will display. Go to the NCM Config Settings and specify the Config Comparisons options.

**Define 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 expressions 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.

Access NCM Configs settings and you can then create, edit, enable, disable, or delete a regular expression.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
3. Under Configs, click Comparison Criteria.

**We provide Comparison criteria: exclusion examples** to help you with the regular expressions. Other resources, such as Regular-Expressions.info, are available online to learn more about regular expressions.
Create a new regular expression

1. Click Add New.
2. Enter a title, and write the regular expression.
3. Select Enable NCM to Ignore This Pattern When Comparing Config Files to activate this pattern, or leave it disabled for future editing.
4. Click OK.

To apply a regular expression, you must enable it.

Edit a regular expression

1. Select a regular expression in the Comparison Criteria screen, and click Edit.
2. Change the title or the regular expression.
3. Select Enable NCM to Ignore This Pattern When Comparing Config Files to activate this pattern, or leave it disabled for future editing.
4. Click OK.

Enable or disable a regular expression

Select one or more items in the Comparison Criteria screen, and click Enable or Disable.

Delete a regular expression

Select one or more regular expressions in the Comparison Criteria screen, and click Delete.

Comparison criteria: exclusion examples

The following are examples of regular expression pattern combinations that SolarWinds NCM could use to exclude lines in comparing selected configurations:

^! Last
   Ignores the !Last Configuration change line in Cisco configurations.
^ntp clock-period
   Ignores the ntp clock-period line in Cisco configurations.
^wlccp ap username cisco
   Ignores the wlccp line in Cisco access point configurations.
Configuration files

Exclusions specified with regular expressions are global, and used for all comparison operations throughout SolarWinds NCM, including scheduled jobs.

For more information, see Regular Expression Pattern Matching.

Comparison results overview

SolarWinds NCM displays a comparison overview 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 you are comparing.

Execute a script on a node

This resource is available to users with the WebUploader, Engineer, or Administrator role.

The script you execute must be saved as a text file that can be uploaded from the client computer. For more information about creating command scripts, see Creating an executable command script.

1. Click My Dashboards > Configs > Configuration Management.

   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 locate it in the file system.

   You can specify a delay in seconds inside a script. A delay is the time SolarWinds NCM waits 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.

**View the results**

1. Click My Dashboards > 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.

If execution fails, see *Troubleshoot script execution*. Alternatively, try executing the script by creating a job.

**Upload a config**

This resource allows you to upload a configuration file you have previously downloaded from this node to SolarWinds NCM.

This resource helps you easily correct unauthorized or incorrect changes made to a device configuration. You can also write the uploaded configuration to NVRAM, essentially making it the startup configuration for the device.

In the case of a multi-node upload/download operation, the Simultaneous Downloads/Uploads setting can be used as a throttle. By default it runs 25 sessions simultaneously.

For IPv6, you can rediscover devices that were previously discovered with the engine using IPv4. 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. Telnet and SSH communications are supported.

ℹ️ If you selected a binary configuration for upload, editing of the configuration is not an option from the Upload Config screen; instead you will see the Binary Config notation in the editing pane.
Configuration files

Upload a config to one or more nodes

1. Click My Dashboards > Configs > Configuration Management.
   If you do not have administrator privileges you may not be able to see some nodes. Your account must be a member of the WebUploader group to upload configs.
2. Select one or more nodes, and click Upload Config.
3. Expand the tree to locate the correct node.
4. Select the config you want to upload.
5. Click Advanced and select options, if desired.
6. Click Upload.

Import config files

You can import configuration files that you have already downloaded from your devices into SolarWinds NCM. NCM imports Configuration files that use the following file formats:

- SolarWinds NCM Archive: .Config
- SolarWinds Cisco Config Downloader: .CiscoConfig
- Text File: .txt
- Configuration File: .cfg
- Any file in ASCII text

Import a config file

1. Click My Dashboards > Configs > Configuration Management.
2. Select a node.
3. Under Nodes Details, click Configs.
4. Under Config List, click Import Config.
5. Click Choose File, and browse to the config file.
6. Click Submit.

What is a baseline?

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.
Set a baseline

Use a baseline to compare future downloads against.

Set a baseline

1. Click My Dashboards > Configs > Configuration Management.
2. Click a node.
3. Click Configs on the left.
4. Under Config List, select the config, and click Set/Clear 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.

Remove a config file as a baseline

1. Click My Dashboards > Configs > Configuration Management.
2. Click a node.
3. Click Configs on the left.
4. Under Config List, select the current baseline.
5. Click Set/Clear 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.

Baseline 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 Adjust inventory settings.
1. Click My Dashboards > 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 an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if this job relates to a business rule, and click Next.
6. On the Choose Nodes tab, click Next.
7. Select an email notification option, and click Next. If you click Email Results, the default Email Notification Settings and SMTP Server Settings and SMTP Server Settings are populated. These settings can be overridden in each job.
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 click Finish.

**Clear all baselines to reset the comparison point for config changes**

1. Click My Dashboards > 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 an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if this job relates to a business rule, and click Next.
6. On the Choose Nodes tab, click Next.
7. Select an email notification option, and click Next. If you click Email Results, the default Email Notification Settings and SMTP Server Settings and SMTP Server Settings are populated. These settings can be overridden in each job.
8. Click Clear All Baselines, and click Next.
9. Review the settings for the job, and click Finish.
Upload configuration changes

For a multi-node upload or download operation, the Simultaneous Downloads/Uploads setting can be used as a throttle. By default it is set to run 25 Sessions simultaneously. To change this setting, see Configuration files.

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.

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

Upload an entire configuration

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

Create a config archive for local or network storage

Create a config archive for local storage

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
3. Under Configs, click Configs.
4. Under Config Archive, select Save a Copy of Each Config to the Config Archive Directory, As It Is Downloaded.
5. If you are low on storage space and only need the last and current configs, select When Configs Are Edited, Only Retain the Last Version.

6. Type the path of the local directory to store the NCM Config Archive.
   By default, SolarWinds NCM sets the directory for the config archive as %PROGRAMDATA%\SolarWinds\NCM\Config-Archive\ As preparation for a growing archive, SolarWinds recommends moving the config archive to a different location.

7. Type the template you want to use when naming the configuration files. For more information, see Configuration archive variables.

8. Click Submit.

Create a config archive for network storage

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
5. Enter credentials, and click Validate Credentials.
   If credentials fail to validate, check that the NCM-related account has Windows permissions for the network storage.
6. Click Settings > All Settings.
7. Under Product Specific Settings, click NCM Settings.
8. Under Configs, click Configs.
9. Under Config Archive, select Save a Copy of Each Config to the Config Archive Directory, As It Is Downloaded.
10. If you are low on storage space and only need the last and current configs, select When Configs Are Edited, Only Retain the Last Version.
11. Type the path of the network storage for the config archive.
12. Type the template you want to use when naming the configuration files. For more information, see Configuration archive variables.
13. Click Submit.
Real time change detection

The Real Time 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 change detection requirements**
- **Configure real time change detection for NCM**

**Real time change detection 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 [Run 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.
Configuration files

Configure real time change detection

The SolarWinds Syslog and Trap Services must be configured to run as administrator so that scheduled jobs are processed correctly. For detailed steps, see Run 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 configuration on your device, you will receive a trap message about those changes only when you enter config mode the next time. That is, usually not until another change to the configuration needs to be done. Due to this behavior, SolarWinds recommends that you use the syslog option for setting up real-time change detection.

Access real-time change detection settings

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
3. Under Real Time Change Detection, click Configure Real Time Change Detection. You must complete all six steps for Real Time Change Detection (RTCD) to operate correctly.

Step 1: Manually configure your devices to send syslog or trap messages

1. Click My Dashboards > Configs > Configuration Management.
2. Select the node(s), and then click Execute Script.
Step 2: Configure alerts and filters triggered by syslog and trap messages

3. Paste in the commands from the following examples, changing the IP address to match your device:

**Syslog (IOS)**

```plaintext
config terminal
  logging 10.199.3.43
  logging trap 6
end
```

**Syslog (CatOS)**

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

**Traps (IOS)**

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

**Traps (CatOS)**

```plaintext
set snmp trap 10.110.68.33 public config
set snmp trap enable config
```

4. Click Execute.

5. Click Transfer Status.

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

7. Click Show Script Results in the Status/Details column.

For more information, refer to the documentation for each network device.

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

Step 2: Configure alerts and filters triggered by syslog and trap messages

**Cisco devices that send change notifications using syslog messages**

1. Start Syslog Viewer in the SolarWinds Orion program folder.
2. Click View > Alerts/Filter Rules.
4. Click OK.
Non-Cisco devices that send change notifications using syslog messages

1. Start Syslog Viewer in the SolarWinds Orion program folder.
2. Click View > Alerts/Filter Rules.
3. Click Add New Rule.
4. Provide the appropriate information under General and DNS Hostname.
5. Click Message.
6. In the Message Type Pattern field, type the pattern to find.
   The message pattern varies 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 of your device.
7. Click Alert Actions, and click Add New Action.
8. Select Execute an External Program, and click OK.
Step 2: Configure alerts and filters triggered by syslog and trap messages

9. 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. 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.

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

10. Click OK.

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

Devices that send change notifications using SolarWinds Kiwi Syslog Server

1. Start the Kiwi Syslog Server Console in the SolarWinds Syslog Server Console program folder.
2. Click File > Setup.
3. Click Filter, and right-click New Filter to rename it.
4. Select Field > Message Text and Filter Type > Simple, and type the message to include with a syslog notification.
5. Right-click Actions, and rename New Action.
Configuration files

6. In the Program File Name field, type
   \Path\Orion\SolarWinds.NCM.RTNForwarder.exe.
   Where:
   \Path
      The location of the Orion folder. If the path contains spaces, enclose the
      path section of the statement in quotation marks: "Path to
      executable".

7. Add the string %MsgIPAddr,RTN,%MsgText to Command Line Options
8. Click Apply/OK.
9. Ensure the appropriate filter and action are selected in Rules lists, and click
   OK.

Devices that send change notifications using SNMP trap messages

1. Start the Trap Viewer in the SolarWinds Orion program folder.

   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.

2. Click View > Alerts/Filter Rules.
3. Click Add Rule.
4. Provide the appropriate information on the General and DNS Hostname tabs.
5. Click Conditions, and click Add a Condition.
6. 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).
7. Click the asterisk, and 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.
8. 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 of your device.

9. Click Alert Actions.
10. Click Add Action.
11. Select Execute an External Program, and click OK.
12. Type the following in the Program to execute field:

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

   Where:

   Path
   The location of the Orion folder. 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.

13. Click OK.
14. Ensure the new rule is selected in the Alerts/Filter Rules tab of the Trap Server Settings window, and click OK.

**Devices that send change notifications to a system other than SolarWinds NCM**

1. Start your third-party Syslog or SNMP Trap receiver.
2. Set up an alert that executes an external program.
3. Type the following in the Program to execute field:

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

   Where:

   Path
   The location of the Orion folder. 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.
Configuration files

4. Save the alert, and make sure it is enabled.

Step 3: Config changes

1. Click Config Changes.
2. 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.

   If the check box is disabled, then Device Login and User Account Credentials is set to Global – Device Level on the Security resource, located at Settings > NCM Settings > Security. Click Security to change that setting if necessary.

3. Select Include Syslog/Trap Message in NCM Email Notification if desired.
4. Click Submit.

Step 4: Config downloads and notifications

1. Click Config Downloads and Notification Settings.
2. Under Previously Downloaded Config File, make a selection from Monitor This File Type.
3. Under Baseline Config File, select the config file type against which you want to compare differences with the file downloaded as part of the RTCD operation.
4. Select the relevant Email Notification Options
5. Enter the Sender Name, Subject, and To address information to be used in sending out RTCD email notifications. Reply Address is optional.
6. Click Submit.

Step 5: Enter NCM SMTP server details

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 Approval system for device configuration changes

1. Click NCM SMTP Server.
2. Enter the fully qualified domain name (FQDN) or IP address of the mail server.
3. Enter the port number on which the mail server handles messages.
4. Select None or Password as the Authentication method.
5. Enter a user name and password.
6. Click Submit.
Step 6: Enable real time config change notifications

1. Click Enable.
2. Click Submit.

Limit real time notification download operations

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

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
3. Under Configs, click Configs.
4. Adjust the number of Simultaneous Download/Uploads. The default number of concurrent sessions is 10.
5. Click Submit.

Run 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 select Administrator.
4. Click OK.
5. Right-click SWTrapService.exe and click Run As.
6. Click The Following User, and select Administrator.
7. Click OK.

Search for config files in the web console

Complete the following procedure to search for specific strings of text within the configuration files stored in the Orion platform database. Search may not find a config newly added to the database for up to 10 minutes.
Configuration files

1. Click My Dashboards > Confis > Config Summary.
2. Under Search NCM, click Advanced Search.
3. Enter a string pattern. For information on using Regular Expressions, see Regular Expression Pattern Matching.
4. Select a search target from the list: All, Nodes, Confis from All Nodes, or Confis 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 click Search again.

Delete config files from the database

1. Click My Dashboards > Confis > Configuration Management.
2. Use the Group By list to find the node, and click it.
3. Under the node list in the center, click + to expand the list of confis under the targeted node.
4. Under the Suggested Action column, click Delete beside the relevant config.

Automate config 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.

1. Click My Dashboards > Confis > Jobs.
2. Click Create New Job.
3. Name the job, and then select Purge Old Confis from Database from Job Type.
4. Select the Schedule Type. If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if this job relates to a business rule, and click Next.
6. Select the nodes to target with this job, and click Next.
9. Select a Save option.
10. Select an email notification option, and click Next. If you click Email Results, the default Email Notification Settings and SMTP Server Settings and SMTP Server Settings are populated. These settings can be overridden in each job.

11. Select a PurgeConfigs option, and then click Next.

12. Review the settings for the job, and click Finish.
Device templates

It may be necessary to create a new device template or modify a supplied template to add support for your device in SolarWinds NCM. To prepare for creating device templates that meet your needs, follow these suggestions:

**Before You Begin**

- First, gather the information you will need for the device template.
- For additional guidance, review the "Best practices for device command templates".
- Review the Communication Process diagrams.

> If using the F5 templates to manage BIG-IP F5 device configurations, see the "F5 device template behavior" in the reference section for important details.

**Gather 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>
</tbody>
</table>
### Device templates

<table>
<thead>
<tr>
<th><strong>QUESTION</strong></th>
<th><strong>NOTE</strong></th>
<th><strong>EXAMPLE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>What command is used to disable pagination?</td>
<td>This command is the value used in the template <strong>RESET</strong> command.</td>
<td>terminal pager 0</td>
</tr>
<tr>
<td>What command is used to reboot the device?</td>
<td>This command is the value used in the template <strong>Reboot</strong> command.</td>
<td>reload noconfirm</td>
</tr>
<tr>
<td>What command is used to enter configuration mode?</td>
<td>This command is the value used in the template <strong>EnterConfigMode</strong> command.</td>
<td>config terminal</td>
</tr>
<tr>
<td>What command is used to exit configuration mode?</td>
<td>This command is the value used in the template <strong>ExitConfigMode</strong> 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 <strong>Startup</strong> command.</td>
<td>startup</td>
</tr>
<tr>
<td>What command is used to</td>
<td>This command is the value used in the template <strong>Running</strong> command.</td>
<td>running</td>
</tr>
<tr>
<td>QUESTION</td>
<td>NOTE</td>
<td>EXAMPLE</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>specify the running configuration?</td>
<td>command.</td>
<td>show ${ConfigType}</td>
</tr>
<tr>
<td>What command sequence is used to directly download the configuration using Telnet or SSH?</td>
<td>This command sequence is the value used in the template DownloadConfig command*.</td>
<td></td>
</tr>
<tr>
<td>What command sequence is used to upload the configuration using Telnet or SSH?</td>
<td>This command sequence is the value used in the template UploadConfig command*.</td>
<td>${EnterConfigMode}${CRLF} ${ConfigText}${CRLF} ${ExitConfigMode}</td>
</tr>
<tr>
<td>What command sequence is used to download the configuration using SNMP, that</td>
<td>This command sequence is used in the template DownloadConfigIndirect command*.</td>
<td>copy ${TransferProtocol}://${StorageAddress}/${StorageFilename} ${ConfigType}${CRLF}${CRLF}</td>
</tr>
</tbody>
</table>
## Device templates

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>NOTE</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>is, indirect transfer?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What command sequence is used to erase the configuration?</td>
<td>This command sequence is used in the template <code>EraseConfig</code> command.</td>
<td><code>write erase ${CRLF}Yes</code></td>
</tr>
<tr>
<td>What command sequence is used to commit a configuration to memory?</td>
<td>This command sequence is used in the template <code>SaveConfig</code> command.</td>
<td><code>write memory</code></td>
</tr>
<tr>
<td>What command sequence is used to show the version information?</td>
<td>This command sequence is used in the template <code>Version</code> command.</td>
<td><code>show version</code></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](#).

### Best practices for device command templates

Review 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.
Best practices for device command templates

- 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 the # character, add the following line to the template: <Command Name="EnableIdentifier" Value="*"/>

- 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%"/>

- Ensure you use the MenuBased command when using the VirtualPrompt command: <Command Name="MenuBased" Value="false"/> or <Command Name="MenuBased" Value="true"/>.
Device templates

- 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=""/>.

<i>Not all commands are supported on all devices.</i>
Communication process diagrams
Create Device Templates in NCM

SolarWinds NCM allows you to create or edit device templates using the following methods:
Create a device template with the interactive wizard

- Using the interactive wizard
- Using the XML editor

Create a device template with the interactive wizard

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
5. Use the Level and Group By lists to organize the node list.
6. Select a node, and click Next. NCM pulls the OID value from the properties of the node you select.
7. Choose the scope of operation for this device template, and click Next.
8. Verify and adjust Connection Profile and Device Template settings.
9. Click Test, and click Next.
10. Verify and adjust Download Command and Config Types settings.
11. Set the config type to use in the download test, and click Perform Download Test.
12. Click Next.
13. Enter and adjust the Device Template and Assign Device Template settings, and click Finish.

Create a device template with the XML editor

The interactive wizard guides you through the options to help you create a device template. If you prefer, you can use an XML editor to create the template.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
4. Click Add New > Using XML Editor.
5. Add information to the template, and modify the XML according to your device.
6. Click Save.
Device templates

Edit a device template

If you need to modify an existing SolarWinds NCM device template, you can edit it using the interactive wizard or the XML editor.

Edit a device template with the interactive wizard

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
4. Select a device template, click Copy, name the copy, and click Save.

Since you may have applied the existing template to nodes, it is best to copy and rename the template before making changes.

5. Select the copied template, and click Edit > Using Interactive Wizard.
6. Use the Level and Group By lists to organize the node list.
7. Select a node, and then click Next. NCM pulls the OID value from the properties of the node you select.
8. Choose the scope of operation for this device template, and click Next.
9. Verify and adjust Connection Profile and Device Template settings.
10. Click Test, and click Next.
11. Verify and adjust Download Command and Config Types settings.
12. Set the config type to use in the download test, and click Perform Download Test.
13. Click Next.
14. Enter and adjust the Device Template and Assign Device Template settings, and click Finish.

Edit a device template with the XML editor

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
4. Select a device template, click Copy, name the copy, and click Save.

Since you may have applied the existing template to nodes, it is best to copy and rename the template before making changes.

5. Select the copied template, and click Edit > Using XML Editor.
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"/>
```

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.

7. Click Save.
8. Select the template again, and click Assign to Nodes.
9. Select nodes, and click Submit.

**Confirm the device template is working**

1. Click My Dashboards > Configs > Config Summary.
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 succeed, the device template is working as expected.

**Sample CLI device command templates**

Two examples of device command templates for CLI devices are provided below:

- **Cisco IOS example**
- **Nortel BayStack 380 example**

For a list of commands and their descriptions, see [Command template commands](#).
Device templates

**Cisco IOS example**

**File Name**
Cisco IOS-1.3.6.1.4.1.9.ConfigMgmt-Commands

**Contents**

```xml
<!--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}${CRLF}"/>  
    <Command Name="UploadConfigIndirect" Value="copy 
${TransferProtocol}://${StorageAddress}/${StorageFilename} 
${ConfigType} ${CRLF}"/>  
    <Command Name="EraseConfig" Value="write erase${CRLF}Y"/>  
    <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
SCP example of config upload and download

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 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} ${TransferProtocol}:${TransferProtocol}/${StorageAddress}/${StorageFilename}${CRLF}"/>  
  <Command Name="UploadConfigIndirect" Value="copy ${TransferProtocol}:${TransferProtocol}/${StorageAddress}/${StorageFilename} ${ConfigType}\{CRLF}"/>  
  <Command Name="Version" Value="show sys info"/>  
  <Command Name="PreCommand" Value="${CTRL+Y}"/>  
</Commands>  
</Configuration-Management>
Create 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="${ENTER}${DownArrow}${DownArrow}${DownArrow}${DownArrow}${DownArrow}${DownArrow}${DownArrow}${DownArrow}"
```

You could instead assign:
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:

```xml
<Commands>
  <Command Name="RESET" Value=""/>
  <Command Name="Reboot" Value=""/>
  <Command Name="EnterConfigMode" Value=""/>
  <Command Name="ExitConfigMode" Value=""/>
  <Command Name="Startup" Value=""/>
  <Command Name="Running" Value=""/>
  <Command Name="DownloadConfigIndirect" Value="${Downarrow}${Downarrow}${Downarrow}${Downarrow}${Downarrow}${Downarrow}${Downarrow}${CRLF}${CRLF}${StorageFilename}${CRLF}${StorageAddress}${CRLF}${DownArrow}${CRLF}"
    Delay="300" RegEx="written"/>
  <Command Name="UploadConfig" Value=""/>
  <Command Name="EraseConfig" Value=""/>
  <Command Name="SaveConfig" Value=""/>
  <Command Name="Version" Value="${DownArrow}${DownArrow}${DownArrow}${DownArrow}${DownArrow}${DownArrow}${DownArrow}${CRLF}${CRLF}" RegEx="Event Log"/>
  <Command Name="PreCommand" Value="${CTRL+Y}"/>
</Commands>
```
Device templates

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}${Downarrow}${Downarrow}${Downarrow}
   ${CRLF}
   ${CRLF}
   ${StorageFilename}${CRLF}
   ${DownArrow}${StorageAddress}${CRLF}
   ${DownArrow} ${CRLF}
   
   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:
   ```xml
   <Command Name="DownloadConfigIndirect" Value="${Downarrow}$
   ${Downarrow}${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 use Enable as the command.</td>
</tr>
<tr>
<td>EnableIdentifier</td>
<td>Only used when a device does not return the # character 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 device. Use pre-command variables to declare the command values. For more information, see Pre-command and command template variables.</td>
</tr>
</tbody>
</table>
## Command template commands

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>EnterConfigMode</code></td>
<td>Series of commands used to enter the configuration mode of a device</td>
</tr>
<tr>
<td><code>ExitConfigMode</code></td>
<td>Series of commands used to exit the configuration mode of a device</td>
</tr>
<tr>
<td><code>IPAddress</code></td>
<td>The IP address of the server where SolarWinds NCM is installed</td>
</tr>
<tr>
<td><code>MenuBased</code></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 <code>VirtualPrompt</code> and <code>EnterCLI</code> commands to do so. Valid values are true or false.</td>
</tr>
<tr>
<td><code>MenuDrivenConfigStart</code></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 <code>##########</code>. The information sent after the ten hash signs is saved as the requested configuration file.</td>
</tr>
<tr>
<td><code>More</code></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><code>Precommand</code></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><code>Reboot</code></td>
<td>Series of commands used to reboot the device</td>
</tr>
<tr>
<td><code>RebootAt</code></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>
</tbody>
</table>
## Device templates

<table>
<thead>
<tr>
<th>PROPERTY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Version</td>
<td>Series of commands used to display the software version of the device.</td>
</tr>
<tr>
<td>VirtualEnablePrompt</td>
<td>Allows you to specify a regular expression and search for the defined value in the entirety of a device response. This command is often used with menu-based devices, allowing you to locate a specific phrase returned by the device. When specified, ensure you also declare the MenuBased command as true or false.</td>
</tr>
<tr>
<td>VirtualPrompt</td>
<td>Specifies the command prompt that will be sent when the device is ready for command input. Use this command along with the MenuBased command to specify the exact prompt SolarWinds NCM should wait to receive before sending commands.</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 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>${CTRL+A}</td>
<td>CTRL + A</td>
</tr>
<tr>
<td>${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>
</tbody>
</table>
## Device templates

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>${CTRL+W}</td>
<td>CTRL + W</td>
</tr>
<tr>
<td>${CTRL+X}</td>
<td>CTRL + X</td>
</tr>
<tr>
<td>${CTRL+Y}</td>
<td>CTRL + Y</td>
</tr>
<tr>
<td>${CTRL+Z}</td>
<td>CTRL + Z</td>
</tr>
<tr>
<td>${CTRL+[}</td>
<td>CTRL + [</td>
</tr>
<tr>
<td></td>
<td>Equivalent to Esc key press</td>
</tr>
<tr>
<td>${CTRL+}</td>
<td>CTRL + \</td>
</tr>
<tr>
<td>${CTRL+]</td>
<td>CTRL + ]</td>
</tr>
<tr>
<td>${CTRL+CTRL}</td>
<td>CTRL + CTRL</td>
</tr>
<tr>
<td>${CTRL+_}</td>
<td>CTRL + _</td>
</tr>
<tr>
<td>${UPARROW}</td>
<td>Up Arrow</td>
</tr>
<tr>
<td>${DOWNARROW}</td>
<td>Down Arrow</td>
</tr>
</tbody>
</table>
### Pre-command device template entry example

<table>
<thead>
<tr>
<th>PROPERTY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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>

**Pre-command device template entry example**

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.

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

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

**Preclude pseudoterminal setup with command template variables**

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:

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

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

Declare a special command prompt with command template variables

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 # character, 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.

Switch user context with command template variables

If you log in 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.

Respond to post-login interaction requests with command template variables

If you log in 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.

**Troubleshoot 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. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
4. Select Enable Session Tracing.
5. Perform the steps to recreate the issue you are troubleshooting.
6. Open the session trace file.
7. Apply the necessary changes to the device command template to resolve the issue. For more information, see [Device templates](#).

**F5 device template behavior**

When using device templates for F5 devices, consider the following behavior.

**Device setup prerequisites**

- Set the Terminal Access user on the device to Advanced Shell. Do not use Traffic Management Shell (TMSH).
- Verify the device can reach the NCM server for configuration transfers using SCP.
Device templates

- If you plan to upload binary user configuration set (UCS) files, the upload can take a long time. Increase the NCM timeouts to have a complete upload report.
  1. Click Settings > NCM Settings > Protocol Settings.
  2. Set Telnet/SSH Connection Timeout: 360 seconds
  3. Telnet/SSH Prompt Timeout: 300 seconds

Template details

If you set up NCM to transfer configurations using SSH:

- The template can download the current running config.
- You cannot download the startup config.
- You cannot upload the running or startup config
  - If you set up NCM to transfer configurations using SCP:
  - The template can download and upload a text single configuration file (SCF) as a running config.
  - The template can download and upload a binary UCS as startup config.
  - You cannot upload the running config to startup, or startup to running config.

Downloading or uploading configs using TFTP is not supported.
**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.

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

**Creating an executable command script**

1. Click My Dashboards > Configs > Configuration Management.
2. Click the Script Management tab.
3. Click Add New Script.
4. Add the script information.
5. Click Save.
6. To execute the script, on the Config Management tab select one or more nodes and follow the steps to Execute a script on a node.

If you experience problems with the script execution, see Troubleshoot script execution.

**Use variables in 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.
Command scripts

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

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

Define 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.

Reference 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:

`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.

**Troubleshoot script execution**

If a script fails to execute on a SolarWinds NCM node, review the log for a possible cause. The log is located at

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

Alternatively, execute the script by creating a job.
Managing Inventory

The inventory engine of SolarWinds Network Configuration Manager compliments the product's configuration management functions. You can perform inventory scans on all of your nodes, node groups, or on a single node. You can also manage the inventory collection process. The collected inventory statistics are displayed in the detail view of each device.

Run an inventory scan

You can run a scan at any time to get the latest statistics on your full inventory of managed devices in NCM. You may also run a single-node 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 Adjust inventory settings.

Run 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 Adjust inventory settings.

1. Click My Dashboards > Configs > Configuration Management.
2. Use the Group By list and select No Grouping.
3. Select all nodes.
4. Click Update Inventory.

To run an inventory scan as a recurrent job, see Baseline your entire network

Run an inventory scan on a single node

1. Click My Dashboards > Configs > Configuration Management.
2. Use Search or the Group By list to find a node.
3. Select the node, and click Update Inventory.
Managing Inventory

Schedule an inventory scan

1. Click My Dashboards > 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 an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if this job relates to a business rule, and click Next.
6. Select the nodes to target with this job, and click Next.
7. Select an email notification option, and click Next. If you click Email Results, the default Email Notification Settings and SMTP Server Settings and SMTP Server Settings are populated. These settings can be overridden in each job.
8. Select the information types to include in the Inventory job, and click Next.
9. Review the settings for the job, and click Finish.

Adjust inventory settings

This setting gives you some control over the type of information collected by NCM for the inventory, as well as other settings that help you manage the inventory process. For example, it may be necessary to change the number of devices that NCM can inventory concurrently.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
3. Under NCM Node Management, click Node Inventory.
4. Select the information types to collect.
5. Adjust the number of devices that should be inventoried concurrently. The default is five.
6. 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.
7. If the inventory process causes the SolarWinds NCM server to hang or if the process takes too long, select Disable Inventory Lookup. Determine what caused the problem, for example, inadequate server capacity, before re-enabling Inventory Lookup.

8. Click Submit.

**View inventory status**

1. Click My Dashboards > Confis > Configuration Management.
2. Click the Inventory Status tab.
3. Click a column to change the sort order.
Policy reports

Policy reports help ensure that device configurations conform to both internal business practices and federal regulations, such as the Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability (HIPAA), and Computer Inventory of Survey Plans (CISP). You might also want to use the Payment Care Industry (PCI) data security policies, and Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG) reports to monitor compliance.

For more information about generating DISA STIG policy reports, see Configuring DISA STIG reports.

Policy reports scan configuration files and report any discovered rule violations. For example, a rule may require 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 includes the line number where the violation occurred in the listed violations. Several example reports, policies, and rules are included with SolarWinds Network Configuration Manager.

If you decide to create policy reports, understand Rules that define the criteria, such as pattern strings, applied in Policies used by NCM to determine compliance.

Create a policy report in SolarWinds NCM

The NCM predefined reports may not fit your exact needs for monitoring compliance of a particular device. You can create a policy report and select policies available in NCM or create your own policies and add them to the report.

1. Click My Dashboards > Configs > Compliance.
2. Click Manage Policy Reports.
4. Name the report, and enter a description.
5. Select settings for Save in Folder and Display Settings.
6. Select policies from folders under All Policies, and click Add. If your policy is
not listed, see Create a policy

7. Click Submit.

Schedule a policy report

1. Click My Dashboards > Configs > Jobs.
2. Click Create New Job.
3. Name the job, and select Generate a Policy Report from Job Type.
4. Select the Schedule Type. If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if this job relates to a business rule, and click Next.
6. On the Choose Nodes tab, click Next.
7. Select an email notification option, and click Next. If you click Email Results, the default Email Notification Settings and SMTP Server Settings and SMTP Server Settings are populated. These settings can be overridden in each job.
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 click Finish.

Remediating a policy violation

1. Click My Dashboards > 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.
Export a policy report to thwack

1. Click My Dashboards > Configs > Compliance.
2. Click Manage Policy Reports.
3. Select a report, and click Export to thwack.
4. If prompted, enter your user name and password, and then Log In.

Export a policy report as a file

1. Click My Dashboards > Configs > Compliance.
2. Click Manage Policy Reports.
4. Verify that a pop-up blocker does not prevent the file from being downloaded.
5. Download the file to a local folder.

Edit a policy report

1. Click My Dashboards > Configs > Compliance.
2. Click Manage Policy Reports.
3. Select a report, and click Edit.
4. Edit the appropriate values.
5. Click Submit.

Delete a policy report

1. Click My Dashboards > Configs > Compliance.
2. Click Manage Policy Reports.
3. Select a report, and click Delete.
4. Click Yes.
Configuring DISA STIG reports

SolarWinds NCM provides for compliance checks of your devices with DISA standards. The Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG) reports are available in your NCM installation. To run the reports that specify the appropriate policies for your devices, make sure that you have first defined the node "Device_Type" in custom properties for your device type.

For example, for Cisco devices, specify the Device_Type and OS in custom properties with the following options:

**Device Types:**
- PRTR, PL3S, IRTR, IL3S, L2SW, FW

**OS types supported:**
- IOS, NX, XE, ASA

Likewise, for F5 devices, specify the Device_Type in custom properties.

Creating a DISA STIG Dashboard

You can set up a dashboard specifically to monitor compliance. To create a DISA STIG compliance dashboard, see the complete details in How to Create a DISA STIG Dashboard on THWACK.

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>
</tbody>
</table>

166
### Customize Policy Violation Levels

<table>
<thead>
<tr>
<th>PROPERTY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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>
<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>

### Customize Policy Violation Levels

By default, NCM provides three violation levels for compliance reports. You can select one of these levels in rules to specify the alert level of the violation.

- Level 1: Informational
- Level 2: Warning
- Level 3: Critical
Policy reports

You can customize the descriptor of the violation level to have a different meaning for the level.

1. Click Settings > All Settings. If you are on the Compliance Policy Reports view, click NCM Settings in the top right of the view.
2. In the Compliance Policy Report Management section, select Manage Violation Level.
3. In the text field for the level that you are changing, replace the word describing that level.
4. Click Submit.

Create 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. Click My Dashboards > Configs > Compliance.
2. Click Manage Policy Reports.
3. Click the Manage Rules tab, and click Add New Rule.
4. Name the rule, and then enter a description.
5. Select settings for Alert Level and Save in Folder.
6. Select the type of Alert trigger.
7. Enter a String and select the String Type.
8. Create a script under Remediation to modify the lines of configuration if they do not comply with the policy rule.
   - 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, such as Telnet or 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 SolarWinds NCM executes commands against targeted devices to remediate a policy rule violation.
   - CLI allows SolarWinds 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.
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.
   - 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 configuration that is not compliant, 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 click Submit.

Advanced string matching

1. Click My Dashboards > Configs > Compliance.
2. Click Manage Policy Reports.
3. Click the Manage Rules tab, and then click Add New Rule.
4. Name the rule, and then enter a description.
5. Select settings for Alert Level and Save in Folder.
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.

   If there are 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, using 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 then create the string.
11. Repeat this step for as many strings as you need to define your search.
   For example: 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, create the following logic:
   
   ```
   Must Contain ^(?=.*?\bAccess-list\b)(?=.*?\joe\b).*$
   OR Must Contain ^(?=.*?\bAccess-list\b)(?=.*?\sam\b).*$
   OR Must Contain ^(?=.*?\bAccess-list\b)(?=.*?\t\tom\b).*$
   ```
   A violation of this rule logic occurs if SolarWinds 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.
   - 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, such as Telnet or 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 Remediaiton Script type. Your selection determines how SolarWinds NCM executes commands against targeted devices to remediate a policy rule violation.
   - CLI allows SolarWinds 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.
   - 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 configuration that is not compliant, 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 SolarWinds 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.

20. Click Select Different Config to continue your rule test on another config.

21. Click Close, and click Submit.

**Edit a policy rule**

When you run policies in NCM, you may determine that you need to modify a rule in the policy if you are getting false positives on violations.

1. Click My Dashboards > Configs > Compliance.
2. Click Manage Policy Reports.
3. Click the Manage Rules tab.
4. Select a rule, and click Edit.
5. Edit the appropriate values.
6. Click Submit.

**Delete a policy rule**

1. Click My Dashboards > Configs > Compliance.
2. Click Manage Policy Reports.
3. Click the Manage Rules tab.
4. Select a rule, and click Delete.
5. Click Yes.
Policy reports

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.

Create 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. Click My Dashboards > Configs > Compliance.
2. Click Manage Policy Reports.
3. Click the Manage Policies tab, and click Add New Policy.
4. Name the policy, and enter a description.
5. Select settings for Save in Folder and Select Nodes.
6. Select the Search Most Recent Config Type to search for with this policy.
7. Select rules from folders under All Policy Rules, and click Add. If your rule is not listed, see Create a policy rule.
8. Click Submit.

Edit a policy

1. Click My Dashboards > Configs > Compliance.
2. Click Manage Policy Reports.
3. Click the Manage Policies tab.
4. Select a policy, and click Edit.
5. Edit the appropriate values.
6. Click Submit.

Delete a policy

1. Click My Dashboards > Configs > Compliance.
2. Click Manage Policy Reports.
3. Click the Manage Policies tab.
4. Select a policy, and click Delete.
5. Click Yes.
Enable the config and policy caches

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

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
5. Click Submit.

Manually refresh the policy cache

1. Click My Dashboards > Configs > Compliance.
2. Click Update All.

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.
Jobs

SolarWinds Network Configuration Manager provides job scheduling to automate the management of network devices and configuration files.

You can schedule numerous operations, including configuration file uploads and downloads, node reboots, and command script execution.

Orion Platform Administrator, NCM Administrator and NCM Engineer roles have full access to all jobs in the job list. Other assigned SolarWinds NCM roles can access and manage only the jobs they create, but not others.

Create or edit 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. Click My Dashboards > 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 click Edit.
4. Name the job, but do not use special characters in the name.
5. Select a Job Type.
6. Select the Schedule Type. If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
7. Add a comment if this job relates to a business rule, and click Next.
8. Select the nodes to target with this job, and click Next.
9. Select an email notification option, and click Next. If you click Email Results, the default Email Notification Settings and SMTP Server Settings and SMTP Server Settings are populated. These settings can be overridden in each job.
10. Add details based on the specific job, and click Next.
11. Review the settings for the job, and click Finish.
Enable a Job

The enable operation applies to jobs that run according to a schedule. You must enable a job in SolarWinds NCM before you can start it. A job that is not enabled will not start.

1. Click My Dashboards > Configs > Jobs.
2. Select a disabled job in the list.
3. Click Enable.

To disable a job, select a job that is scheduled and enabled in the Jobs list and then click Disable.

Disable a job

The disable operation applies to jobs that run according to a schedule. You can delete any job in SolarWinds NCM that you no longer use.

Disable a job to suspend it, but not delete it.

1. Click My Dashboards > Configs > Jobs.
2. Select a scheduled job in the list.
3. Click Disable.

Start a job

Though using a schedule is the most efficient way to manage jobs, you can manually start a job if necessary.

You can start any job that is enabled.

1. Click My Dashboards > Configs > Jobs.
2. Select a job in the list.
3. If the job is disabled, click Enable.
4. Click Start Job.
Stopping a Job

Though using a schedule is the most efficient way to manage jobs, you can manually stop a job if necessary.

A job currently running shows the status: running.

1. Click My Dashboards > Configs > Jobs.
2. Select a running job in the list.
3. Click Stop Job.

View job logs

View the job log to verify that a job was run as scheduled, or to view the history of the job.

1. Click My Dashboards > 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.

Delete a job

Permanently remove a job, rather than temporarily disable it.

1. Click My Dashboards > Configs > Jobs.
2. Select a disabled job in the list.
3. Click Delete.
Approval system for 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.

Set up config change approval

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. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
4. Select an approval mode, and click Submit.
5. Enter SMTP settings, and click Submit.
6. Enter Admin Email settings.
   - If you are using one-level approval, the addresses in the To field receive 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.
7. Click Submit.
Approval system for device configuration changes

8. If you selected one-level approval, click Manage Users to adjust the NCM role for accounts that will be submitting upload requests, and follow the steps in Create, edit, and delete NCM accounts. Otherwise, click Finish.

9. 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 click Finish.
   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 click Edit.

10. 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.

Turn on approval system

After setting up the configuration change approval system in NCM, you need to enable the system to send approval notifications and process acknowledgments. The approval system can be disabled at any time.

Enable config change approval

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.

- 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. Review the default settings and user roles and make adjustments as necessary before enabling the approval system.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
3. Under Config Management Change Approval, click Enable Approval System.
4. Click Enable.
Disable config change approval

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 WebUploader account privileges.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
3. Under Config Management Change Approval, click Disable Approval System.

View, approve, and decline approval requests

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
3. Under Config Management Change Approval, click Pending Approval.
4. Select a request in the list, and click Approve or Decline.

Create, edit, and delete NCM accounts

Only a user with Administrator privileges can create a new account and prepare it for use with NCM.

Access account settings

1. Click Settings > All Settings.
2. Under User Accounts, click Manage Accounts.

Create a new account

1. Click Add New Account.
2. Select Orion Individual Account, and click Next.
3. Enter credentials for the new account, and click Next.
4. 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.

5. Click Submit.

**Edit an existing account**

1. Select an account, and click Edit.
2. 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.
3. Click Submit.

**Delete an account**

1. Select an account.
2. Click Delete.

**Device access information**

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 Set 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.

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 login flow.
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

Access and log in to the Orion Web Console

To access 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 in 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.

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 Personalize the web console.
Orion Web Console

**Summary**

Click My Dashboards > Home > Summary to view 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.

**Node Details**

Navigate to Node Details by clicking the name of a node in the SolarWinds NCM Web Console. Then click the Configs tab on the left.

**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.

**Inventory Details**

Displays a list of inventory reports that pertain to the selected device.
Firmware Vulnerabilities

Lists vulnerabilities discovered in the last run of the vulnerability matching logic.

Policy Violations

Displays a list of the policy reports available that pertain to the selected device.

Last 5 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 Configs

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.

All Active Alerts

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.

Search NCM

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. Click My Dashboards > Configs > Config Summary.
2. Under Search NCM, click Advanced Search.

**Config Summary**

Click My Dashboards > Configs > Config Summary.

**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.
Find Connected Port for End Host

Search for currently connected ports on wired or wireless end hosts.

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.

End of Support Devices

Displays a list of devices that have reached or will soon reach their end of support dates.

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 devices that have been backed up using SolarWinds NCM in comparison to those that have not been backed up.

NCM Events

Specify a time period and the configuration events you want to see displayed. To modify the time period, click Edit.

Overall Devices Inventoried vs. Not Inventoried

Displays a pie chart designating the percentage of devices inventoried in relation to those that have not.
Orion Web Console

**Configuration Management**

Click My Dashboards > Configs > Configuration Management.

**Download**

Download running, startup, or custom configurations for the selected nodes.

**Compare Nodes(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.

**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**

Click My Dashboards > Configs > Config Change Templates.

**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.

**Compliance**

Click My Dashboards > Configs > 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**

Click My Dashboards > Configs > Jobs.

The Jobs list in SolarWinds NCM displays the jobs that NCM supplies by default and those created by users. SolarWinds NCM provides a set of unique jobs. You can create your own jobs and duplicate jobs to schedule a new job.

Use the Jobs page to create and run jobs, monitor run times, and enable or disable scheduled jobs.

**End of Support**

Click My Dashboards > Configs > End of Support.

End of Support tracks the end of support and sales statuses of your SolarWinds NCM nodes.

**Personalize the web console**

Click My Dashboards > Configs > Config Summary. Then click Customize Page.

You can then select the resources to include, drag and drop resources from one column to another, or drag and drop resources in a different order in the same column. Changes are saved as preferences associated with the logged on user account.

**Integration 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
Orion Web Console

- Run a trace route to the selected node
- Remote desktop to the selected node
Alerts for SolarWinds NCM actions

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.

Types of alert actions

In executing one of its alert-related actions, SolarWinds NCM requires a role with sufficient permissions and cannot use device access credentials to authorize its action.

As a security enhancement related to executing NCM actions, NCM account passwords are not stored in the database. As part of configuring NCM 7.5, 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 alert:

- Backup Running Config
- Execute Config Script
- Show Last Config Changes
Alerts for SolarWinds NCM actions

**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 at Alerts & Activity > 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.

**Apply 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 in the device configuration trigger it, this predefined alert does these three things in order:
1. Backs up the running config on the alerting device.
2. Determines the last config changes made on the device.
3. Sends an email regarding the alert to a relevant administrator that includes the results of both NCM actions.

**Apply the default NCM alert**

1. Click Alerts & Activity > Alerts.
2. Click Manage Alerts.
3. Select Object Type from the Group By list, and 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 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 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 alert actions.
13. On Reset Actions, create actions to execute when the resets the alert, and 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.
Add scripted commands to the default NCM alert

You can modify the default SolarWinds 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. Click Alerts & Activity > Alerts.
2. Click Manage Alerts.
3. Select Object Type from the Group By list, and select Node.
4. Select Alert Me and Trigger an NCM Action.
5. Click Duplicate & Edit.
7. Select Execute an NCM Action, and click Configure Action.
8. Select Execute Config Script, and enter a 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.

Navigate 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 three ways:

- Settings Page (Recommended)
  - Click Settings > All Settings in the menu bar. Under Alerts & Reports, click Manage Alerts.
Use alerts to monitor your environment

- Active Alerts Details
  - From the Active Alerts Details page, click Manage Alerts in the Management resource.
- Node Details
  - On the Node Details page, navigate to the All Alerts this Object can trigger resource, and then click Manage Alerts.

**Use alerts to monitor your environment**

An alert is an automated notification that a network event has occurred, such as a server becoming unresponsive. The network event that triggers an alert is determined by conditions you set up when you configure your alert. You can schedule alerts to monitor your network during a specific time period, and create alerts that notify different people based on how long the alert has been triggered.

The types of events for which you can create alerts vary, depending on the Orion Platform products you have installed. For example, you can create an alert to notify you if a node in a specific location goes down or if the network response time is too slow when you have NPM. If you have installed SAM, you can receive alerts about application response times or when your Exchange mailbox database is almost full.

You can create alerts for any monitored object. Most Orion Platform products allow you to alert against interfaces, volumes, and nodes.

Use the following topics to get started if you have never used Orion Platform products:

- Alert preconfiguration tasks
- Best practices and tips for alerting
- Navigate to the Alert Manager
- Create new alerts to monitor your environment
- Alert me when a server goes down

Use the following topics to get started with web-based alerts if you have upgraded to Core version 2016.1 or later:

- Changes in the Alerting Engine
- Manually set a custom status
Alerts for SolarWinds NCM actions

- Build complex conditions
- Manage alert actions

You can also view our Alert Lab on thwack for community-based alert information.

**Alert preconfiguration tasks**

Some alerts require extra configuration, separate software installations, or information that you may need to request from other departments.

Alert actions that require set up before creating or configuring alerts include:

- Send an email or page
- Dial a paging or SMS service
- Play a sound when an alert is triggered
- Send an SNMP trap
- Use the speech synthesizer to read alerts

ℹ️ Monitored objects in the SolarWinds Orion database must exist before creating or configuring alerts. Monitored objects can include items such as nodes, databases, and applications.

**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.

**Enable out of the box alerts**

If there are out of the box alerts that match your monitoring needs, enable them in your environment. You can customize the alert actions for those alerts. If you want to modify the conditions, use the alert as a template.
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.

Create new alerts to monitor your environment

Navigate to the Alert Manager to create a completely new alert definition, or duplicate an alert that is similar to the alert you want to create.

1. Enter the alert properties, which includes who can view the alert, severity, and how frequently the alert conditions are evaluated.
2. Define the conditions must exist to trigger the alert.
3. Define what event occurs to reset the alert.
4. Schedule when you want the alert to monitor your environment.
5. Define what happens when an alert is triggered.
6. Define what happens when the alert is reset.
7. Review your alert, including the number of alerts that will be triggered based on the conditions you defined.

You can skip to different steps if you clicked Duplicate & Edit or if you are editing a saved alert.
Alerts for SolarWinds NCM actions

Once you have created an alert, it is added to the list of available alerts in the Alert Manager. When the alert is enabled, it immediately monitors your environment for the conditions necessary to trigger it.

Set alert properties

After creating a new alert, use the Alert Properties to describe the alert, including which users can view the alert.

Name of alert definition

This is a required field. 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 them.

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.

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.

Evaluation Frequency

Set how frequently you want to evaluate the conditions. If you choose 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.

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.
Severity of Alert

Control how the alert in the Active Alerts resource looks, and use to group or filter alerts more easily.

Alert Custom Properties

Use custom properties to 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 use it in an alert.

Alert Limitation Category

Restrict who can view the alerts. For example, managed service providers can restrict alerts to their specific customers. Create a new alert limitation by editing or creating a user account.

Click Next to define the conditions must exist to trigger the alert.

Define the conditions that must exist to trigger an alert

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. To see an example of completed trigger conditions, see the Alert me when a server goes down 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.

Filter your environment to just the objects you want to monitor in The scope of alert. Use the Show List link to view all of the objects that the alert monitors.
Alerts for SolarWinds NCM actions

1. Choose what objects you want to monitor in the I want to alert on field.
2. Establish how much of your environment you want to monitor in The scope of alert.

   - All objects in my environment (Show List)
   - Only following set of objects

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

   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".

   You can evaluate objects based on variables or macros.
Define the conditions that must exist to reset an alert

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.
   - Send an alert immediately when the condition is met by clearing any selection for Condition must exist for more than.
   - Wait before sending an alert by selecting Condition must exist for more than, and entering how long the condition must exist. This option prevents multiple alerts firing if the condition is temporary.

If you have successfully created an alert condition, you can move to the next step in the alert wizard. The Summary step evaluates the conditions against your environment and returns how many objects will trigger the alert.

Click Next to define what event occurs to reset the alert.

See the following topics for condition examples, explanations, or more information:

- Alerting When a Server is Down
- Building Complex Conditions

Define the conditions that must exist to reset an alert

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 add actions that occur when the reset conditions are met.
Alerts for SolarWinds NCM actions

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.

**When the alert is reset, escalation actions are halted.**

Select one of the following 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 action**

  The alert is active and is never reset. To re-trigger the alert, the alert must be manually cleared from the Active Alerts view.
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.

The alert wizard evaluates the reset condition for errors. If there are no errors, you can proceed to the next step, or go back to previous steps.

See Define the conditions that must exist to trigger an alert or Build complex conditions for more information on creating conditions.

Click Next to schedule when you want the alert to monitor your environment.

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.

Build 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.
Alerts for SolarWinds NCM actions

- 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.

1. Navigate to the Trigger Condition page.
2. Expand Advanced options.
3. Select Enable complex conditions.

You can use complex conditions to do the following:
- Wait for multiple objects to meet the trigger condition before alerting
- Evaluate multiple condition blocks
- Evaluate multiple object types

Manage alert actions

You can edit, test, enable, disable, and delete alert actions from the Action Manager.

Mostly for bulk actions and assigning previously created actions to alerts. View meta data about the action to help troubleshoot alert actions from a single area instead of trying to find the action in an alert.

Assign an action to an alert

You can use actions that you have already configured in multiple alerts. For example, if you have configured an action to email emergency response teams, you can assign this action to multiple alerts. When you assign an alert, it is added to the highest escalation level.

Enable and Disable Alerts

Use the On/Off toggle or select an alert and click Enable/Disable to enable or disable alerts.

Alerts must be enabled to be evaluated. For example, if an alert is scheduled to run for a short period of time each year, it must be enabled so the schedule runs. A disabled alert will not be evaluated, even if it is scheduled to run.
Schedule when an alert monitors your environment

You can configure when an alert monitors your environment. 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 schedule the alert to monitor your network during off hours, and disable the alert during your maintenance windows.

<i>Alerts must be enabled to allow schedules to run.</i>

1. Select Specify time of day schedule for this alert.
2. Click Add Schedule.
Alerts for SolarWinds NCM actions

3. Enter the following information:
   - **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.
   - **Frequency**
     Choose when to monitor on a high level, such as daily, weekly, or monthly.
   - **Enable or Disable 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 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.
     - If you selected Weekly...
       Choose which days the alert is enabled or disabled. You may want to disable alerts during a weekly maintenance window.
     - 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.
   - **Starting on**
     Choose a when to begin 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.

4. Click Add Schedule to create the schedule.

When you add a schedule to an alert, the alert only monitors during the time period you have scheduled, or does not monitor during that time. Alert actions can also have schedules, so not all alert actions may occur during the scheduled period.

Click Next to configure **what happens when an alert is triggered.**
Define what happens when an alert is triggered

Choose actions that occur whenever the trigger conditions are met. You can also set up escalations levels so that different actions occur if the alert has not been acknowledged quickly enough.

Add actions to alerts

By default, what you enter into the Message displayed when this alert field is displayed in the All Active Alerts resource.

You can create a new action or use an action that you have already created. When you reuse an action, you are also reusing all of its configurations, including its schedule and execution settings.

If you are alerting others through email, SolarWinds recommends that you notify a small number of users while you fine tune your alerts.

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. 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 Alert preconfiguration tasks.

Each action has the following sections:

- **Name of action** - This is not required, but makes it easier to organize and find your actions in the Action Manager.
- **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 save it to the list of actions in the alert.

**Add a preexisting action to the alert**

You can add actions that have already been configured to an alert. For example, if you configured an action to reboot a VM, you can add that action to a separate alert.

1. Click Assign Action(s).
2. Select one or more actions from the list.
3. Click Assign.

**Add what happens when an alert is not acknowledged**

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.

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. This lets you quickly craft actions to indicate that the issue has been acknowledged or resolved. Click Copy Actions to Reset Actions Tab.

When an alert is triggered, the actions will be performed in the order that they appear on the list. You can test each action to ensure the action does what you expect it to do.

Click Next to define what happens when the alert is reset.

**Test alert triggers and actions**

You do not have to actually experience a device failure to confirm that your alerts are working. The trigger condition is automatically evaluated and trigger and reset actions can be tested individually.

**Test trigger conditions**

Alert conditions are automatically evaluated on the Summary tab. Scroll to the bottom of the page and view the information box above the Submit button.

**Test alert actions while creating or editing an alert**

When you simulate actions, the action will be performed once regardless of whether the trigger condition is true. If the action sends a message to a recipient, you should reduce the recipient list to yourself and a small number of team members until you are confident the alert is ready to be enabled in your production environment.
Alerts for SolarWinds NCM actions

The Send Email/Page, Play a Sound, and Text to Speech Output actions do not have to fire. You can view what the message will look like when the trigger or reset action fires without performing the action.

1. Click Trigger Actions or Reset Actions.
2. Click Simulate next to the alert action you want to test.
3. Select an object to resolve any variables you have used in your alert action.
4. Click Execute. Test email, play a sound, and text to speech actions without sending an email by clicking Simulate.

**Test alert actions in the Action Manager**

You can also test actions independently by using the Action Manager.

1. Select the action you want to test.
2. Click Test.
3. Select an object to resolve any variables you have used in your alert action.
4. Click Execute. Test email actions without sending an email by clicking Simulate.

After the alert test completes, you can view the results of your alert actions.

- To view the results of your email alert action, open EvaluationAlertLog in your Orion folder, typically `<Volume:>`\ProgramData\Solarwinds \Logs\Orion\ActionsExecution.log.
- To view results of your Syslog message action, click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Syslog Viewer.
- To view the results of your Syslog message action, click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer.

**Define what happens when the alert is reset**

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.

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. Select from the list of Alert 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 and find your actions in the Action Manager.
   - 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.
5. Click Add Action to save it to the list of reset actions in the alert.

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.

When an alert is reset, the actions will be performed in the order that they appear on the list. You can test each action to ensure the action does what you expect it to do.

Click Next to review your alert settings.

**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.
Alerts for SolarWinds NCM actions

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.

Add 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.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Alerts & Reports 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.

   ▪ 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, select Use SSL.

   ▪ Opting to use SSL automatically changes the SMTP port number to 465.

7. If your SMTP server requires authentication, select This SMTP Server requires Authentication, and provide requested credentials.
8. Click Save.
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:

- Change a custom property
- Create a ServiceNow incident
- Dial a paging or SMS service
- Email a web page to users
- Execute an external batch file
- Execute an external Visual Basic script
- Log the alert message to a file
- Log the alert to the NPM event log
- Change the resource allocation of a virtual machine
- Delete a snapshot of a virtual machine
- Move a virtual machine to a different host
- Move a virtual machine to a different storage
- Pause a virtual machine
- Power off a virtual machine
- Power on a virtual machine
- Restart a virtual machine
- Suspend a virtual machine
- Take a snapshot of a virtual machine
- Play a sound when an alert is triggered
- Send a Windows Net message
- Restart IIS sites or application pools
- Send an SNMP trap
- Send a GET or POST request
- Send a syslog message
- Send an email or page
- Manually set a custom status
- Use the speech synthesizer to read alerts
- Log an alert to the Windows Event Log on a specific server
Alerts for SolarWinds NCM actions

Change a custom property

Custom properties are additional fields, such as country, building, asset tag, or serial number, that you can define and store in your SolarWinds Orion database. After properties are added, you can view or filter using them.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Change Custom Property option, and then click Configure Action.
3. Under Custom Property Settings, select the custom property and enter the value you want to change it to.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the value of the custom property you selected changes.

Create a ServiceNow incident

This alert management action is only available if the integration with ServiceNow® is enabled.

For information about configuring ServiceNow integration, see Configure ServiceNow integration.

To use this action, make sure the integration with ServiceNow is enabled on the Alert Summary page. If the Integrate alert with other SolarWinds box is not selected, the incident is created but the integration is not two-sided, so you cannot reset or clear the incidents in ServiceNow®.
Use reference fields

When you configure ServiceNow incidents, you can use reference fields to refer to different database tables in ServiceNow.

The reference value you provide in the Orion Web Console is used in ServiceNow to locate a referenced record. This enables you to use advanced ServiceNow filter expressions.

The reference field's value is usually the Sys ID of the referenced record, and the application by default tries to locate the referenced record by Sys ID.

You can also specify which fields should be used for specific referenced tables when trying to locate a referenced record. Some definitions are defined by default. For example, setting a field user_name for the sys_user table allows you to use the user name in reference fields such as Caller or Assigned to.

You can specify your own reference fields in the SolarWinds Alert Integration application, under Configuration > Incident Reference Fields Definitions, and you can control the order of different fields on the same table by setting different priorities.

Filter expression examples

Reference fields can also be used as filter expressions. The following examples show the configuration of reference fields.

<table>
<thead>
<tr>
<th>REFERENCE FIELD</th>
<th>VALUE</th>
<th>PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment group</td>
<td>name=Hardware</td>
<td>Assigns the incident to the group called Hardware.</td>
</tr>
<tr>
<td>Location</td>
<td>state=TX^city=Austin^streetLIKESouthwest Parkway</td>
<td>Sets the location to Southwest Parkway, Austin, TX.</td>
</tr>
<tr>
<td>Configuration item</td>
<td>mac_address=${N=SwisEntity;M=MAC}</td>
<td>Locates the configuration item based on the MAC address of the interface, by using a</td>
</tr>
</tbody>
</table>
Alerts for SolarWinds NCM actions

<table>
<thead>
<tr>
<th>REFERENCE FIELD</th>
<th>VALUE</th>
<th>PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>macro.</td>
</tr>
</tbody>
</table>

For more information, see the ServiceNow Wiki about reference fields.

Configure a ServiceNow incident

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Create ServiceNow Incident, and click Configure Action.
3. Under Select ServiceNow Instance, specify the ServiceNow instance where you want to create the incident.
4. Under Incident Detail, define the properties of an incident template that will be used for new incidents. For example, here you can define the urgency, impact, and other properties of incidents. Text areas can hold macro variables to add information about alerts and alert objects.

   If the property you want is not displayed in the Incident Detail section, click Select Properties at the bottom of the section, and select the property from the list. Then you will be able to use the properties as reference fields.

5. Under State Management, define the status of the incident when the incident is reset, reopened, acknowledged, and closed. You can also specify notes to be added to the incident.
6. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   This is often used to prevent an action from occurring during specific windows.

7. Select how frequently this action occurs for each triggered alert in Execution Settings.
8. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, an incident will be created or updated in the specified ServiceNow instance.
When you use this alert action, we recommend that you only use it on the trigger tab. It is also recommended that you only use one ServiceNow action per alert.

To deactivate the integrated behavior, remove the alert action from the alert definition.

You can specify one alert action for one ServiceNow instance. To create an incident in another ServiceNow instance, specify another alert action and use a different ServiceNow instance.

### Send an email or page

This action sends an email from the product to selected recipients for investigation into the cause of the alert.

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.

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

Configure the SMTP server in the alert action or from the Settings page.

For more instructions about configuring the SMTP server, see Add an SMTP server.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Send an Email/Page option, then click Configure Action.
3. Enter recipients and the message.

- 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.
- Messaging is disabled if both the Subject and Message fields are empty.

4. Enter the SNMP information.

5. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   This is often used to prevent an action from occurring during specific windows.

6. Select how frequently this action occurs for each triggered alert in Execution Settings.

7. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the email or page is sent.

**Play a sound when an alert is triggered**

The Play a Sound action uses the 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.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Play a Sound option, and then click Configure Action.
3. Under Play a sound settings:
   - If not installed, click Download our desktop notification client to download and install the notification client. From the notification client, select an alert sound.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, a sound plays through the client.
Log the alert message to a file

SolarWinds can be configured to log alerts to a designated file which can be viewed at a later time.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Log the Alert to a File option, then click Configure Action.
3. Under Log to File Settings:
   a. Enter the log filename in the Alert Log Filename field.
   b. Enter a maximum log file size in MB (0 = unlimited).
   c. Enter the Message of your alert trigger in the field provided.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   
   This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the alert is logged to the file with the message you created.

Log an alert to the Windows Event Log on a specific server

You may specify that an alert be logged to the Windows Event Log either on the SolarWinds server or on a remote server for later investigation.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Windows Event Log option, then click Configure Action.
3. Under Event Log Settings:
   b. Enter the Message of your alert trigger.
Log the alert to the NPM event log

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   ![This is often used to prevent an action from occurring during specific windows.]

5. Select how frequently this action occurs for each triggered alert in Execution Settings.

6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the alert message is added to the Windows Event log.

Log the alert to the NPM event log

Record when an alert is triggered to the NetPerfMon (NPM) event log on your SolarWinds Orion server or on a remote server for later investigation.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Log the Alert to the NetPerfMon Event Log from the options, and then click Configure Action.
3. Under Log the Alert to the NetPerfMon Event Log settings, enter the text you want written to the file.

   ![Use variables to make the message dynamic.]

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   This is often used to prevent an action from occurring during specific windows.

5. Expand Execution Settings to select when the action occurs.

6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the alert is logged to the NPM event log with the message you created.
Alerts for SolarWinds NCM actions

Change the resource allocation of a virtual machine

If a virtual machine is experiencing performance issues, you can have an alert trigger a specified allocation of resources. This alert management action is available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Change CPU/Memory Resources, and click Configure Action.
3. Enter a name for the action.
4. Under Select Virtual Machine, specify the virtual machine on which you want to adjust the number of CPUs, the memory capacity, or both.
   a. To change the resource allocation of the virtual machine that triggered the alert, click Execute this action.
   This option is only available if the alert is built to trigger for virtual machines.
   b. To change the resource allocation of a different virtual machine, click Select specific VM, and search for a virtual machine.
5. To power off the virtual machine before changing the resource allocation, and then power it on again after the resource allocation has been changed, select the relevant option.
   If the option is not selected, the action will be performed live on the virtual machine.
6. Under Specify New Resources, specify whether you want to add more resources to the virtual machine, or replace the existing resources with new resources, and then specify the parameters of the new resource or resources.
   a. Select Number of processors, and specify the number of processors to allocate.
   b. Select Memory, and specify the memory capacity to allocate.
7. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   This is often used to prevent an action from occurring during specific windows.
8. Select how frequently this action occurs for each triggered alert in Execution Settings.

9. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified CPU and memory resources will be allocated to the virtual machine.

**Send a syslog message**

SolarWinds can log received alerts to the syslog of a designated machine for later investigation. The following procedure configures an alert to send a message to a designated syslog server.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.

2. Select the Send a SysLog Message option, then click Configure Action.

3. Under Send a SysLog message settings:
   a. Enter the Hostname or IP Address of the syslog server in the field provided.

   > Multiple syslog servers should be separated by commas.

   b. Select a Severity and a Facility from the drop down lists.

4. Enter the Message of your alert trigger in the field provided.

5. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   > This is often used to prevent an action from occurring during specific windows.

6. Select how frequently this action occurs for each triggered alert in Execution Settings.

7. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the syslog message is sent.
Execute an external batch file

There are several circumstances where you may want to execute a program when a specific network event occurs. For example, you may want to run a custom script to reboot your SQL servers.

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.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Execute an External Program option, then click Configure Action.
3. 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 poller and test.bat is your external program to be executed.
   b. Select either Define User or No User Defined for Optional Windows Authentication
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the external program runs.

Execute an external Visual Basic script

In some situations, you may want to execute a Visual Basic (VB) script when a network event occurs to perform a specific action.
SolarWinds recommends that scripts and batch files be placed on the root of C:\ to simplify the path for the batch file.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Execute an External VB Script option, then click Configure Action.
3. Under Execute an External VB Script settings:
   a. Select a VB Script Interpreter from the drop down list.
   b. Enter the Network path to the external VB Script in the field provided. For example: Use c:\test.vbs, where c:\ is the disk on your main Orion poller and test.vbs is your external VB Script to be executed.
   c. Select either Define User or No User Defined for Optional Windows Authentication
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the VB script runs.

**Email a web page to users**

Send a web page, including content of resources available in the Orion Web Console, to others.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Email a Web Page option, then click Configure Action.
3. Enter the Recipients.

   Multiple addresses must be separated with commas.
4. Enter the Subject and Message of your alert trigger email/page.
   - For the Optional Web Server Authentication section, select User currently logged in, Another user, or No user defined.
   - Use variables to make the message dynamic.
   - You can create a dynamic URL to send information about the object that triggered the alert.

5. Enter your SMTP server information.

6. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   - This is often used to prevent an action from occurring during specific windows.

7. Select how frequently this action occurs for each triggered alert in Execution Settings.

8. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, an email is sent to the recipients.

Create a dynamic URL

Use variables to create a URL that changes based on the object that triggers the alert. Click Insert Variable and search for URL to find all of the variables you can use to create the dynamic URL.

For example, enter ${N=SwisEntity;M=DetailsUrl} in the URL field to email a link to the Details view of the object that triggered the alert. When the email is sent, the variable resolves to a valid URL such as http://myserver/Orion/View.aspx?NetObject=N:3 and the email contains the content of the Details view in the body.

Use the speech synthesizer to read alerts

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.

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.

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.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Text to Speech Output option, then click Configure Action.
3. Under Text to Speech Output settings click Download our desktop notification client to download, install, and configure the notification client.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the message is read.

Send a Windows Net message

If a computer is experiencing issues, you can have an alert trigger a Windows Net Message to be sent to a specific computer or to all computers.

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.
Alerts for SolarWinds NCM actions

The only operating systems supporting Windows Net Messaging are Windows Server 2003 and Windows XP or earlier.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Send Net Message option, then click Configure Action.
3. Under Send a Net Message settings:
   a. Enter Computer Name or IP address in the field provided.
   
   You can enter multiple computers or IP addresses by separating them with commas.
   b. Enter the Message of your alert trigger in the field provided.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the message is sent to the selected computers.

Send an SNMP trap

SNMP traps signal the occurrence of significant events by sending SNMP messages to a monitoring device. You can have an alert trigger this action to inform you of these events.

This action requires the following information:

- UDP port number
- SNMP version number
- SNMP credentials

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Send SNMP Trap option, then click Configure Action.
3. Under Send SNMP Trap Message:
   a. Enter SNMP Trap Destinations in the field provided.
      
      Multiple IP Addresses should be separated by commas or semicolons.

   b. Select a Trap Template from the drop down list.
4. Enter the Message of your alert trigger in the field provided.
   a. Optionally click Insert Variable to add variables using the following procedure:
5. 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.
6. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   This is often used to prevent an action from occurring during specific windows.
7. Select how frequently this action occurs for each triggered alert in Execution Settings.
8. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the SNMP trap message is sent.

**Send a GET or POST request**

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.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Send a GET or POST Request to a Web Server option, then click Configure Action.
Alerts for SolarWinds NCM actions

3. Under HTTP request settings:
   a. Enter a URL in the field provided.
   b. Select either Use HTTP GET or Use HTTP POST.

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.

6. Click Add Action.

   The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the GET or POST request is sent to the server. You can view the server logs to confirm that the action occurred.

**Dial a paging or SMS service**

This action forwards alerts to a paging or SMS service. You must download and install NotePager Pro from Notepage.net to your SolarWinds Orion server to use this action.

For instructions on configuring this action, see the NotePage Technical Support page at [http://www.notepage.net/solar-winds/technicalsupport.htm](http://www.notepage.net/solar-winds/technicalsupport.htm) and SolarWinds Network Performance Monitor Integration at [www.notepage.net](http://www.notepage.net).

**Alert me when a server goes down**

Use the following procedure to create an alert that writes to a log and sends an email when a Windows server goes down.

1. Search for "Email me when a Node goes down" in the Alert Manager.
2. Select the check box next to the alert, and then click Duplicate & Edit.
3. Enter a name for the alert, such as "Notify me when a Windows 2008 servers go down".
4. Enable the alert, and then click Trigger Condition or Next.
5. In The scope of alert, select Only following set of objects.
6. Select **Node Machine Type is equal to Windows 2008 Server** as the child condition.

You can further refine your scope by entering another AND condition. For example, you can enter **Node IP Address starts with 10.10.45** to restrict the scope of the alert to a specific subnet.

7. The actual trigger condition should be **Node Status is equal to Down**.

Select and enter a value for **Condition must exist for more than** to prevent being alerted when a node enters the down state frequently within a set amount of time. This prevents you from receiving alerts until the node has been in the down state for longer than the time you have selected.

You can further suppress alerts by enabling complex conditions in the Advanced options. This allows you to choose to wait until multiple nodes are down before triggering a single alert.

8. Click **Reset Condition**. The default action should be to reset the alert when the node is up.

9. Click **Trigger Actions**, and then click **Add Action**.

10. Select **Log the Alert to a file**, and then click **Configure Action**.

    a. Enter the location of the log. For example, enter **C:\ExampleAlertLog.txt** in the **Alert Log Filename** Field.

    b. In the **Message** text box, type **Node ${N=SwisEntity;M=Caption} is currently down.**

    c. Click **Add Action**.

11. Click **Add Escalation Level**, and enter 5 minutes to wait for 5 minutes before escalating to the next level.
12. Click Add Action in Escalation Level 2, and select Send an Email/Page. Click Configure Action.
   a. Enter your email as the recipient.
   b. Add a message.  
   ![Note](image)
   You can use variables to customize your message. You can also use a variable that allows you to acknowledge an alert from email \(\$(N=Alerting;M= AcknowledgeUrl)\).
   c. Enter your SMTP server information if you have not already done so. 
   ![Note](image)
   You can enter a default SMTP server that is used for all your email in the Configure Default Send Email Action setting. 
   d. Go to Execution settings to click Add Action.

13. Click Copy Actions to Reset Actions Tab, and then click Next.

14. Click Edit next to your logging action, and modify your message to Node \(\$(N=SwisEntity;M=Caption}\) is back up.

15. Click Edit next to your email action, and modify your message. You can also delete the email if you do not want to know if the situation has been resolved.

16. Click Summary to see if any object will trigger the alert, and then click Submit.

Once you have created the alert, it is added to the list of available alerts in the Alert Manager. You can test and view the results of each of your alert actions. See Testing Alerts for more information.

**Take a snapshot of a virtual machine**

If a virtual machine is experiencing issues, you can have an alert trigger a snapshot of the virtual machine to be taken. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Take Snapshot, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine of which you want to take a snapshot.
   a. To take a snapshot of the virtual machine that triggered the alert, click Execute this action.
      
      ![This option is only available if the alert is built to trigger for virtual machines.](image)
   b. To take a snapshot a different virtual machine, click Select specific VM, and search for a virtual machine.

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   ![This is often used to prevent an action from occurring during specific windows.](image)

5. Select how frequently this action occurs for each triggered alert in Execution Settings.

6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, a snapshot is taken of the specified virtual machine.

### 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.
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.

Important: As of Orion Platform version 2015.1, alerts are no longer created with the desktop-based, Advanced Alerts Manager or Basic Alerts Manager. Alerts are instead created and managed in the SolarWinds Orion Web Console. See Use alerts to monitor your environment for more information.

**Remove alerts from the Active Alerts list**

When an alert has triggered and becomes active, you can then acknowledge it. After an alert is acknowledged, alert actions in higher escalation levels are halted and the time it was acknowledged and the account that acknowledged it is recorded. You can also add notes that other users can read.

Depending on your organization, acknowledging an alert can have different purposes outside of halting further notifications. The most common purposes are to provide an audit trail or to prevent multiple people from working on the same issue.

ℹ️ You must enable the Allow Account to Clear Events privilege to acknowledge alerts. For more information about access privileges for Orion Web Console users, see Define what users can access and do.

1. Click Alerts & Activity > Alerts in the menu bar.
2. Click Acknowledge next to the alerts you want to acknowledge.

Tip: Depending on how you configure the email, you can acknowledge an alert directly from an email notification.

You can hide acknowledged alerts by clicking More, and then selecting Hide Acknowledged Alerts.

**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.

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 NPM recognizes an alert condition, NPM 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.
Alerts for SolarWinds NCM actions

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, NPM 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.

Important: As of Orion Platform version 2015.1, alerts are no longer created with the desktop-based, Advanced Alerts Manager or Basic Alerts Manager. Alerts are instead created and managed in the SolarWinds Orion Web Console. See Use alerts to monitor your environment for more information.

Viewing Alerts from Mobile Devices

NPM 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.
Syslog alert variables

The following variables can be used in syslog alert messages. Each variable must begin with a dollar sign and be enclosed in curly braces as, for example, `${VariableName}`. Syslog alerts also support the use of Node alert variables.

For more information on the use of variables, see Orion Variables and Examples.

Syslog date/time variables

<table>
<thead>
<tr>
<th>SYSLOG DATE/TIME VARIABLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${AbbreviatedDOW}</code></td>
<td>Current day of the week. Three character abbreviation.</td>
</tr>
<tr>
<td><code>${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, 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 &quot;Short Date&quot; and &quot;Short Time&quot; 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, 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>
<tr>
<td><code>${LongDate}</code></td>
<td>Current date. (Long Date format)</td>
</tr>
<tr>
<td><code>${LocalMonthName}</code></td>
<td>Current month name in the local language.</td>
</tr>
<tr>
<td><code>${LongTime}</code></td>
<td>Current Time. (Long Time format)</td>
</tr>
</tbody>
</table>
### Alerts for SolarWinds NCM actions

<table>
<thead>
<tr>
<th>Syslog Date/Time Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>${Application}</td>
<td>SolarWinds application information</td>
</tr>
<tr>
<td>${Copyright}</td>
<td>Copyright information</td>
</tr>
<tr>
<td>${DNS}</td>
<td>Fully qualified node name</td>
</tr>
<tr>
<td>${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>
</tbody>
</table>
### Other Syslog Variables

<table>
<thead>
<tr>
<th>SYSLOG VARIABLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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>
Reports

The Orion platform database accumulates much information that can be presented in a variety of formats.

Click Reports > All Reports to access all reports.

Predefined NCM reports

The following reports are predefined and included with SolarWinds Network Configuration Manager.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCM Audit</td>
<td>Displays results of audit checks of performance, activity, configuration transfers, real-time change notifications, and vulnerability state changes</td>
</tr>
<tr>
<td>Brocade Inventory</td>
<td>Displays information about the physical entities and agent config modules running on the chassis of Brocade devices</td>
</tr>
<tr>
<td>Cisco Inventory</td>
<td>Displays information about the physical properties of the system</td>
</tr>
<tr>
<td>F5 Inventory</td>
<td>Display information about the physical entities of the discovered F5 systems and LTM and GTM object activity details</td>
</tr>
<tr>
<td>NCM Inventory</td>
<td>Displays Information about physical entities and network services configured on NCM discovered devices.</td>
</tr>
<tr>
<td>Node Details</td>
<td>Displays details such as status, availability, response times, events, and alerts for each node under NCM management</td>
</tr>
<tr>
<td>Polling Status</td>
<td>Displays information about polling and rediscovery cycles</td>
</tr>
<tr>
<td>Route Tables Inventory</td>
<td>Displays routing tables for relevant devices</td>
</tr>
<tr>
<td>Security</td>
<td>Displays information about logins, vulnerabilities, and security settings such as the SNMP community strings used by devices</td>
</tr>
</tbody>
</table>
Reports

<table>
<thead>
<tr>
<th>Windows Server Inventory</th>
<th>Displays information about the software and services installed on Windows nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>STIG compliance</td>
<td>Displays results from a compliance check with DISA STIG</td>
</tr>
</tbody>
</table>

**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.

**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.

**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.
Reports

F5 Inventory

GTM Object Activity
Displays details about Global Traffic Manager object activity that indicates usage rates for the relevant devices.

Capacity Planning
Displays capacity details such as CPU usage, memory, and throughput relevant to the F5 devices in your network.

F5 Device Inventory
Displays information about the physical entities, software, and state of each F5 device discovered by NCM in your network.

LTM Node Inventory
Displays status and configuration information about the Local Traffic Manager node.

LTM Object Activity
Displays activity details that indicate usage rates for Local Traffic Manager objects in your NCM-managed network.

NCM 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.

Node Details Report

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.
Reports

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.

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.
Route Tables Inventory

Route Tables
Displays route tables for relevant devices.

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.
Reports

Vulnerabilities for Each Node - Remediation Planned
Lists remediation planned vulnerabilities for each device.

Vulnerabilities for Each Node - Waiver
Lists waiver vulnerabilities for each device.

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.

Predefined Orion reports

The following reports are predefined and included with the Orion platform.

Current Node Status
The following node status reports are provided by default with Orion.

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 by default. This report 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**

The following node availability reports are provided by default with Orion.

**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.

**Availability - Yesterday**

Displays the IP address and average daily availability of all monitored nodes over the previous day.

**Events**

The following network events reports are provided by default with Orion.
Reports

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.
Historical CPU and Memory Reports

Orion provides a CPU Load - Last Month report by default. This report displays the vendor icon and average and peak CPU load percentages for all monitored nodes with CPUs over the previous calendar month.

Historical Response Time Reports

The following response time reports are provided by default with Orion.

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

Orion provides the following VMware ESX Server performance reports by default with Orion.

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 7 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 7 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.
Reports

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 7 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 by default. For all monitored volumes, this report 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. Volumes are listed beneath their respective parent nodes.

Groups: Current Groups and Groups Members Status
The following group and group members status reports are provided by default with Orion.

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
The following group availability reports are provided by default with Orion.
Groups: Group Availability (with members)

**Group Availability – Last Month**
- Group Availability – Last Month

**Group Availability – This Month**
- Group Availability – This Month

**Group Availability – This Year**
- Group Availability – This Year

**Groups: Group Availability (with members)**
The following group availability reports that include member availability are provided by default with Orion.

**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

**Groups: Historical Groups Status**
The following historical group status reports are provided by default with Orion.

**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

**Inventory**
The following network inventory reports are provided by default with Orion.
Reports

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.

Create a new web-based report

Web-based reports are created in the Orion Web Console, and can be restricted to specific users through report limitations. Users may be assigned specific report limitation categories and can only view reports that are in the same report limitation category.

SolarWinds recommends that you duplicate and edit an existing web-based report instead of creating a new one.

1. Click Reports > All Reports > Manage Reports > Create New Report.
2. On the Layout Builder panel, click Add Content. You may be prompted to add content as soon as you click Create New Report.
3. Select the first resource to add to the report and click Select and Continue. Some resources require you to choose a specific object to report on. For example, if you want to track how many people use a specific application, you must choose the application when adding the resource. The Layout Builder view is displayed with the selected resource added.

4. In the Content area, click Add Content and continue to add resources to the report. You can also modify the layout.
   a. Click Add content to add resources to your report. For more information, see Add content to a web-based report.
b. Click Add section to add more rows of content to this report.

5. To filter a resource to include a specific set of data, click Edit Resource. Not all resources can be filtered.
6. Filter the resource and click Submit.
   Each resource has different filter options.

```
Edit Resource: Availability of Each Node
Title:
Availability of Each Node
Subtitle:
Time Period:
Select a Time Period: Today ▼
- or -
Beginning Date/Time: 
Ending Date/Time: 
Filter Nodes (SQL)
Device_Owner Like 'New'
Filters are optional and can be used to limit the list of Nodes displayed.
This is an advanced feature. We recommend you have a basic understanding of SQL Queries
» Show Filter Examples
```

7. After adding and filtering the resource, enter a report name, and click Next.
8. On the Preview panel, click Next.
9. Add report properties, such as categories, custom properties, or limitations, and click Next.
10. To schedule the report, click Schedule this report to run regularly, create a new schedule or assign a schedule, and click Next.
    You can schedule a report to be generated, emailed, saved, or printed.
11. Review the Summary and click Submit to save the report.

Run a config change report once

1. Click My Dashboards > Configs > Jobs.
2. Click Create New Job.
3. Name the job, and elect Generate a Config Change Report from Job Type.
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 this job relates to a business rule, and click Next.
7. Select the nodes to target with this job, and click Next.
8. Select an email notification option, and click Next. If you click Email Results, the default Email Notification Settings and SMTP Server Settings and SMTP Server Settings are populated. These settings can be overridden in each job.
9. Select the type of config change report to generate, and click Next.
10. Select Only Send Devices That Had Changes if desired, and click Next.
11. Review the settings for the job, and click Finish.

To create a config change report to run recurrently, see Schedule a recurring config change report.

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, SolarWinds NCM uses the connection profile associated with the device.

**Schedule a recurring config change report**

1. Click My Dashboards > Confis > Jobs.
2. Click Create New Job.
3. Name the job, and select Generate a Config Change Report from Job Type.
4. Select the Schedule Type. If you are creating an Advanced schedule, use the five fields to create an appropriate cron expression.
5. Add a comment if this job relates to a business rule, and click Next.
6. Select the nodes to target with this job, and click Next.
7. Select an email notification option, and click Next. If you click Email Results, the default Email Notification Settings and SMTP Server Settings and SMTP Server Settings are populated. These settings can be overridden in each job.
8. Select the type of config change report to generate, and click Next.
9. Review the settings for the job, and click Finish.
Schedule a report to run automatically while creating or editing a report

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 login credentials set, NCM uses the connection profile associated with the device. For details on managing a connection profile, see Define and apply global device logins.

Schedule a report to run automatically while creating or editing a report

You can directly assign a report to a schedule while editing the report.

1. Navigate to the Schedule Report page.
2. Click Schedule this report to run regularly, and select Create new schedule.
3. Click Add Frequency, and then select when you want to run the report.

   Click Add Time to select additional dates and times.

   - To delay when the report runs, select Specific Date in the Starting On field, and then select the date and time when you want the schedule to start.
   - To stop the report from running automatically, select Ending On, and then select the date and time when you want the schedule to end.

4. Click Add Frequency.
5. Click Add Action, and select the action (Email, Print, or Save to Disk) to be executed on the configured schedule.
6. Click Configure Action.

   - For email actions, enter the recipients, the message, and the SMTP server. Select Include Report's URL to allow recipients to access the report remotely.
   - For print actions, enter the Windows credentials necessary to access your printer, the printer, and print settings.
   - For save actions, enter the location you want to save the report to, the credentials in domain\username format, and the file type you want to save the report as. The location must be accessible from the Orion Web Console server.

7. Click Add Action.

The action is added to the Actions list. You can add multiple actions.
Create and assign report schedules in Report Manager

The Report Manager provides a list of all reports that have been set up for your SolarWinds Orion web-based reports. You can create schedules and assign reports to schedules.

Create a report schedule

1. Select a report.
2. Click on Schedule Report > Create New Schedule to display the Properties view.
3. Add additional reports to this schedule by clicking Assign another Report.
4. Include a snapshot of the selected website by clicking Assign Webpage, and enter the URL in the field displayed. You can assign multiple webpages.

   - Start each URL with http:// or https://.

5. Specify a user account so that its limitations are applied to this schedule by expanding Advanced Settings. Click Another User, and enter the User name or Account ID and Password.
6. Click Next to display the Frequency view.
7. Click Add Frequency, and then select when you want to run the report.

   - Click Add Time to select additional dates and times.

   - To delay when the report runs, select Specific Date in the Starting On field, and then select the date and time when you want the schedule to start.
   - To stop the report from running automatically, select Ending On, and then select the date and time when you want the schedule to end.
8. Click Add Frequency, and then click Next to display the Actions view.
9. Click Add Action, and select the action (Email, Print, or Save to Disk) to be executed on the configured schedule.
10. Click Configure Action.
   - For email actions, enter the recipients, the message, and the SMTP server. Select Include Report's URL to allow recipients to access the report remotely.
   - For print actions, enter the Windows credentials necessary to access your printer, the printer, and print settings.
   - For save actions, enter the location you want to save the report to, the credentials in `domain\username` format, and the file type you want to save the report as. The location must be accessible from the Orion Web Console server.

11. Click Add Action.
12. Click Next to display the Summary view.
13. If the schedule summary is correct, click Create Schedule.

The schedule is displayed in the Schedule Manager.

**Assign a report to a schedule or multiple schedules**

1. Select one or more reports.
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).

**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.
Reports

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.

Add content to a web-based report

You can include any Orion Web Console resource, including charts and graphs, in a report.

The following procedure assumes you are already creating or editing a report in the Orion Web Console.

- Resources can be dragged between columns and sections.

1. On the Layout Builder page, click Add Content in the column to which you want to add a new resource.
2. Use the Group by field to filter the available resources or search for a specific resource.
   - The Classic category grouping provides the most comprehensive list of available resources.
3. Select the resource from the list in the main pane.
   - If you are an advanced user and want to add a Custom Chart or Table, see Add a custom chart or table to a web-based report.
4. Click Select and Continue.
5. If the resource requires you to select specific objects:
   a. Select the required object(s) from the left pane.
   b. Click Add to Layout.
6. You can edit the resource if you want to change the title or subtitle.
7. If you want to add another row to your report, click Add section. You can now add content to this row as described above.
Add a custom chart or table to a web-based report

You can create custom charts or tables for inclusion in web-based reports. Custom charts or tables are usually added when you are familiar with your SolarWinds Orion database or are comfortable creating SQL or SWQL queries. Because the Orion Platform generates so much 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.

You can reuse customized charts or tables by clicking Use previously specified objects when adding the chart or table and then selecting the object.

1. Click Add Content in the column to which you want to add a custom chart.
2. Group by Reports to find the Custom Chart or Custom Table resources.
3. Select Custom Chart or Custom Table, and click Select and Continue.
4. Use one of the following methods to configure the objects displayed in the chart or table:
   - Specific Objects (static selection) - use when you know which objects you want to include in your chart or table.
     a. Filter or search for the objects you want to include.
     b. Select the objects' check boxes.
   - Dynamic Query Builder - use to select objects based on object properties.
     a. Select Basic Selector to create simply and/or queries or select Advanced Selector to create complex queries.
     b. Choose the object type you want to include.
     c. Enter your conditions.

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 use if you are comfortable querying your SolarWinds database directly using SQL or SWQL.
   a. Select SQL or SWQL, and enter your query.
   b. Click Preview Results to test your query.

5. Enter a name for this selection in the Selection Name field, and click Add to Layout.

You must now edit the chart or table to choose the data series or columns you want to use and modify display and filtering settings.

**Add a data series and customize a chart**

Once you have specified the objects for your custom chart, you need to select the data series. You can also change the sample interval and filter the results.

1. If you have just added a custom chart, the Edit Resource page opens. You can open this page by clicking Edit Chart on the resource in the Layout Builder page.
2. Click Add Data Series in Left Y-axis.
3. Filter or search for the data series, and select the one you want to use.

   The groups available and the data series within these groups will depend on the object selected.

4. Click Add Data Series. The data series is added to the Left Y-axis.
5. 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.
6. Enter a Custom label for the Left axis.
7. Select the Units displayed, Chart type, and select the Show the sum of all data series, if required.
8. Select the Sample Interval. This can be as frequent as once a minute to once a week. Data within each sample interval are summarized so that a single point or bar is plotted for each of these periods.

   It is possible to select a sample interval that is longer than the reporting period.
9. Choose how you want to filter your report.
   a. Select how you want to sort this selection of records from the Sort records by drop-down. The choices depend on the data series selected.
   b. Select either Ascending or Descending from the Sort order drop-down.
   c. Select the Data aggregation method required to summarize your data by time period.
   d. Click Advanced if you want to sort records using a secondary field.

10. 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.

    You cannot use a separate time period or filter results settings for the right axis series.

11. Click Submit to return to the Add Report page.

Add a data series and customize a table

Once you have specified the objects to be reported on for a custom table, you need to select the data series. You can also sort and filter the results.

1. If you have just added a custom table, the Edit Resource page opens. You can open this page by clicking Edit Table on the resource in the Layout Builder page.
2. Click Add Column.
3. Filter or search for the column, and select the column you want to use.

   The columns and options available depend on the object selected.

4. Click Add Column.
5. For additional settings for a column, click Advanced. Here you can:
   - Edit the Display name for this column.
   - Select 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.
   - Select 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.
Select the Data aggregation method to use for this column, to summarize your data by time period.

Select the Alignment for this data. This can be left, right or center.

6. Click on the plus sign in the table layout section to add more columns.

7. Filter the number of records shown in the table by either a specific number or a percentage.

8. Restrict data in your table to a specific time period by selecting Yes from the Time-based settings drop-down.

   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.

9. Use the Group results by option to organize the table by the values in the columns you select.

10. Click Submit to return to the Add Report page.

**Build conditions**

Use the Dynamic Query Builder selection when objects may change over time. For example, as your network ages, you will replace or upgrade various pieces of equipment. You can select each piece of equipment individually, or you can create a dynamic query that adds objects to the custom chart or table based on the properties you select.

   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.

1. Select the type of selector query you want to use (Basic or Advanced).

2. Select the type of objects to report on from the I want to report on drop-down.
3. Use the following steps if you choose Basic Selector:
   a. Click Add Condition.
   b. Select All child conditions must be satisfied (AND) or At least one child condition must be satisfied (OR).
   c. Select a property of the monitored object, a conditional relation, and provide a value.
   d. Click Add Simple Condition if you want to add another condition.

4. Use the following steps if you choose Advanced Selector:
   a. Select All child conditions must be satisfied (AND) or At least one child condition must be satisfied (OR).
   b. Select which field you want to evaluate, a conditional relation, and provide a value.
   c. 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
Servers for file transfers and email notifications

Use the following topics to configure servers for file transfers and email notifications regarding real time config detection.

Use the SolarWinds TFTP server

SolarWinds NCM uses TFTP for file transfers.

- 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. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
4. Enter the TFTP Server settings, and click Validate.
5. Click Submit.

Use the SFTP & SCP server

The SFTP & SCP Server runs as a service, but some basic configuration may be necessary to ensure it behaves in a way that works best in your environment.

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 type the TCP Port.
7. If you want to specify the IP address configuration, select Use Custom IP Address Binding, and select the IP address you want to use.
Servers for file transfers and email notifications

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 click Apply Changes.
   d. If you want to remove a user, select the user, and click Remove.
9. Click the Startup & System Tray tab, and select the desired options.
10. Click OK.

Use a third-party SCP server

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
4. Select Use Third-Party SCP Server.
5. 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.
6. Enter a valid user name and password.
7. Specify a config transfer directory, and click Validate to verify that the SCP Root Directory is set to be the same as the third-party server.
8. Click Submit.

The user must have receive and transmit permissions configured in the third-party SCP server.

Configure email notifications

SMTP server credentials used to send notifications for config change approvals, real time change detection, and running jobs

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
3. Under Manage Notifications, click SMTP Server.
4. Enter the fully qualified domain name (FQDN) of the server in Email Server Address.
5. Enter the Port Number on which the server handles messages.
6. Select an Authentication type.
7. If you selected Password as your Authentication type, enter a user name and password that the server accepts.
8. Click Submit.

**Email notification defaults used in new scheduled jobs**

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.
3. Under Manage Notifications, click Email Notification.
4. Enter in Sender Name the name you want to appear in a job completion notification.
5. Enter a Reply Address if desired.
6. Enter the Subject to be used to send a job completion notification.
7. Enter recipients in the To field.
8. Click Submit.
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.

The basics of config change templates

A change config template enables you to accomplish a specific device configuration task for a set of NCM-managed nodes. Template describes the run-time 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

Config Change Templates

Click My Dashboards > Configs > Config Change Templates.

Config Change Templates

Create, edit, import, export, tag, and delete config change templates.
Config change templates

**Shared Config Change Templates on thwack**

View and download config change templates from thwack.

**Preparation and use of a template**

Every change config template executes changes based on NCM device inventory objects. Those objects are the database entities that the SolarWinds Information System accesses in managing the communication of NCM 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 SolarWinds [SolarWinds Information Service 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.

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.

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

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.
Config change templates

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.

/*
.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
.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) to remove. Selecting VLANs
irrelevant to interfaces results 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.

```plaintext
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
```

273
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.

```bash
NCM Node bgp-2651-03configure terminalinterface
FastEthernet0/0no switchport access vlan 1004
switchport access vlan 1002
exitend

NCM Node cur-3725Configure terminalinterface
FastEthernet0/1no switchport access vlan 1004
switchport access vlan
1002exitend
```

Set up the 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 vertical bar character (|) divides the items in the list.
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.
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:

```plaintext
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**

```plaintext
script ConfigureVLANmembershipCiscoIOS ( NCM.Nodes @ContextNode, NCM.Interfaces[] @TargetPorts, NCM.VLANs[] @VlansToRemove, NCM.VLANs[] @VlanToAssign )
{
```

```plaintext
277
```
Config change templates

```plaintext
CLI {
    vlan database vlan @vlanid@description @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 (@ItemVariable 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**

```
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

Click Select Interfaces List to load a tree that displays available interfaces and NCM nodes previously selected in the wizard.

**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
}
```

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 the following operators to specify a parenthetical condition. Use single quotes around string values.

<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>

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).

```python
foreach @portItem in @TargetPorts
{
    if (@PortItem.InterfaceDescription != 'Loop0')
    {
        CLI
        {
            interface @portItem.InterfaceDescription
        }
    }
}```
Config change templates

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>
</table>
| Substring | Specify a starting point within a string and the length from the starting point that you want to capture for manipulation. | string Substring (string str, int startIndex, int length) | - 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 |
| StrLength | Return the length of a string. | In StrLength (string str) | - str is the user-input string whose length is used as the integer value |
| IndexOf | Find the number of characters in a string. | int IndexOf (string str, string search) | - str is a string to search on |
### Function Description

<table>
<thead>
<tr>
<th>FUNCTION</th>
<th>DESCRIPTION</th>
<th>DECLARATION</th>
<th>VARIABLE DEFINITIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SetOctet</td>
<td>Replace an octet within an IP address.</td>
<td>string SetOctet (string ipAddr, int octetPosition, string octet)</td>
<td>- search is a user-input string NCM uses to find the numerical value of the string being searched</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>- ipAddress is the IP address - octetPosition marks the position where the target octet begins - octet is the new value of the target octet</td>
</tr>
</tbody>
</table>

#### Example 1: Manipulating a String

```plaintext
script IPshuffle(string @str, string @search )
{
    int @length = strlength(@str)
    int @startIndex = indexOf(@str,@search)
}
```
The user enters $\text{ABCDEF}$ for the $\@str$ variable and $\text{CD}$ for the $\@search$ variable in the template's wizard. Based on those values, the script does the following:

1. Uses $\text{ABCDEF}$ in the $\text{strlen}$ function to give a value of 6 to a variable called $\@length$.
2. Uses $\text{CD}$ as the substring of $\text{ABCDEF}$ 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 $\text{ABCDEF}$ and calculates a result ($\@res$) using $\@startIndex$ to count in two positions and $\@substringLength$ to count four positions from the start index.
5. Outputs $\text{CDEF}$ 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 $\text{10.10.@id.10}$, where the value of $\@id$ is determined by user input.

The user enters $\text{10.10.10.10}$ 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.
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 10.10.22.10 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
Config change templates

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:

```plaintext
script OpenACLs(NCM.Nodes @ContextNode, string[] @IpRouters)
{
    foreach (@ipRouter in @ipRouters)
    {
        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:
Enable NetFlow on CiscoASA example

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.

```plaintext
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 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 (for example: SolarWinds NetFlow Traffic Analyzer).

.PARAMETER_LABEL @NetFlowExportPort
 NetFlow Export Port
.PARAMETER_DESCRIPTION @NetFlowExportPort
 Enter the NetFlow export port. The default for SolarWinds NTA is 2055.
*/

script EnableNetflowOnCiscoASA (  
    NCM.Nodes @ContextNode,  
    string @NetFlowCollectorIPAddress,  
    int @NetFlowExportPort  
)  
{
    // Enter configuration mode and generate NetFlow commands
    CLI
}
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.

```plaintext
{  
    configure terminal
    flow-export destination inside @NetFlowCollectorIPAddress
    @NetFlowExportPort
    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**

**@NetFlowCollectorIPAddress**
NetFlow Collector IP Address

Enter the IP address of the server running the NetFlow traffic analysis solution (e.g. SolarWinds NetFlow Traffic Analyzer--NTA).

**@NetFlowExportPort**
NetFlow Export Port

Enter the NetFlow export port (default for SolarWinds NTA is 2055).
Config change templates

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 Service 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

The previous line of code generates the following output:

flow-export destination inside 10.10.18.157 2055

Execute a config change template

1. Click My Dashboards > Configs > Config Change Templates.
2. Select a template in list.
3. Click Define Variables & Run.
4. Select the target nodes.
5. Click Next.
6. 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.
7. Click Next.
8. If you want to see the CLI commands for a device, click Show Commands in New Window.
9. Click Execute.

Create a config change template

1. Click My Dashboards > Configs > Config Change Templates.
2. Click Create New Config Change Template.
3. Name the template, enter a description, and add tags.
4. Create your Config Change Template.
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, SolarWinds NCM validates the syntax of the template. If validation succeeds, SolarWinds NCM saves a copy of the template and loads the relevant interface for user input.
   
   If validation fails, SolarWinds NCM displays an error that guides you to make changes.

**Import a config change template**

1. Click My Dashboards > Configs > Config Change Templates.
2. Click Import.
3. Click Choose File to find the file on your computer. Config change template files have a .ncm-template file extension.
4. Click Submit.
5. Change the name, edit the description, and add tags, if necessary.
6. Modify the logic of your Config Change Template.
7. Click Validate to check syntax.
8. Click Submit.

**Tag a config change template**

1. Click My Dashboards > Configs > Config Change Templates.
2. Select a template in the list.
3. Click Tags.
4. Edit tags: Add Existing, Add New, or Remove.
5. Click Submit.

**Edit a config change template**

1. Click My Dashboards > Configs > Config Change Templates.
2. Select a template in the list.
3. Click Advanced Modify.
4. Change the name, edit the description, and add tags, if necessary.
5. Modify the logic of your Config Change Template.
6. Click Validate to check syntax.
7. Click Submit.

Export a config change template to thwack

1. Click My Dashboards > Configs > Config Change Templates.
2. Select a template in the list.
3. Click Export to thwack.
4. If prompted, enter your user name and password, and click Log In.

Export a config change template as a file

1. Click My Dashboards > 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. Click Return to Config Change Templates.

Delete a config change template

1. Click My Dashboards > Configs > Config Change Templates.
2. Select a template in the list.
3. Click Delete.

SolarWinds Information Service 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>
<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. Possible Values: Other (1) Invalid (2) Dynamic (3) Static (4)</td>
</tr>
</tbody>
</table>
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 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>
### Config change templates

<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>DATATYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>PortStatus</td>
<td>System.String</td>
<td>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)</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 bridge port 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.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), 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), atmads1l1(74), atmads1l2(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), atmshdsl1(90), atmshdsl2(91), atmshdsl4(92), atm25m(93), atm3e(94), atm3t(95), xdsl-fec(96), xdsl-adsl(97), xdsl-gshdsl(98), xdsl-bri(99), xdsl-scc(100), ge1(101), pos155m(102), cpos(103),
<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>DATATYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| 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-1vitfxs(126), sic-1vitfxyo(127), sic-2vitfxs(128), sic-2vitfxyo(129), xdsl-titfxs-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), atm1shdsl4wire(151), atm1ima4shdsl(152), ls4(153), ls8(154), ls16(155), sic-adls2plus-isdn(156), sic-adls2plus-pots(157), ft3(158), ce32(159), bsv2(160), bsv4(161), rpu(162), erpu(163), ssl(164), nsa(165), wsx6ksup12ge(200), wsx6408gbic(201), wsx6224mmmt(202), wsx6248rj45(203), wsx6248tel(204), wsx6302smm(206), wsx6kmsfc(207), wsx6024fmlmt(208), wsx6101oc12mmf(209), wsx6101oc12smf(210), wsx6416gemt(211), wsx61822pa(212), osm2oc12AtmMM(213), osm2oc12AtmSI(214), osm4oc12PosMM(216), osm4oc12PosSI(217), osm4oc12PosSL(218), wsx6ksup1a2ge(219), fe18-75(220), fe18-120(221), ft18(222), cf-card(223), bsv2-v2(224), e1vi1-v2(225), e1vi2(226), t1vi1-v2(227), t1vi2(228), osm(229), sd707(230), dm-epri(231), dm-tpri(232), erpu-h(233), wsx6kmsfc2(234), wsx6324mmt(235), wsx6348rj45(236), wsx6ksup22ge(237), wsx6324sm(238), wsx6516gbic(239),
<table>
<thead>
<tr>
<th>PROPERTY_NAME</th>
<th>DATATYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>wx44122Gbtx(321).</td>
<td>wsx2980(322).</td>
</tr>
<tr>
<td></td>
<td>wsx2980grj(323).</td>
<td>wsx4019(325).</td>
</tr>
<tr>
<td></td>
<td>wsx4148rj45v(326).</td>
<td>wxs4424grj45(330).</td>
</tr>
<tr>
<td></td>
<td>wsx4148fxmt(331).</td>
<td>wxs4448gblx(332).</td>
</tr>
<tr>
<td></td>
<td>wxs4448grj45(334).</td>
<td>wxs4148xmt(337).</td>
</tr>
<tr>
<td></td>
<td>wxs4428rj21v(341).</td>
<td>wxs4302gb(342).</td>
</tr>
<tr>
<td></td>
<td>wxs4248rj45v(343).</td>
<td>wxs2948ggetx(345).</td>
</tr>
<tr>
<td></td>
<td>wxs2948ggetxgrj(346).</td>
<td>wxs6516agbic(502).</td>
</tr>
<tr>
<td></td>
<td>wxs6148getx(503).</td>
<td>wxs6148x2rj45(506).</td>
</tr>
<tr>
<td></td>
<td>wxs6196rj21(507).</td>
<td>wssup32ge3b(509).</td>
</tr>
<tr>
<td></td>
<td>wssup3210ge3b(510).</td>
<td>mec6524gs8s(511).</td>
</tr>
<tr>
<td></td>
<td>mec6524gt8s(512).</td>
<td>me6524mfsc2a(598).</td>
</tr>
<tr>
<td></td>
<td>osm12ct3t1(600).</td>
<td>osm12t3e3(601).</td>
</tr>
<tr>
<td></td>
<td>osm24t3e3(602).</td>
<td>osm4gewanbicplus(603).</td>
</tr>
<tr>
<td></td>
<td>osm1choc12t3s1(604).</td>
<td>osm2hoch12t3s1(605).</td>
</tr>
<tr>
<td></td>
<td>osm20c12atmmpplus(606).</td>
<td>osm20c12atmsiplus(607).</td>
</tr>
<tr>
<td></td>
<td>osm20c12posmplplus(608).</td>
<td>osm20c12posiplus(609).</td>
</tr>
<tr>
<td></td>
<td>osm16oc3posiplus(610).</td>
<td>osm1oc48possslplus(611).</td>
</tr>
<tr>
<td></td>
<td>osm1oc48posiplus(612).</td>
<td>osm1oc48possslplus(613).</td>
</tr>
<tr>
<td></td>
<td>osm4oc3posiplus(614).</td>
<td>osm8oc3possiplus(615).</td>
</tr>
<tr>
<td></td>
<td>osm8oc3possiplus(616).</td>
<td>osm4oc12posiplus(617).</td>
</tr>
<tr>
<td></td>
<td>wsvecsclpsec1(903).</td>
<td>wsvecsg1(911).</td>
</tr>
<tr>
<td></td>
<td>wsx6148rj45v(912).</td>
<td>wxs6148rj21v(913).</td>
</tr>
<tr>
<td></td>
<td>wssvcnam1(914).</td>
<td>wxs6548getx(915).</td>
</tr>
<tr>
<td></td>
<td>wsx6066sbkmk(920).</td>
<td>wssvcgetx(921).</td>
</tr>
<tr>
<td></td>
<td>wssvcgetx(921).</td>
<td>wsx6148arj45(923).</td>
</tr>
<tr>
<td></td>
<td>wsxvecsclpsec1(924).</td>
<td>wsx6148feftp(928).</td>
</tr>
<tr>
<td></td>
<td>wsxvecnam1(929).</td>
<td>wsxvecsclpsec1(930).</td>
</tr>
<tr>
<td></td>
<td>ace10650k9(926).</td>
<td>wsxvecnam1(930).</td>
</tr>
<tr>
<td></td>
<td>wsxvecsclpsec1(936).</td>
<td>wssup720(1001).</td>
</tr>
<tr>
<td></td>
<td>wssup720base(1002).</td>
<td>m7600sip600(1004).</td>
</tr>
<tr>
<td></td>
<td>wssup720base(1004).</td>
<td>wxs6748getx(1007).</td>
</tr>
<tr>
<td></td>
<td>wxs670410g(1008).</td>
<td>301</td>
</tr>
</tbody>
</table>
## 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>
<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>
</tbody>
</table>
### NCM.CatalystCards entity relationships

<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>DATATYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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.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>
</tbody>
</table>
## Config change templates

<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>DATATYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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>ccardIndex 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>OperStatus</td>
<td>System.String</td>
<td>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.</td>
</tr>
</tbody>
</table>

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)
**PROPERTY NAME** | **DATATYPE** | **DESCRIPTION**
--- | --- | ---
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.)
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.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>PROPERTY NAME</td>
<td>DATATYPE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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>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>
<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>
Config change templates

**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>
<tr>
<td>chassisVersion</td>
<td>System.String</td>
<td>Chassis hardware revision level, or an empty string if unavailable.</td>
</tr>
<tr>
<td>chassisID</td>
<td>System.String</td>
<td>Unique ID string. Defaults to chassis serial number if available, otherwise empty. Can also be set with 'snmp-server chassis-id'.</td>
</tr>
<tr>
<td>chassisSerialNumberString</td>
<td>System.String</td>
<td>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.</td>
</tr>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>romSysVersion</td>
<td>System.String</td>
<td>ROM system software version or an empty string if unavailable.</td>
</tr>
<tr>
<td>processorRAM</td>
<td>System.Int32</td>
<td>Bytes of RAM available to CPU.</td>
</tr>
<tr>
<td>nvRAMSize</td>
<td>System.Int32</td>
<td>Bytes of nonvolatile configuration memory.</td>
</tr>
<tr>
<td>nvRAMUsed</td>
<td>System.Int32</td>
<td>Bytes of non-volatile configuration memory in use.</td>
</tr>
<tr>
<td>chassisSlots</td>
<td>System.Int32</td>
<td>Number of slots in this chassis, or -1 of neither applicable nor determinable.</td>
</tr>
<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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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>
</tbody>
</table>
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 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>
<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>Data Type</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>
<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>
</tbody>
</table>
### Config change templates

<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>DATATYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>
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).
## 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>
### MaxPartitions

**Property Name:** MaxPartitions  
**Datatype:** System.Int32  
**Description:** 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 example, 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.
<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<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) on-line removal and insertion; 2) interrupt generation on removal or insertion.</td>
</tr>
</tbody>
</table>
**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.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>PROPERTY NAME</td>
<td>DATATYPE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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>
<tr>
<td>FlashFileStatus</td>
<td>System.String</td>
<td>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)</td>
</tr>
</tbody>
</table>
### 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.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>
</tbody>
</table>
### NCM.CiscoImageMIB entity relationships

<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.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>PROPERTY NAME</td>
<td>DATATYPE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</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>
<tr>
<td>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<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>
</tbody>
</table>
Config change templates

<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>DATATYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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 snmpUDPDoman, 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 snmpUDPDoman.</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>
<tbody>
<tr>
<td>EntityName</td>
<td>System.String</td>
<td>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 <code>console'. This might be a text name, such as </code>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.</td>
</tr>
<tr>
<td>EntityDescription</td>
<td>System.String</td>
<td>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.</td>
</tr>
<tr>
<td>PROPERTY NAME</td>
<td>DATATYPE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EntityType</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>
<tr>
<td><strong>PROPERTY NAME</strong></td>
<td><strong>DATATYPE</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<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>
</tbody>
</table>
### 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><strong>FirmwareRevision</strong> System.String 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 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></td>
<td></td>
<td><strong>SoftwareRevision</strong> System.String The vendor-specific software 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>Property Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>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.</strong></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>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>
</tbody>
</table>
### Config change templates

<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>DATATYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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>

### 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>
</tbody>
</table>
### Config change templates

<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>DATATYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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>PortStatus</td>
<td>System.String</td>
<td>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:</td>
</tr>
</tbody>
</table>
## NCM. Interfaces

<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>DATATYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLANType</td>
<td>System.Int32</td>
<td>The type of this VLAN</td>
</tr>
<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>
## 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>
# Config change templates

<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 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.</td>
</tr>
<tr>
<td>InterfaceMTU</td>
<td>System.Int32</td>
<td>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.</td>
</tr>
<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><strong>PROPERTY NAME</strong></td>
<td><strong>DATATYPE</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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>
<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>
</tbody>
</table>
### 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.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>
</tbody>
</table>
**NCM.IpAddresses entity relationships**

<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.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>
</tbody>
</table>
### Config change templates

<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>DATATYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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>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>SysLocation</td>
<td>System.String</td>
<td>The physical location of this node (e.g., ‘telephone closet, 3rd floor’).</td>
</tr>
</tbody>
</table>
### Config change templates

<table>
<thead>
<tr>
<th><strong>PROPERTY NAME</strong></th>
<th><strong>DATATYPE</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<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>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>
</tbody>
</table>
**NCM.Nodes entity relationships**

<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>DATATYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

**NCM.Nodes 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.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>TYPE</td>
<td>ENTITY</td>
<td>JOINED DATA ENTITY</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------</td>
<td>---------------------------------------------</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>
<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>TCPEndPoint</td>
<td>System.Int32</td>
<td>The local port number for this TCP connection.</td>
</tr>
<tr>
<td>TCPEndPointName</td>
<td>System.String</td>
<td>Port description based on TCPEndPoint 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>TCPSlot</td>
<td>System.String</td>
<td>The state of this TCP connection. The only value which may be set by a management station is deleteTCB(12). Accordingly, it is appropriate for an agent to return a `badValue' response if a management station attempts to set this object to any other value.</td>
</tr>
</tbody>
</table>

---

345
If a management station sets this object to the value deleteTCB(12), then this has the effect of deleting the TCB (as defined in RFC 793) of the corresponding connection on the managed node, resulting in immediate termination of the connection.

As an implementation-specific option, a RST segment may be sent from the managed node to the other TCP endpoint (note however that RST segments are not sent reliably).

<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>DATATYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCPRemotePortName</td>
<td>System.String</td>
<td>Port description based on TCPRemotePort value</td>
</tr>
</tbody>
</table>

**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>PROPERTY NAME</td>
<td>DATATYPE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</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>
</tbody>
</table>
## 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>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:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mask network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>255.0.0.0 class-A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>255.255.0.0 class-B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>255.255.255.0 class-C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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)

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)
- ciscolorp(11)
- bbnSpflgp(12)
- ospf(13)
- bgp(14)
### Config change templates

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>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>PROPERTY NAME</td>
<td>DATATYPE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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>
<tr>
<td>Metric3</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>
</tbody>
</table>
| 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. |
### Config change templates

<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. 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>PROPERTY NAME</td>
<td>DATATYPE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
<td>-------------</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>
<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>
</tbody>
</table>
Config change templates

<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>DATATYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLANState</td>
<td>System.Int32</td>
<td>The state of this VLAN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible Values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>operational(1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>suspended(2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mtuTooBigForDevice(3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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>
EnergyWise devices

The following topics explore how you can use SolarWinds Network Configuration Manager in conjunction with SolarWinds Network Performance Monitor to enable and manage your Cisco EnergyWise devices.

**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.

**Manage and enable 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 Add nodes via Network Discovery.

1. Click Settings > All Settings.
2. Under Node & Group Management, click Manage Nodes.
3. Select the Cisco node for which you want EnergyWise enabled, and 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.

**Manage Power over Ethernet 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.

1. Click Settings > All Settings.
2. Under Node & Group Management, click Manage Nodes.
3. Expand the Cisco node containing the interface you want to configure.
4. Select the interface you want to enable EnergyWise, and click More Actions > Manage EnergyWise.
5. Click Enable EnergyWise on these nodes.
6. Specify the appropriate values on the Manage EnergyWise Interface page.
7. Click Execute Config Actions.
References

The following sections contain supplemental reference material for SolarWinds NCM.

Node and configuration 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 can be used in most custom properties. They can 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.

Node variables

The following are valid node variables.

<table>
<thead>
<tr>
<th>Node Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${N=SwisEntity;M=AgentPort}</td>
<td>Node SNMP port number</td>
</tr>
<tr>
<td>Node Variable</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>${N=SwisEntity;M=Node.Allow64BitCounters}$</td>
<td>Node allows 64-bit counters (1), or not (0)</td>
</tr>
<tr>
<td>${N=SwisEntity;M=AvgResponseTime}$</td>
<td>Average node response time, in msec, to ICMP requests</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BlockUntil}$</td>
<td>Day, date, and time until which node polling is blocked</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferBgMissThisHour}$</td>
<td>Device-dependent count of big buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.30</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferBgMissToday}$</td>
<td>Device-dependent count of big buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.30</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferHgMissThisHour}$</td>
<td>Device-dependent count of huge buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.62</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferHgMissToday}$</td>
<td>Device-dependent count of huge buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.62</td>
</tr>
<tr>
<td>Node Variable</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferLgMissThisHour}</td>
<td>Device-dependent count of large buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.38</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferLgMissToday}</td>
<td>Device-dependent count of large buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.38</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferMdMissThisHour}</td>
<td>Device-dependent count of medium buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.22</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferMdMissToday}</td>
<td>Device-dependent count of medium buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.22</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferNoMemThisHour}</td>
<td>Count of buffer errors due to low memory on node in current hour</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferNoMemToday}</td>
<td>Count of buffer errors due to low memory on node in current day</td>
</tr>
</tbody>
</table>
## References

<table>
<thead>
<tr>
<th>Node Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${N=SwisEntity;M=BufferSmMissThisHour}</td>
<td>Device-dependent count of small buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.14</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferSmMissToday}</td>
<td>Device-dependent count of small buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.14</td>
</tr>
<tr>
<td>${N=SwisEntity;M=Caption}</td>
<td>User friendly node name</td>
</tr>
<tr>
<td>${N=SwisEntity;M=Community}</td>
<td>Node community string</td>
</tr>
<tr>
<td>${N=SwisEntity;M=Contact}</td>
<td>Contact information for person or group responsible for node</td>
</tr>
<tr>
<td>${N=SwisEntity;M=CPULoad}</td>
<td>Node CPU utilization rate at last poll</td>
</tr>
<tr>
<td>${N=SwisEntity;M=CustomPollerLastStatisticsPoll}</td>
<td>Day, date, and time of last poll attempt on node</td>
</tr>
<tr>
<td>${N=SwisEntity;M=CustomPollerLastStatisticsPollSuccess}</td>
<td>Day, date, and time that node was last successfully polled</td>
</tr>
<tr>
<td>${N=SwisEntity;M=NodeDescription}</td>
<td>Node hardware and software</td>
</tr>
<tr>
<td>${N=SwisEntity;M=DNS}</td>
<td>Fully qualified node name</td>
</tr>
</tbody>
</table>

360
<table>
<thead>
<tr>
<th>Node Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${N=SwisEntity;M=DynamicIP}</td>
<td>If node supports dynamic IP address assignment via BOOTP or DHCP (1); static IP address return (0)</td>
</tr>
<tr>
<td>${N=SwisEntity;M=EngineID}</td>
<td>Internal unique identifier of the polling engine to which node is assigned</td>
</tr>
<tr>
<td>${N=SwisEntity;M=GroupStatus}</td>
<td>Filename of status icon for node and, in NPM, its interfaces</td>
</tr>
<tr>
<td>${N=SwisEntity;M=IOSImage}</td>
<td>Family name of Cisco IOS on node</td>
</tr>
<tr>
<td>${N=SwisEntity;M=IOSVersion}</td>
<td>Cisco IOS version on node</td>
</tr>
<tr>
<td>${N=SwisEntity;M=IP_Address}</td>
<td>Node IP address</td>
</tr>
<tr>
<td>${N=SwisEntity;M=IPAddressType}</td>
<td>Node IP address version (IPv4 or IPv6)</td>
</tr>
<tr>
<td>${N=SwisEntity;M=LastBoot}</td>
<td>Day, date and time of last node boot</td>
</tr>
<tr>
<td>${N=SwisEntity;M=LastSync}</td>
<td>Time and date of last node database and memory synchronization</td>
</tr>
<tr>
<td>${N=SwisEntity;M=Location}</td>
<td>Physical location of node</td>
</tr>
<tr>
<td>${N=SwisEntity;M=MachineType}</td>
<td>Node manufacturer or distributor and family or version information</td>
</tr>
<tr>
<td>Node Variable</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=MaxResponseTime}</code></td>
<td>Maximum node response time, in msec, to ICMP requests</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=MemoryUsed}</code></td>
<td>Total node memory used over polling interval</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=Stats.MinResponseTime}</code></td>
<td>Minimum node response time, in msec, to ICMP requests</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=NextPoll}</code></td>
<td>Day, date and time of next scheduled node polling</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=NextRediscovery}</code></td>
<td>Time of next node rediscovery</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=NodeID}</code></td>
<td>Internal unique identifier of node</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=PercentLoss}</code></td>
<td>ICMP packet loss percentage when node last polled</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=PercentMemoryUsed}</code></td>
<td>Percentage of total node memory used over polling interval</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=PollInterval}</code></td>
<td>Node polling interval, in seconds</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=RediscoveryInterval}</code></td>
<td>Node rediscovery interval, in minutes</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=ResponseTime}</code></td>
<td>Node response time, in milliseconds, to last ICMP request</td>
</tr>
<tr>
<td>Node Variable</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>${N=SwisEntity;M=SNMPv3Credentials.RWAuthenticationKey}</td>
<td>SNMPv3 read/write credential authentication key</td>
</tr>
<tr>
<td>${N=SwisEntity;M=SNMPv3Credentials.RWAuthenticationKeyIsPassword}</td>
<td>States if the SNMPv3 read/write credential authentication key is the password</td>
</tr>
<tr>
<td>${N=SwisEntity;M=SNMPv3Credentials.RWAuthenticationMethod}</td>
<td>SNMPv3 read/write credential authentication method</td>
</tr>
<tr>
<td>${N=SwisEntity;M=SNMPv3Credentials.RWContext}</td>
<td>SNMPv3 read/write security context information</td>
</tr>
<tr>
<td>${N=SwisEntity;M=SNMPv3Credentials.RWPrivacyKey}</td>
<td>SNMPv3 read/write credential key</td>
</tr>
<tr>
<td>${N=SwisEntity;M=SNMPv3Credentials.RWPrivacyKeyIsPassword}</td>
<td>States if the SNMPv3 read/write credential privacy key is the password</td>
</tr>
<tr>
<td>${N=SwisEntity;M=SNMPv3Credentials.RWPrivacyMethod}</td>
<td>SNMPv3 read/write credential privacy encryption method</td>
</tr>
<tr>
<td>${N=SwisEntity;M=SNMPv3Credentials.RWUsername}</td>
<td>User friendly name for SNMPv3 read/write credential</td>
</tr>
<tr>
<td>Node Variable</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>${N=SwisEntity;M=Severity}$</td>
<td>A network health score determined additively by scoring the status of monitored objects. In NPM 1 point is provided for an interface in a warning state, 1000 points for a down interface, and 1 million points for a down node. In SAM, 100 points is provided for an application in a warning state, 200 points for an application in critical state, 500 is status is unknown, and 1000 for a down application.</td>
</tr>
<tr>
<td>${N=SwisEntity;M=SNMPv3Credentials. AuthenticationKey}$</td>
<td>SNMPv3 authentication key</td>
</tr>
<tr>
<td>${N=SwisEntity;M=SNMPv3Credentials. AuthenticationKeyIsPassword}$</td>
<td>States if node SNMPv3 authentication key is password</td>
</tr>
<tr>
<td>${N=SwisEntity;M=SNMPv3Credentials. AuthenticationMethod}$</td>
<td>SNMPv3 authentication type</td>
</tr>
<tr>
<td>${N=SwisEntity;M=SNMPv3Credentials. Context}$</td>
<td>Group or domain of user with SNMPv3 access to node</td>
</tr>
<tr>
<td>${N=SwisEntity;M=SNMPv3Credentials. PrivacyKey}$</td>
<td>SNMPv3 credential key</td>
</tr>
<tr>
<td>Node Variable</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=SNMPv3Credentials. PrivacyKeyIsPassword}</code></td>
<td>States if node SNMPv3 credential key is the password</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=SNMPv3Credentials. PrivacyMethod}</code></td>
<td>SNMPv3 credential key type</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=SNMPv3Credentials. Username}</code></td>
<td>User friendly name for SNMPv3 credential</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=SNMPVersion}</code></td>
<td>States the version of SNMP used by the node</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=StatCollection}</code></td>
<td>Statistics collection frequency, in minutes</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=Status;F=Status}</code></td>
<td>Numerical node status. For more information, see Status Variables.</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=StatusDescription}</code></td>
<td>User friendly node status</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=StatusLED}</code></td>
<td>Filename of node status icon</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=SysName}</code></td>
<td>String reply to SNMP SYS_NAME OID request</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=SysObjectID}</code></td>
<td>Vendor ID of the network management subsystem in OID form. Clearly determines the type of node.</td>
</tr>
</tbody>
</table>
### Node Variable

<table>
<thead>
<tr>
<th>Node Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${N=SwisEntity;M=SystemUpTime}</code></td>
<td>Time, in hundredths of a second, either since network monitoring started (WMI) or since the monitored device rebooted (SNMP).</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=TotalMemory}</code></td>
<td>Total node memory available</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=UnManaged}</code></td>
<td>States if node is currently unmanaged</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=UnManageFrom}</code></td>
<td>Day, date, and time when node is set to “Unmanaged”</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=UnManageUntil}</code></td>
<td>Day, date, and time when node is scheduled to be managed</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=Vendor}</code></td>
<td>Node manufacturer or distributor</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=VendorIcon}</code></td>
<td>Filename of node vendor logo</td>
</tr>
</tbody>
</table>

### Status Variables

When using the `${Status}` variable with a monitored object, status values are returned, as appropriate. The following table provides a description for each status value.

<table>
<thead>
<tr>
<th>Status Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Unknown</td>
</tr>
<tr>
<td>1</td>
<td>Up</td>
</tr>
<tr>
<td><strong>STATUS VALUE</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>2</td>
<td>Down</td>
</tr>
<tr>
<td>3</td>
<td>Warning</td>
</tr>
<tr>
<td>4</td>
<td>Shutdown</td>
</tr>
<tr>
<td>5</td>
<td>Testing</td>
</tr>
<tr>
<td>6</td>
<td>Dormant</td>
</tr>
<tr>
<td>7</td>
<td>Not Present</td>
</tr>
<tr>
<td>8</td>
<td>Lower Layer Down</td>
</tr>
<tr>
<td>9</td>
<td>Unmanaged</td>
</tr>
<tr>
<td>10</td>
<td>Unplugged</td>
</tr>
<tr>
<td>11</td>
<td>External</td>
</tr>
<tr>
<td>12</td>
<td>Unreachable</td>
</tr>
<tr>
<td>14</td>
<td>Critical</td>
</tr>
<tr>
<td>15</td>
<td>Mixed Availability</td>
</tr>
<tr>
<td>16</td>
<td>Misconfigured</td>
</tr>
<tr>
<td>17</td>
<td>Could Not Poll</td>
</tr>
<tr>
<td>19</td>
<td>Unconfirmed</td>
</tr>
<tr>
<td>22</td>
<td>Active</td>
</tr>
<tr>
<td>24</td>
<td>Inactive</td>
</tr>
<tr>
<td>25</td>
<td>Expired</td>
</tr>
<tr>
<td>26</td>
<td>Monitoring Disabled</td>
</tr>
</tbody>
</table>
Important: As of Orion Platform version 2015.1, SolarWinds alerts use a new variable format. See General alert variables for more information.

**General alert variables**
The following are valid, general alert variables.

<table>
<thead>
<tr>
<th>General Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{N=Alerting;M=AlertID}</td>
<td>The ID of the alert</td>
</tr>
<tr>
<td>{N=Alerting;M=AlertName}</td>
<td>The name of the alert from the alert field Name of alert definition in Alert Properties</td>
</tr>
<tr>
<td>{N=Alerting;M=AlertDescription}</td>
<td>The description of the alert from the alert field Description of alert definition in Alert Properties</td>
</tr>
<tr>
<td>{N=Alerting;M=AlertDetailsURL}</td>
<td>The URL used to get more information about the triggered alert</td>
</tr>
<tr>
<td>{N=Alerting;M=AlertMessage}</td>
<td>The alert message from the alert field Message displayed when this alert is triggered in Trigger Actions</td>
</tr>
<tr>
<td>{N=Alerting;M=DownTime}</td>
<td>The amount of time the alert has been active</td>
</tr>
<tr>
<td>{N=Alerting;M=ObjectType}</td>
<td>The object type that the alert is monitoring</td>
</tr>
<tr>
<td>{N=Alerting;M=Severity}</td>
<td>The severity of the alert from the alert field Severity of Alert in Alert Properties</td>
</tr>
<tr>
<td>{N=Alerting;M=LastEdit}</td>
<td>The last time the alert definition has been edited</td>
</tr>
<tr>
<td>{N=Alerting;M=Acknowledged}</td>
<td>Acknowledged status</td>
</tr>
</tbody>
</table>

### Status Value

<table>
<thead>
<tr>
<th>Status Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>Disabled</td>
</tr>
<tr>
<td>28</td>
<td>Not Licensed</td>
</tr>
</tbody>
</table>
### General Variable Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${N=Alerting;M=AcknowledgedBy}</code></td>
<td>Who the alert was acknowledged by</td>
</tr>
<tr>
<td><code>${N=Alerting;M=AcknowledgedTime}</code></td>
<td>Time the alert was acknowledged</td>
</tr>
<tr>
<td><code>${N=Alerting;M=Notes}</code></td>
<td>Information from the Notes field when you acknowledge alerts through the Web Console</td>
</tr>
<tr>
<td><code>${N=Alerting;M=AlertTriggerCount}</code></td>
<td>Count of triggers</td>
</tr>
<tr>
<td><code>${N=Alerting;M=AlertTriggerTime}</code></td>
<td>Date and time of the last event for this alert. (Windows control panel defined “Short Date” and “Short Time”)</td>
</tr>
<tr>
<td><code>${N=Generic;M=Application}</code></td>
<td>SolarWinds application information</td>
</tr>
<tr>
<td><code>${N=Generic;M=Copyright}</code></td>
<td>Copyright information</td>
</tr>
<tr>
<td><code>${N=Generic;M=Release}</code></td>
<td>Release information</td>
</tr>
<tr>
<td><code>${N=Generic;M=Version}</code></td>
<td>Version of the SolarWinds software package</td>
</tr>
</tbody>
</table>

It is possible to use previous generation variables, for example `${NodeName}`. However, when using the variable picker, the new format is displayed by default. Previous generation variables can only be entered manually.

> Some variables are no longer valid. See [Defunct Alert Variables](#).

### 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>
</tbody>
</table>
## References

<table>
<thead>
<tr>
<th>PROPERTY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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>
<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>PROPERTY</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</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>
<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>

**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.

**Characters**

<table>
<thead>
<tr>
<th>CHARACTER</th>
<th>DESCRIPTION</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any character except [^,$,,,,,*,,,+,,,()]</td>
<td>All characters except the listed special characters match a single instance of themselves.</td>
<td>a matches a</td>
</tr>
<tr>
<td>\ (backslash) followed by any of [^,$,,,,,*,,,+,,,()]</td>
<td>A backslash escapes special characters to suppress their special meaning.</td>
<td>+ matches +</td>
</tr>
<tr>
<td>CHARACTER</td>
<td>DESCRIPTION</td>
<td>EXAMPLE</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>\xFF where FF are 2 hexadecimal digits</td>
<td>Matches the character with the specified ASCII/ANSI value, which depends on the code page used. Can be used in character classes.</td>
<td>\xA9 matches © when using the Latin-1 code page.</td>
</tr>
<tr>
<td>\n, \r and \t</td>
<td>Match an LF character, CR character and a tab character respectively. Can be used in character classes.</td>
<td>\n\n matches a DOS/Windows CRLF line break.</td>
</tr>
</tbody>
</table>

**Character Classes or Character Sets [abc]**

<table>
<thead>
<tr>
<th>CHARACTER CLASSES or SETS</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>
</tbody>
</table>
### Character Classes or Sets

<table>
<thead>
<tr>
<th>Character Classes or Sets</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<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>
<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>

### Anchors

<table>
<thead>
<tr>
<th>Anchors</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\n\ndef. Also matches d in &quot;multi-line&quot; mode.</td>
</tr>
</tbody>
</table>
### References

<table>
<thead>
<tr>
<th>ANCHORS</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.</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>

### Quantifiers

<table>
<thead>
<tr>
<th>QUANTIFIERS</th>
<th>DESCRIPTION</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>? (question mark)</td>
<td>Makes the preceding item optional. The optional item is included in the match, if possible.</td>
<td>abc? matches ab or abc</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 due to its limited use.</td>
<td>abc?? matches ab or abc</td>
</tr>
<tr>
<td>Quantifiers</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</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 (\geq 1)</td>
<td>Repeats the previous item exactly n times.</td>
<td>a(3) matches aaa</td>
</tr>
<tr>
<td>{n,m} where (n \geq 1) and (m \geq 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>QUANTIFIERS</td>
<td>DESCRIPTION</td>
<td>EXAMPLE</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| \{n,m\}?  
where n >= 1 and m >= n | Repeats the previous item between n and m times. Will try to repeat n times before increasing the repetition to m times. | a(2,4)? matches aaaa, aaa or aa |
| \{n\} where n >= 1 | 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. | a(2,)? matches aaaaa in aaaaa |
| \{n\}? where n >= 1 | 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. | a(2,)? matches aa in aaaaa |

**Dot**

<table>
<thead>
<tr>
<th>DOT 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>

**Word Boundaries**

<table>
<thead>
<tr>
<th>WORD BOUNDARY</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>
</tbody>
</table>
**Alternation**

<table>
<thead>
<tr>
<th>ALTERNATION CHARACTER</th>
<th>DESCRIPTION</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td></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>
<td>abc</td>
</tr>
<tr>
<td></td>
<td>The vertical bar has the lowest precedence of all operators. Use grouping to alternate only part of the regular expression.</td>
<td>abc(def</td>
</tr>
</tbody>
</table>

**View database details and data in the Database Manager**

The Database Manager is used to add additional servers to your Orion configuration, perform queries, view database and table details, export data, and edit database values.

For more advanced database maintenance, SolarWinds recommends that you use the Server Management Studio provided with Microsoft SQL Server to back up, clear historical maintenance records, and perform other maintenance.

If you need to backup or restore a database, you should use the SQL Server Management Studio. For details, see Creating a Database Backup.
Add a server to Database Manager

If you have not already designated a backup or supplementary database for use with your Orion Platform product, add a SQL server.

1. Start the Database Manager in the SolarWinds Orion > Advanced Features program folder.
2. To add a default server, click Add Default Server.
3. To select a server:
   a. Click Add Server.
   b. Select or enter the SQL Server instance you want to use in the server/instance format.
   c. Select the appropriate authentication method, enter your credentials, and click Connect.

You can now see the server and associated databases in the tree structure of the Database Manager.

View database details

The Database Manager provides details per database to review current information. If the SQL server hosting your database is not listed, you should add the database.

1. Start the Database Manager in the SolarWinds Orion > Advanced Features program folder.
2. If the SQL Server hosting your SolarWinds Orion database is not listed in the left pane, add the SQL Server hosting your Orion database.
3. Click + in the left pane to expand the SQL Server hosting your SolarWinds Orion database, and right-click the database.

   The default database name is SolarWindsOrion.

4. Click Database Details.
   - The Properties tab shows general statistics and descriptions of the selected database.
   - The Tables tab lists the tables and their respective sizes.
   - If you have not yet made a backup of the database, the Last Backup field on the Properties tab is blank.
View table details

You can view the Table details for a selected database including the include property, column, and index information through the Database Manager. You can also query the selected table directly from the Table Details window for specific or additional data.

1. Start the Database Manager in the SolarWinds Orion > Advanced Features program folder.
2. If the SQL Server hosting your SolarWinds Orion database is not listed in the left pane, add the SQL Server hosting the database.
3. Expand the SQL Server hosting your SolarWinds Orion database in the left pane, and expand the SolarWinds Orion database.
   - The default database name is SolarWinds Orion.
4. From the tables displayed for the database, right-click any table to view the Table Details.
   - The Properties tab includes general statistics relating to the selected table size and creation date.
   - The Columns tab lists keys, column names, size and data types in the selected table.
   - The Indexes tab shows indexes used in the table.
5. To execute a query:
   a. Right-click the table name, and click Query Table.
   b. Adjust the default SQL query or create a new one, and click Execute.
      - The default SQL query lists the contents of the table.
6. To export a table, right-click the table name, and click Export to CSV. You will be asked to enter a name for the comma separated value file created.

Database backups and restorations

You may need to move your SolarWinds database to a different SQL Server host. Search the Microsoft Developer Network for instructions on how to back up and restore your SQL Server database.

Before you begin, shut down the SolarWinds services with Orion Service Manager from the SolarWinds Orion > Advanced Features program folder.
References

**Update NCM to use a new database server**

After you restore the SolarWinds database backup file, update your SolarWinds NCM server to recognize the restored database on the new database server.

1. Log in to your SolarWinds NCM server.
2. Start the SolarWinds Configuration Wizard.
3. Select Database, and click Next.
4. Specify your new database server in the SQL Server field.
5. To use SQL authentication, check Use SQL Server Authentication, and enter your credentials.

   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 click Next.
8. If you are prompted to use the existing database, click Yes.
9. Select Create a New Account, and then enter a new account name.
   - 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 `securityadmin`.
10. Provide and confirm an account password.
11. Click Next to start database configuration, and click Finish.

**Monitor SNMP traps**

If you monitor a large number of devices, where each device may have many connected objects of its own, requesting information from each device is impractical. You can set up the SNMP Trap Server, and each managed device can notify it about any issues by sending a trap message.

You can monitor SNMP traps with SolarWinds NPM or SolarWinds SAM.
SNMP traps are received by the SolarWinds Trap Service, which listens for incoming trap messages on UDP port 162, and then decodes, displays, and stores the messages in the SolarWinds Orion database.

The SolarWinds Trap Service can receive and process SNMP traps from any type of monitored network device, and can handle large numbers of simultaneously incoming traps.

A SolarWinds installation can process approximately 500 traps per second. Higher capacity can only be achieved with significant hardware improvements over minimum SolarWinds requirements.

You can view SNMP traps either in the Orion Web Console or in the Trap Viewer application. The Trap Viewer application allows you to configure trap-specific alerts, to view, filter, and search for traps.

**Before you begin**

- Configure devices to send SNMP traps to the IP address assigned to the Orion server. For more information about proper configuration, refer to the documentation supplied by the vendor of your devices.
- Make sure the UDP port 162 is open for IPv4 and IPv6.
- When you use SNMPv3 for polling a device and receiving traps from it, confirm that the same authentication type (auth, noauth, or priv) is configured for both polling and traps.

**What is a Trap Template?**

Trap templates are used to format your trap templates. You can use SolarWinds macros or variables in the OID Value and ValueName attributes or call values from your MIB.

The templates are placed in the following locations:

- `/SolarWinds/Common/Orion-Detailed-Alert.trap`
- `/SolarWinds/Common/Orion-Generic-Alert.trap`
- `/SolarWinds/Orion/ForwardSyslog.trap`
The following table describes the OIDs section of the Orion Generic Alert trap template. This is the section you modify to display the information you want in your trap messages.

<table>
<thead>
<tr>
<th>TEMPLATE OID line</th>
<th>INFORMATION RETURNED</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID OID=&quot;1.3.6.1.2.1.1.3.0&quot; MIB=&quot;RFC1213-MIB&quot; Name=&quot;sysUpTime.0&quot; Value=&quot;0&quot; DataType=&quot;67&quot; ValueName=&quot;0&quot; HexValue=&quot;&quot;</td>
<td>This line displays how long the device has been up.</td>
</tr>
<tr>
<td>OID OID=&quot;1.3.6.1.6.3.1.1.4.3.0&quot; MIB=&quot;SNMPv2-MIB&quot; Name=&quot;snmpTrapEnterprise.0&quot; Value=&quot;1.3.6.1.4.1.11307&quot; DataType=&quot;6&quot; ValueName=&quot;enterprises.11307&quot; HexValue=&quot;&quot;</td>
<td>This line displays the enterprise associated with the trap.</td>
</tr>
<tr>
<td>OID OID=&quot;1.3.6.1.4.1.11307.10.1&quot; MIB=&quot;SNMPv2-SMI&quot; Name=&quot;enterprises.11307.10.1&quot; Value=&quot;${AlertMessage}&quot; DataType=&quot;4&quot; ValueName=&quot;${AlertMessage}&quot; HexValue=&quot;&quot;</td>
<td>When the template is used in an alert, this line displays the alert message associated with the triggered alert.</td>
</tr>
</tbody>
</table>

Add more information by adding another OID element and incrementing the OID.

**Define how many traps to display, if you want to refresh the traps view, trap retention, and the information displayed in the Trap Viewer**

1. Click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer.
2. Click File > Settings.
3. On the General tab, configure the Trap server settings:
   a. Position the top slider to set the Maximum Number of Traps to Display in Current Traps View.
   b. If you want to Automatically Refresh the Current Traps View, select the option, and position the middle slider to set the refresh rate.
   c. Position the Retain Trap Messages For How Many Days slider to set the length of time that traps remain in the database.
Configure Trap Viewer filters and alerts

In the Trap Viewer, you can filter trap messages, and configure actions that trigger when received trap messages match defined rules.

1. Click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer.
2. Click File > Settings, and click the Alerts / Filter Rules tab.
3. Click Add Rule or click Edit Rule.
4. Click the General tab, and select Enabled.
5. Select the servers from the Apply This Rule To list.
6. Apply the rule to specific messages.
   - Click DNS Hostname, and enter a DNS Hostname Pattern to apply the rule to messages from specific hosts, domains, or hostname patterns.
     - The DNS Hostname Pattern rule is case-sensitive.
   - Click Trap Details, and enter a Trap Details Pattern to apply the rule based on the Trap Details field.
   - Click Community String, and enter the patterns in the Community String Pattern field to apply the rule to specific community strings.
7. Click Conditions to define what triggers the rule.
   - Select object identifiers and comparison functions from the linked context menus.
   - Click Browse (...) to insert conditions.

Selecting this option can slightly reduce the size of your database.

With the exception of the asterisk (*) and underscore (_) wildcards, SolarWinds recommends against using non-alphanumeric characters in filter definitions. Trap rules are not applied to unmanaged nodes. For more information, see Setting Interface Management States.
8. Click Time of Day > Enable Time of Day Checking to apply the rule during a specific period of time. Messages received outside the specified time frame will not trigger alerts.

WARNING: Enabling Time of Day checking creates more overhead for the CPU.

9. Click Trigger Threshold > Define a Trigger Threshold for this Rule to suppress alert actions until a specified number of traps arrive that match the rule.

i When Suspend Further Alert Actions For is selected, alert actions are not sent until the specified amount of time has expired. When the time period expires, only new alerts are sent. All alerts that are suppressed during the time period will never be sent.

10. Click Alert Actions.

   - Associate the rule with a new action by clicking Add New Action, and then selecting an action from the list to configure. For more information about assigning and configuring alert actions, see Define what happens when an alert is triggered.
   
   - Edit an existing action for the rule.

11. Use the arrow buttons to set the order in which actions are performed.

   i Actions are processed in the order they appear, from top to bottom.

12. Click OK to save all changes and return to Trap Viewer Settings.

13. Use the arrow buttons to arrange the order in which the rules are applied.

   i Rules are processed in the order they appear, from top to bottom.

Trap messages are now filtered by the rules and alert actions are triggered when the rule conditions are met.

**Available trap alert actions**

**Discard the Trap**

Delete unwanted traps sent to the SNMP Trap server.

**Tag the Trap**

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

Assign a specific color for display in the Orion Web Console and the Trap Viewer to flag traps matching the rule.

Log the Trap to a file

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

Write a message to a local or a remote Windows Event Log.

Forward the Trap

Specify the IP address or hostname and the port on which to forward the trap. Specify the IP address or hostname of the trap destination and the port on which the trap should be sent. Check Include Source Address to include the IP address of the trap source.

Play a sound

Play a sound when a matching SNMP trap is received.

Text to Speech output

Define a specific speech engine, the speed, pitch, volume, and message to read.

Execute an external program

Specify an external program to launch using a batch file. This action is used when creating real-time change notifications in SolarWinds NPM.

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

Send a Windows Net message either to a specific computer or to an entire domain or workgroup.
Send an E-mail / Page

Send an email from a specified account to an 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.

Change the status of an interface

SolarWinds NPM can change the status of an interface from which a trap is received. Designate the status to which the interface should change.

Search for traps in the Trap Viewer

You can search collected trap messages and format the search results list in the Trap Viewer.

1. Click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer.
2. Click View > Search Traps.
3. Enter search criteria, and click Search Database.
4. To group messages for easier navigation, select the type of grouping from the Grouping list.
5. To limit the number of displayed messages, enter or select a number in the Maximum number of messages to display field.
6. To view messages that meet your search criteria as they arrive, select a number for the Auto Refresh Every number seconds field.

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.

7. To hide the search criteria pane, toggle the pane open and closed by clicking the double up arrows in the top right of the page.

You can now see the traps according to your settings.
View current traps in the Trap Viewer

The Trap Viewer is an application which allows you to view, search for traps, or configure filters and alerts.

You must be able to log in to the computer running your SolarWinds Orion server.

1. Click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer.
2. Click View > Current Traps.
3. Click a column header to order listed traps by the selected trap characteristic.
4. Configure the Trap Viewer by clicking and dragging columns to order the presentation of trap characteristics.

The current traps are now displayed according to your settings.

Trap alert variables

The following variables can be used in trap alert messages with the Orion Trap Server. Each variable must begin with a dollar sign and be enclosed in curly braces as, for example, ${>VariableName>}.

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>
</tbody>
</table>

Trap alerts may also use any valid node variable.
<table>
<thead>
<tr>
<th><strong>DATE/TIME VARIABLE</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<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>
<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-MM-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>
General Trap Variables

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>${Application}</td>
<td>SolarWinds application information</td>
</tr>
<tr>
<td>${Community}</td>
<td>Node community string</td>
</tr>
<tr>
<td>${Copyright}</td>
<td>Copyright information</td>
</tr>
<tr>
<td>${DNS}</td>
<td>Fully qualified node name</td>
</tr>
<tr>
<td>${Hostname}</td>
<td>Host name of the device triggering the trap</td>
</tr>
<tr>
<td>${IP}</td>
<td>IP address of device triggering alert</td>
</tr>
<tr>
<td>${IP_Address}</td>
<td>IP address of device triggering alert</td>
</tr>
<tr>
<td>${Message}</td>
<td>Message sent with triggered trap and displayed in Trap Details field of Trap Viewer</td>
</tr>
<tr>
<td>${MessageType}</td>
<td>Name or type of trap triggered</td>
</tr>
<tr>
<td>${Raw}</td>
<td>Raw numerical values for properties sent in the corresponding incoming trap</td>
</tr>
<tr>
<td>${RawValue}</td>
<td>Raw numerical values for properties sent in the corresponding incoming trap. The same as ${Raw}</td>
</tr>
</tbody>
</table>

Orion Variables and Examples

Orion Platform products, including the Alert Manager, the Traps Viewer, the Syslog Viewer, and Network Atlas can employ Orion variables. These variables are dynamic and, in the case of alerts, parse when the alert is triggered or reset.

As of Orion Platform version 2015.1, variables have changed to a more flexible format. The previous implementation was SQL based, and the new version is based on SolarWinds Information Service (SWIS). For example, the variable ${ResponseTime} is now ${N=SwisEntity;M=ResponseTime}.

Check your version number by scrolling to the bottom of the page in the Orion Web Console.
Monitor Syslog messages

Syslog messages are received by the SolarWinds Syslog Service, which listens for incoming messages on UDP port 514. Received messages are decoded and stored in the SolarWinds Orion database. The SolarWinds Syslog Service can handle large numbers of simultaneously incoming Syslog messages from all your monitored devices.

A SolarWinds installation can process approximately 1 million Syslog messages per hour, which is about 300 Syslog messages per second. You can process more by increasing your hardware requirements over the minimum requirements.

You can view Syslog messages in the Orion Web Console or in the Syslog Viewer application.

Before you begin

- Confirm that your network devices are configured to send Syslog messages to the SolarWinds Orion server IP address. For proper configuration of network devices, refer to the documentation supplied by the device vendor.
- Ensure UDP port 514 is open for IPv4 and IPv6.
- The message must be formatted according to the Request for Comments (RFC) requirements.
- If a long message is split into smaller parts, these parts should be formatted to not be skipped.

SolarWinds recommends setting up Enable RFC Relay in the service to true to allow the service to restructure the message by adding the default facility, severity, or date.

Syslog message priorities

At the beginning of each Syslog message, there is a priority value. The priority value is calculated using the following formula:

Priority = Facility * 8 + Severity

See Syslog facilities and Syslog severities.
Syslog facilities

The facility value indicates which machine process created the message. The Syslog protocol was originally written on BSD Unix, so Facilities reflect the names of UNIX processes and daemons.

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.

<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>
<tr>
<td>6</td>
<td>line printer subsystem</td>
<td>18</td>
<td>local use 2 (local2)</td>
</tr>
<tr>
<td>7</td>
<td>network news subsystem</td>
<td>19</td>
<td>local use 2 (local3)</td>
</tr>
<tr>
<td>8</td>
<td>UUCP subsystem</td>
<td>20</td>
<td>local use 2 (local4)</td>
</tr>
<tr>
<td>9</td>
<td>clock daemon</td>
<td>21</td>
<td>local use 2 (local5)</td>
</tr>
<tr>
<td>10</td>
<td>security/authorization messages</td>
<td>22</td>
<td>local use 2 (local6)</td>
</tr>
</tbody>
</table>
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>
<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 issues before ALERT-level problems.</td>
</tr>
<tr>
<td>3</td>
<td>Error</td>
<td>Non-urgent failures. Notify developers or administrators as errors 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>
</tbody>
</table>
Define the number of messages displayed, message retention, and the displayed columns in the Syslog Viewer

### Table: Suggested Actions

<table>
<thead>
<tr>
<th>Number</th>
<th>Severity</th>
<th>Suggested Actions</th>
</tr>
</thead>
<tbody>
<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>

1. Click **Start** > **All Programs** > **SolarWinds Orion** > **Syslog and SNMP Traps** > **Syslog Viewer**.
2. Click **File** > **Settings**.
3. Click the **General** tab in the **Syslog Server Settings** window.
4. Adjust the **Maximum Number of Messages to Display in Current Messages view** slider to set the number of messages you want to display.
5. Automatically refresh the current messages view by selecting the option, and setting the refresh rate with the middle slider.
6. Adjust **Retain Syslog Messages for How Many Days** to set the length of time Syslog messages should stay in the database.

   - **This setting significantly affects the database size and performance.**

7. Click the **Displayed Columns** tab.
8. Use the arrow keys to select and order the fields of information you want to see in the **Current Messages view**.

   - **Clearing Syslog messages is easier if you add the Acknowledged column to your view.**

9. To wrap Syslog message text in the **Current Messages view**, select **Word Wrap Long Messages**.
10. If you do not expect to use the Syslog Viewer as your primary viewer for Syslog messages, select the **Message Parsing** tab, and select what should be removed:
    - Remove embedded **Date/Time from Syslog Messages**
    - Remove **Message Type from Syslog Messages**
References

- Remove Domain Name from DNS Lookups.

Removing the added data from each record helps you reduce the size of your SolarWinds Orion database.

**Trigger alerts when receiving specific Syslog messages**

You must be able to log in to the computer running your SolarWinds Orion server.

1. Click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Syslog Viewer.
2. Click File > Settings.
3. Click Alerts/Filter Rules.
4. Click Add New Rule to create a rule, or edit a selected rule.
5. On the General tab, complete the following steps:
   a. Provide or edit the Rule Name.
   b. Select Enabled.
   c. Select the servers from the Apply this Rule To list.
   d. Enter the IP addresses or subnets to which this rule applies in the Source IP Addresses area.

Syslog rules may not be applied to nodes in an unmanaged state. For more information about designating nodes as unmanaged, see Suspend collecting data for monitored nodes.

6. To limit the rule only to messages from specific hosts, domains, or host name patterns, click the DNS Hostname tab, and enter a DNS Hostname Pattern.

The DNS Hostname Pattern rule is case-sensitive.

To use regular expressions, select Use Regular Expressions in this Rule. See Regular Expression Pattern Matching.

7. To limit the rule only to specific message types or texts within a Syslog message, go to the Message tab, and enter rules for Message Type Pattern and Syslog Message Pattern.

8. To apply specific severity or facility types, go to the Severity / Facility tab, and select the severity and facility types.

By default, all message severities and facilities are selected.
Configure the SolarWinds Orion server to use the correct syslog port

9. To apply the rule only during a specific period of time, select the Time of Day tab, select Enable Time of Day Checking, enter the time period, and select the days of the week on which to apply the rule. Messages received outside the specified time frame will not trigger alerts.

10. 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, and select Define a Trigger Threshold for this Rule.
   b. Enter option values.

   When Suspend Further Alert Actions For is selected, alert actions are not sent until the specified amount of time has expired. When the time period expires, only new alerts are sent. All alerts suppressed during the time period are discarded.

11. Configure Syslog alert actions on the Alert Actions tab:
   a. To create an action for the rule, click Add New Action.
   b. To edit an action for the rule, select the action, and click Edit Selected Action.
   c. Configure the action. See Syslog alert actions.

   Syslog alerts use a unique set of variables. See Syslog alert variables.
   d. To delete an action, select the action, and click Delete Action.
   e. Use the arrow buttons to set the order in which actions are performed. Actions are processed in the order listed, from top to bottom.
   f. Click OK to save all changes and return to Syslog Viewer Settings.

12. Use the arrow buttons to arrange the order in which the rules are applied. Rules are processed in the order they appear, from top to bottom.

Configure the SolarWinds Orion server to use the correct syslog port

By default, SolarWinds Syslog Service listens for syslog messages on port 514 (UDP). If your devices use a different port for sending syslog messages, consider reconfiguring the port on devices, or change the port on which the service listens.
Running the Configuration Wizard will revert all changes made to the SyslogService.exe.config file.

If you run the Configuration Wizard, you must repeat this procedure to restore the port setting.

1. Log in to the Orion Web Console as an administrator.
2. Go to Advanced Configuration settings. Copy /Admin/AdvancedConfiguration/Global.aspx, and paste it into your browser address bar, after /Orion.
   The address in the address bar should look as follows:
   <your product server>/Orion/Admin/AdvancedConfiguration/Global.aspx
3. On the Global tab, scroll down to SyslogService.SyslogSettings, and enter the UDP port number in the UDPListenPort entry.
4. Click Save.

**Suspend collecting data for monitored nodes**

Monitored devices are regularly polled for operational status. Collected statistics are displayed in the Orion Web Console.

You can temporarily suspend data collection on individual nodes and resume data collection as necessary.

If you suspend data collection for a node, it is suspended automatically for all interfaces and volumes on the selected node.

Suspending data collection is helpful when you need to perform maintenance on a node or its components, such as upgrading firmware, installing new software, or updating security. Suspend polling data for the node while the device is down for maintenance to maintain the accuracy of data and prevent unnecessary alert messages.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Locate the node(s).
4. Select the nodes, and click Unmanage.
5. Provide start and end times and dates for your management suspension, and click OK.
   Data for the selected node and monitored resources on the node will be suspended for the specified time period.

**Resume data collection for nodes**

On Manage Nodes, select the node, and click Remanage.
Information for the selected node, all monitored interfaces and volumes on it will be collected again.

**Syslog alert actions**

**Discard the Syslog Message**
Delete unwanted Syslog messages sent to the Syslog server.

**Tag the Syslog Message**
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**
Modify the severity, facility, type, or contents of a Syslog message.

**Log the Message to a file**
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**
Write a message to local or remote Windows Event Logs.

**Forward the Syslog message**
Specify the IP address or hostname and the port to forward a Syslog event.

**Send a new Syslog message**
Trigger a new Syslog message, sent to a specific IP address or hostname, on a specific port, with a customizable severity, facility, and message.
Send an SNMP Trap

Send a trap to an IP address following a specific trap template and using a specific SNMP community string.

Play a sound

Play a sound when a matching Syslog message is received.

Text to Speech output

Define the speech engine, speed, pitch, volume, and message to read.

Execute an external program

Allows you to specify an external program to launch using a batch file. This action is used when creating real-time change notifications in Orion.

Execute an external VB Script

Launch a VB Script using the selected script interpreter engine and a saved script file.

Send a Windows Net Message

Send a net message either to a specific computer or to an entire domain or work group.

Send an E-mail / Page

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.

Suspend a virtual machine

If a virtual machine is experiencing performance issues, you can have an alert trigger the virtual machine to be suspended. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Suspend, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to suspend.
   a. To suspend the virtual machine that triggered the alert, click Execute this action.

   ![This option is only available if the alert is built to trigger for virtual machines.]

   b. To suspend a different virtual machine, click Select specific VM, and search for a virtual machine.

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   ![This is often used to prevent an action from occurring during specific windows.]

5. Select how frequently this action occurs for each triggered alert in Execution Settings.

6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine is suspended.

**Restart a virtual machine**

If a virtual machine is experiencing issues, you can have an alert trigger the virtual machine to be restarted. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Reboot, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to reboot.
   a. To reboot the virtual machine that triggered the alert, click Execute this action.

   ![This option is only available if the alert is built to trigger for virtual machines.]

   b. To reboot a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   ![Tip](This is often used to prevent an action from occurring during specific windows.)

5. Select how frequently this action occurs for each triggered alert in Execution Settings.

6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine restarts.

**Power off a virtual machine**

If a virtual machine is experiencing issues, you can have an alert trigger the virtual machine to be powered off. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.

2. Select Manage VM - Power Off, and click Configure Action.

3. Under Select Virtual Machine, specify the virtual machine that you want to power off.
   a. To power off the virtual machine that triggered the alert, click Execute this action.

   ![Information](This option is only available if the alert is built to trigger for virtual machines.)

   b. To power off a different virtual machine, click Select specific VM, and search for a virtual machine.

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   ![Tip](This is often used to prevent an action from occurring during specific windows.)

5. Select how frequently this action occurs for each triggered alert in Execution Settings.

6. Click Add Action.
The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be powered off.

**Power on a virtual machine**

If a virtual machine is powered off, you can have an alert trigger the virtual machine to be powered on. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Power On, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to power on.
   a. To power on the virtual machine that triggered the alert, click Execute this action. 

   This option is only available if the alert is built to trigger for virtual machines.

   b. To power on a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be powered on.

**Pause a virtual machine**

If a virtual machine is experiencing issues, you can have an alert trigger a pause for the virtual machine. This alert management action is only available if the integration with Virtualization Manager is enabled.
This action can only be configured for Hyper-V virtual machines.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Pause, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to pause.
   a. To pause the virtual machine that triggered the alert, click Execute this action.
      
      This option is only available if the alert is built to trigger for virtual machines.
      
   b. To pause a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   
   This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be paused.

**Move a virtual machine to a different host**

If a virtual machine is experiencing issues, you can have an alert trigger the virtual machine to be moved to a different host. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Move to a Different Host, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to move.
   a. To move the virtual machine that triggered the alert, click Execute this action.
      
      ![This option is only available if the alert is built to trigger for virtual machines.]

      To apply the action only to virtual machines of a specific vendor, select the relevant option, and specify whether you want to perform to action on Hyper-V or VMware virtual machines.

      b. To move a different virtual machine, click Select specific VM, and search for a virtual machine.

4. To power off the virtual machine before moving it to a different host, and then power it on again after the action has been completed, select the relevant option.

   ![If the option is not selected, the action will be performed live on the virtual machine.]

5. Under Select Target Host, search for the host where you want to move the selected virtual machine.

6. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   This is often used to prevent an action from occurring during specific windows.

7. Select how frequently this action occurs for each triggered alert in Execution Settings.

8. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be moved to a different host.

**Move a virtual machine to a different storage**

If a virtual machine is experiencing storage issues, you can have an alert trigger the moving of the virtual machine to a different storage location. This alert management action is only available if the integration with Virtualization Manager is enabled.

   1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Move to a Different Storage, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to move.
   a. To move the virtual machine that triggered the alert, click Execute this action.
      
      This option is only available if the alert is built to trigger for virtual machines.

      To apply the action only to virtual machines of a specific vendor, select the relevant option, and specify whether you want to perform to action on Hyper-V or VMware virtual machines.

   b. To move a different virtual machine, click Select specific VM, and search for a virtual machine.
4. To power off the virtual machine before moving it to a different storage, and then power it on again after the action has been completed, select the relevant option.

   If the option is not selected, the action will be performed live on the virtual machine.
5. Under Select Target Datastore, search for the datastore where you want to move the selected virtual machine.
   a. In a VMware environment, select one of the available datastores.
   b. In a Hyper-V environment, select one of the available datastores, and click either Use the default location to move the virtual machine to the default location of the datastore, or click Specify custom path, and enter a custom location.
6. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   This is often used to prevent an action from occurring during specific windows.
7. Select how frequently this action occurs for each triggered alert in Execution Settings.
8. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be moved to a different datastore.
Syslog alert variables

The following variables can be used in syslog alert messages. Each variable must begin with a dollar sign and be enclosed in curly braces as, for example, \${VariableName}. Syslog alerts also support the use of Node alert variables.

For more information on the use of variables, see Orion Variables and Examples.

**Syslog date/time variables**

<table>
<thead>
<tr>
<th><strong>SYSLOG DATE/TIME VARIABLE</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>${AbbreviatedDOW}</td>
<td>Current day of the week. Three character abbreviation.</td>
</tr>
<tr>
<td>${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 &quot;Short Date&quot; and &quot;Short Time&quot; format)</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>${Hour}</td>
<td>Current hour. 24-hour format</td>
</tr>
<tr>
<td>${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>
</tbody>
</table>
### Syslog Date/Time Variables

<table>
<thead>
<tr>
<th>Syslog Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>${Application}</td>
<td>SolarWinds application information</td>
</tr>
<tr>
<td>${Copyright}</td>
<td>Copyright information</td>
</tr>
<tr>
<td>${DNS}</td>
<td>Fully qualified node name</td>
</tr>
<tr>
<td>${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>
</tbody>
</table>
Delete a snapshot of a virtual machine

<table>
<thead>
<tr>
<th>SYSLOG VARIABLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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>

**Delete a snapshot of a virtual machine**

If a virtual machine is experiencing resource issues, you can have an alert trigger a virtual machine snapshot to be deleted. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Delete Snapshot, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine from which you want to delete a snapshot.
   a. To delete a snapshot of the virtual machine that triggered the alert, click Execute this action.
      
      This option is only available if the alert is built to trigger for virtual machines.

   b. To delete a snapshot of a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the **trigger** or **reset** action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the snapshot of the specified virtual machine will be deleted.
Change the resource allocation of a virtual machine

If a virtual machine is experiencing performance issues, you can have an alert trigger a specified allocation of resources. This alert management action is available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Change CPU/Memory Resources, and click Configure Action.
3. Enter a name for the action.
4. Under Select Virtual Machine, specify the virtual machine on which you want to adjust the number of CPUs, the memory capacity, or both.
   a. To change the resource allocation of the virtual machine that triggered the alert, click Execute this action.
      
      This option is only available if the alert is built to trigger for virtual machines.
   b. To change the resource allocation of a different virtual machine, click Select specific VM, and search for a virtual machine.
5. To power off the virtual machine before changing the resource allocation, and then power it on again after the resource allocation has been changed, select the relevant option.

      This option is only available if the alert is built to trigger for virtual machines.
6. Under Specify New Resources, specify whether you want to add more resources to the virtual machine, or replace the existing resources with new resources, and then specify the parameters of the new resource or resources.
   a. Select Number of processors, and specify the number of processors to allocate.
   b. Select Memory, and specify the memory capacity to allocate.
7. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   
   This is often used to prevent an action from occurring during specific windows.
8. Select how frequently this action occurs for each triggered alert in Execution
Settings.

9. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified CPU and memory resources will be allocated to the virtual machine.

**Restart IIS sites or application pools**

If IIS or application pools are experiencing performance or resource issues, you can use an alert to restart them.

- You must know the IIS Server name and the Site or Application Pool to restart a remote instance of IIS.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Restart IIS Site/Application Pool from the options, and then click Configure Action.
3. Expand Restart IIS Site/Application PoolSettings.
   a. Select the IIS Action to Perform from the drop down list.
   b. Choose the Site or Application Pool.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   - This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the selected site or pool restarts.
Manually set a custom status

Setting a custom status can be useful if you want to change the status of a familiar node, but does not affect actual, polled values. For example, if the custom status is set to Up, but the server is down or unresponsive, packet loss continues to be 100%. Alerts based on the status do not trigger in this instance, but alerts based on a polled value, such as packet loss, do trigger.

When the status is set with an alert, the status does not update to the actual, polled status. The status must be switched manually to a different status or configured to use the polled status. Change the status to use the polled status from the node details page or create a reset action to set the status to use the polled status.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Set Custom Status option, then click Configure Action.
3. Under Change Object Status Manually:
   a. Select Change to a specific status if you are creating a trigger action, and choose a status.
   b. Select Use polled status if you are creating a reset action.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   - This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the status for the object changes.

View Syslog messages in the Orion Web Console

The Orion Web Console provides both syslog-specific resources and a syslog view with a table of syslog messages received by your SolarWinds Orion server.
View Syslog messages in the Orion Web Console

The Syslog view displays a list of all the syslog messages generated by monitored network devices. The messages are listed by time of transmission, with the most recent at the top of the list.

1. Log in to the Orion Web Console, and click Alerts & Activity > Syslogs in the menu bar.
2. To filter syslog messages so that only messages relevant for specific devices are displayed:
   - To view messages for a specific syslog-enabled network object, select it in the Network Object list.
   - Only objects that have sent a syslog message to the Orion server will be listed in this field.
   - To view messages for a specific device, provide the IP address in the IP Address field.
   - To view messages for a specific device type, select it in the Type of Device list.
   - To view messages for a specific vendor, select the vendor in the Vendors list.
3. To select which syslog messages should be displayed:
   - To view only messages with a severity, select the severity.
   - To view messages for a facility, select the facility.
   - To view messages of a type, type the string into the Message Type field.
   - To view only messages containing a pattern, provide the string in the Message Pattern field.
   - You can use the following wildcards:
     - Asterisk (*): Use * before or after the pattern string if the provided pattern is not the beginning, the end or the full message.
     - Underscore (_): Use _ as a placeholder for one character.
   - To view syslog messages from a specific period of time, select either a period of time or enter custom Beginning and Ending Date/Times.
   - Type the number of syslog messages you want to view into Number of Displayed Messages.
   - To view cleared and acknowledged syslog messages, select Show Cleared Messages.
4. Click Refresh to update the syslog messages list with your settings.

Syslog messages matching the selected criteria display in a list beneath the search area.

Click Hide or Show in the top-right corner of the view to remove or restore the Syslog messages search criteria area.

Click the Hostname or Message to open the Device Details view for the device.

**Search for Syslog messages in the Syslog Viewer**

In the Syslog Viewer, you can search through collected Syslog messages and format search results.

1. Click View > Search Messages.
2. Enter the search criteria.
3. Click Search Database.
4. To group messages for easier navigation, select the type of grouping from the Grouping list.

   ![Note]
   You can acknowledge messages both in the search results and in the Current Messages view. See Define the number of messages displayed, message retention, and the displayed columns in the Syslog Viewer.

5. To limit the number of displayed message, enter or select a number in the Maximum Number of Messages to Display field.
6. To view messages that meet your search criteria as they arrive, select a number for the Auto Refresh Every number of 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.

**Custom properties**

Every object you monitor includes a list of default properties used to describe the devices, such as IP address, host name, or MAC address. You can also create custom properties and use them to create special alerts, reports, views, and groups.

Custom properties are user-defined fields, such as country, building, asset tag, or serial number, that you can associate with monitored network objects.
Create a custom property

Custom properties must use the Latin1 character set.

Custom property uses include:

- Add information to nodes, such as contact, owner, or support contract.
- Add a custom property that is used as an account limitation on nodes.
- Add a custom property to nodes for grouping on the web or in a report.
- Add a custom property and display it as an annotation on a chart.

A collection of the most commonly used properties is available out-of-the-box, but you can create custom properties to meet your precise requirements.

When a custom property is defined, you can import values for the property from a text- or comma-delimited file.

To apply a property to only a few objects, go to the Edit view in the Orion Web Console.

You may also create external records by exporting custom properties from selected objects as a spreadsheet.

When you create, edit or remove a custom property, an event is logged. These events are audited, and you can display them in Audit Events resources.

Create a custom property

Custom properties help you add custom labels to monitored objects, group objects based on the property or alert on objects with a certain value for the property.

Depending on the selected object type, some options are not available.

1. Click Settings > All Settings in the menu bar.
2. In the Node & Group Management grouping, click Manage Custom Properties.
3. Click Add Custom Property.
4. Select the object type for the property, and click Next.

The available object types depend on the Orion Platform products installed. All installations allow you to create Node and Volume custom properties.
5. Define the custom property, and click Next.

- Frequently used custom properties are available as templates. Select a template, and adjust the settings if necessary. Templates ensure that naming conventions are met when necessary for certain workflows, such as drawing lines signifying a certain value in resources.

  a. Edit the Property Name and Description fields.

  - Property names are not case-sensitive, and must be unique for each object type. For example, you can have separate Comment properties for Nodes, Volumes, and other object types.

  b. Select the Format for the property.

  - We recommend that you limit the string length for text properties. The string length can affect SQL performance, especially when custom properties are used in limitations. The shorter the string length, the faster the queries.

  To limit the string length, click Edit, and provide the maximum number of characters:

    Format: [Text] Any alpha and numeric text (up to 400 characters) Edit

  c. Create a drop-down menu with specific values for the property by selecting Restrict values, and adding the values.

  - Restricting values helps to maintain the consistency of values for individual custom properties.

  d. If you want to limit how the custom property for nodes should be used, clear boxes in the Usage section.

6. Select objects for which you want to define the custom property.

  a. Click Select <Objects>, and locate, and select the objects in the Available <Objects> pane.

  b. Click Add, and then click Select <Objects>.
Create a custom property

7. Enter or select a default value for the property.

To add a value for properties with restricted values, select Add New Value from the drop-down menu, and enter the new value.

8. To apply the selected property to a different group of objects, click Add More, select the objects, and click Submit.

You have created a custom property and provided its value for the selected objects.

Now, you can specify the property value in the object properties. For example, for node properties, click Settings > Manage Nodes, select the object, and click Edit Properties.
You can now use the custom property for sorting objects of the type in Group By lists.

### Assigning values to a custom property

The following procedure provides steps required to assign new values to an existing custom property.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. Click Manage Custom Properties in the Node & Group Management grouping.
4. Select the custom property for which you want to assign values, and then click Assign values.
5. 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.
6. Check all monitored objects to which you want the selected custom property to apply.

   Tips: Click > to expand listed objects to view available child objects.

7. Click Add to add checked objects to the Selected Objects list.
8. In the Selected Objects list, check all objects to which you want the selected property to apply.
9. If you have selected all objects to which you want the selected property to apply, click Select Objects.
10. For each selected object, select or enter an appropriate property value.
11. 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.
12. If you want to apply the selected property to a different group of objects, click Add more, and then select objects as indicated above.
13. If you have selected values for all objects to which you want the selected property to apply, click Submit.

**Change custom properties values**

You can change the value of a custom property from the Manage Custom Properties page or bulk edit the values of a custom property assigned to objects.

Tips: You can only edit properties of one object type at a time.

**Edit values for custom properties**

When you are entering a large amount of data, it can be easier to import the values from a spreadsheet.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Custom Properties.
4. Select the custom properties, and click View / Edit Values. You can filter objects to find the custom properties more easily.
5. To add or change a value for a property, enter the value into the field.
References

6. To add the same custom property value for multiple objects, select the objects, and click Edit Multiple Values. Select the property, enter the value, and click Save Changes.

7. When you have added or edited the values, click Save Changes.

**Import custom property values**

If you have a spreadsheet listing custom property values, such as asset tags of all your network nodes, you can make this information available for reporting and publication in the Orion Web Console.

Your data must be formatted as a table, and at least one column title should match an existing object property such as IP Address.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Custom Properties.
4. Click Import Values.
5. Browse to the custom property data file, and click Open.
6. Select the object type you want in the Import Values For drop-down, and click Next.
7. For each detected Spreadsheet Column in your data, select the corresponding Orion Database Column, and select the Relationship between the columns.
   - Select Matches to indicate columns in the spreadsheet that correspond to existing columns in the SolarWinds Orion database, such as IP Address or MAC address.

<table>
<thead>
<tr>
<th>SPREADSHEET COLUMN</th>
<th>RELATIONSHIP</th>
<th>ORION DATABASE COLUMN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caption</td>
<td>matches</td>
<td>Caption</td>
</tr>
<tr>
<td>IP_Address</td>
<td>matches</td>
<td>IP_Address</td>
</tr>
</tbody>
</table>

- Select Imports To to import the data in the spreadsheet column to the selected SolarWinds Orion database column.

This option overwrites any existing data in the corresponding custom properties.
Select Imports To, and select <No Match Found, Ignore> for any spreadsheet column you do not want to import.

- Click Create This Custom Property Now to open the Add Custom Property in a new browser tab if you need to create a custom property for this spreadsheet column.

8. Click Import.

When you view the values of the object type, the values of the custom property you selected are populated.

Exporting custom properties

With the Export Custom Properties feature, you can download a spreadsheet of any selected custom property, as it is stored in your SolarWinds Orion database.

To export a custom property:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. Click Manage Custom Properties in the Node & Group Management grouping.
4. Check the property you want to export, and then click Export.
5. 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.
6. Select the columns you would like to export.
7. Choose a file type for the exported file, and then click Export.
8. The exported file is saved with the file name exportCP in the locally designated downloaded files folder for your web console browser.

Remove a custom property

If the custom property is used in reports or alerts, remove it from the definition of all alerts and reports before you remove it from the Orion Web Console. Reports defined using removed custom properties do not work, and alerts stop triggering.
1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Custom Properties.
4. Select properties you want to remove, and click Delete.
5. Confirm your action when prompted.

**Configure automatic login**

You can log in automatically to the Orion Web Console using any of the following methods.

**Use a Windows Active Directory Account**

Create users based on active directory or local domain accounts, and enable automatic login for users logged in to the server. See Create users based on existing Active Directory or local domain accounts.

- Windows authentication must be enabled in the Configuration Wizard and the Web Console Settings. See Enable Windows Authentication with Active Directory.

**Automatically log in with Windows Pass-through Security**

Users can be authenticated through Windows Security, with no need to log in with separate credentials. For more information, see Log in with Windows pass-through security.

**Share content to non-SolarWinds users with the DirectLink account**

If the DirectLink account is active, any URL referring directly to an Orion Web Console page will bypass the login page by logging the user into the DirectLink account. See Share views with non-Orion Web Console users.

**Pass-through user credentials in a URL**

See Automatically login by passing your credentials through the URL.

Users are authenticated in the following priority:

1. Windows Active Directory Authentication when enabled
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 Pass-through Security is enabled
5. The Windows Domain to which the User belongs, for example, Development\Everyone
6. A DirectLink Account

**Log in with Windows pass-through security**

To authenticate users through Windows pass-through security, IIS NT Security must be enabled on your server.

Pass-through security can be configured to employ Domain security, Local computer security, or both Domain and Local computer security at the same time.

The Orion Platform account credentials must match the credentials used for the Domain or Local computer security.

- This procedure requires access to the computer that hosts the SolarWinds Orion server.
- When authenticating users with Windows Security, ensure your Orion server uses the NetBIOS domain name, instead of the fully qualified domain name.

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. For example:
   - Washington\Edward
   - StLouis\Bill
2. If you are using Local Computer Authentication Format for passthrough accounts, create these accounts in the Orion Web Console Account Manager using Computer\UserID as the User Name. For example:
   - SolarWindsS2\Edward
   - Server3\JonesR
Log in to the Orion Web Console using the Windows account credentials you have already established.

**Automatically login by passing your credentials through the URL**

Create a favorite or bookmark that includes your Orion individual account user name and password as parameters within the URL.

⚠️ HTTP requests are not encrypted, so account information sent in HTTP requests are not secure. For more information about enabling HTTPS on your Orion Platform product server, consult www.microsoft.com.

Create a favorite with a link in the following form to pass the login information:


Provide the hostname or IP address of your SolarWinds Orion server as the DOMAIN. Provide your Orion user name as the USER, and then provide your Orion user account password as the PASSWORD.

**Share views with non-Orion Web Console users**

Any URL referring directly to a Orion Web Console page bypasses the login screen, logging the user into the DirectLink account. If the DirectLink account does not exist, users are directed to the login page.

- The DirectLink account is created like any other account, and it can include custom views and account limitations.
- If you embed a view in another website, you may need to either disable cross-frame (X-Frame) protection in your IIS configuration, or add the website to the X-Frame-Options header in IIS. SolarWinds enables cross-frame protection by default to decrease security risks. Consult microsoft.com for more information.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the User Accounts grouping, click Manage Accounts.
4. Click Add New Account.
Enable Windows Authentication with Active Directory

5. Type DirectLink as the User Name.
6. Type a Password, confirm it, and click Next.
7. Edit DirectLink account options. See Define what users can access and do.
8. Click Submit.

Users can now look at views without an account on the Orion Web Console.

Enable Windows Authentication with Active Directory

The Orion Web Console can authenticate Active Directory users and users who are members of Active Directory security groups by using MSAPI or LDAP. By default, Windows individual or group accounts use MSAPI to authenticate accounts.

You can only use one authentication protocol at a time. All Windows accounts are authenticated through MSAPI or LDAP, depending on which one is enabled.

SolarWinds offers a free analyzer tool for Active Directory that provides instantaneous visibility into effective permissions and access rights. The tool provides a complete hierarchical view of the effective permissions access rights for a specific file folder (NTSF) or share drive. Download it for free from here: http://www.solarwinds.com/products/freetools/permissions_analyzer_foractive_directory/.

Authenticate users through MSAPI

1. Enable the Orion Web Console to use automatic Windows Authentication.
   a. Start the Configuration Wizard in the SolarWinds Orion > Configuration and Auto-Discovery program folder.
   b. Select Website, and click Next.
   c. Provide the appropriate IP Address, Port, and Website Root Directory, and select Yes – Enable Automatic Login Using Windows Authentication.
   d. Click Next, and complete the Configuration Wizard.
2. Log in to the Orion Web Console using the appropriate domain and user, providing Domain\Username or Username@Domain as the User Name.
3. Run the Configuration Wizard and enable Windows authentication.
4. Login to the Orion Web Console, and navigate to Settings > All Settings. In Web Console Settings, select Enable automatic login in the Windows Account Login drop-down.
Enable users to authenticate through LDAP

You can choose to have all of your AD users authenticate through LDAP. The SolarWinds Orion server does not need to be added to the Windows domain with this authentication method.

We do not support Anonymous authentication through LDAP.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. Click Advanced AD Settings in the User Accounts grouping.
4. Toggle Authenticate Active Directory Users via LDAP.
5. Enter your LDAP server information and select the authentication method that matches what is used in LDAP.

Windows individual accounts now use LDAP. If you created Orion Web Console accounts that use Active Directory or local accounts and those accounts cannot authenticate through LDAP, those accounts cannot login.

If you disable this selection, Windows users or group members created while it was enabled cannot login.

Define what users can access and do

Each user or group account can have different privileges applied to it, such as the ability to modify alert definitions or delete nodes.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. Click Manage Accounts in the User Accounts grouping.
4. Select an account, and click Edit.
Define what users can access and do

5. Specify the login options.

<table>
<thead>
<tr>
<th>LOGIN OPTION</th>
<th>SETTING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Should the user be able to log in immediately?</td>
<td>Set Account Enabled to Yes. Disabling an account does not delete it. Account definitions and details are stored in the SolarWinds Orion database and can be enabled later.</td>
</tr>
<tr>
<td>Should the user be able to log in only temporarily?</td>
<td>Specify the expiration date.</td>
</tr>
<tr>
<td>Should the user be logged in indefinitely even if the browser is closed?</td>
<td>Select Yes for the Disable Session Timeout option. Session timeouts are global and set in Web Console Settings. By default, new user accounts are configured to timeout automatically.</td>
</tr>
</tbody>
</table>
6. Specify what tasks the user should be able to do.

<table>
<thead>
<tr>
<th>Task</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add and edit user accounts and reset passwords.</td>
<td>Allow Administrator Rights</td>
</tr>
<tr>
<td><strong>SolarWinds recommends that you do not allow users to change their own Orion Web Console account passwords.</strong></td>
<td>Granting administrator rights does not assign the Admin menu bar to a user. For more information, see <a href="#">Set default menu bars and views for users.</a></td>
</tr>
<tr>
<td>Add, edit, and delete nodes.</td>
<td>Allow Node Management Rights</td>
</tr>
<tr>
<td>Create, edit, and delete maps in the Network Atlas.</td>
<td>Allow Map Management Rights</td>
</tr>
<tr>
<td>Add, edit, schedule, and delete reports.</td>
<td>Allow Report Management Rights</td>
</tr>
<tr>
<td><strong>To only allow access to some reports, select the report category the user can access.</strong></td>
<td></td>
</tr>
<tr>
<td>Add, edit, and delete alerts.</td>
<td>Allow Alert Management Rights</td>
</tr>
<tr>
<td><strong>To only allow some actions, keep No in Allow Alert Management rights and Allow items in the Alerts section as appropriate.</strong></td>
<td><strong>To only access some alerts, select the category the user can access, or No Limitation.</strong></td>
</tr>
<tr>
<td>Customize views.</td>
<td>Allow Account to Customize Views</td>
</tr>
<tr>
<td><strong>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.</strong></td>
<td></td>
</tr>
<tr>
<td>Enable/disable monitoring elements.</td>
<td>Allow Account to Unmanage Objects</td>
</tr>
<tr>
<td>Acknowledge and clear events, advanced alerts, and Syslogs.</td>
<td>Allow Account to Clear Events, Acknowledge Alerts and Syslogs.</td>
</tr>
</tbody>
</table>
Define what users can access and do

7. If you want the user to use additional browser functions, such as right-click menu options, set Allow Browser Integration to Yes.

   Right-click menu options also depend on installing the SolarWinds Desktop Toolset and running the Toolset Integration Tray application on each client computer.

8. Provide the maximum Number of Items in the Breadcrumb List.

   To show all available items in breadcrumb drop-downs, set this option to 0.

9. Click Submit.

New account settings are applied when a user next logs in.

The user account also controls the default menu bars and views, and how much of your network they can access through the Orion Web Console.