SolarWinds

Network Configuration Manager Administrator Guide

NETWORK CONFIGURATION
MANAGER

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.

Portions of the following SolarWinds SAM Documentation is excerpted from:

IBM DeveloperWorks, © Copyright IBM Corporation 1994, 2012. Available at http://www.ibm.com/developerworks/

Microsoft TechNet, “TechNet Library”, © 2010 Microsoft Corporation. All rights reserved. Available at technet.microsoft.com.

Oracle Corporation, 2012 © 2010 Oracle Corporation. All rights reserved. Available at www.oracle.com

SolarWinds SolarWinds Network Configuration Manager 07.29.2014 Version 7.3.1.

About SolarWinds

SolarWinds, Inc develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today's network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Contacting SolarWinds

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

Team	Contact Information
Sales	sales@solarwinds.com www.solarwinds.com 1.866.530.8100 +353.21.5002900
Technical Support	www.solarwinds.com/support
User Forums	thwack.com

Conventions

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

Convention	Specifying
Bold	Window items, including buttons and fields
Italics	Book and CD titles, variable names, new terms
`Fixed font`	File and directory names, commands and code examples, text typed by you
Straight brackets, as in [*value*]	Optional command parameters
Curly braces, as in {*value*}	Required command parameters
Logical OR, as in *value1*|*value2*	Exclusive command parameters where only one of the options can be specified

SolarWinds Network Configuration Manager Documentation Library

The following documents are included in the SolarWinds SolarWinds Network Configuration Manager documentation library:

Document	Purpose
Administrator Guide	Provides detailed setup, configuration, and conceptual information.
Page Help	Provides help for each resource in the Web Console accessed through the Help button.
Quick Start Guide	Provides installation, setup, and common scenarios for which SolarWinds Network Configuration Manager provides a simple, yet powerful, solution.
Release Notes	Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at www.solarwinds.com.

Contents

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 9

Chapter 10

Chapter 11

Chapter 12

Chapter 13

Chapter 14

Chapter 15

Chapter 16

Appendix A

Appendix B

Appendix C

Appendix D

Appendix E

Index

Chapter 1

Introduction

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

Why Install SolarWinds SolarWinds Network Configuration Manager

Out of the box, SolarWinds SolarWinds Network Configuration Manager offers numerous management features, including the ability to:

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

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

Key Features of SolarWinds Network Configuration Manager

Considering the previously mentioned benefits of SolarWinds Network Configuration Manager, coupled with the following features, SolarWinds Network Configuration Manager is the clear choice to make:

Scheduled Configuration Backups

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

Policy Management

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

Role-Based Access Control

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

Multivendor Support

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

Bulk Changes

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

Configuration Change History

You can receive reports on what devices have had configuration changes over any time period you specify. Configuration change reports can also compare current configurations with a baseline configuration alerting you whenever a change is discovered.

Web-Based NCM Settings

You can use a web browser to set and adjust NCM Settings.

Web-Based Configuration Viewing, Tracking, and Comparing

You can use SolarWinds Network Configuration Manager to remotely view, track changes, and compare network device configurations without logging on to the physical SolarWinds Network Configuration Manager server. The Orion Web Console offers these powerful functions to the users you select.

Orion Web Console Integration

With NCM you gain these important resources in the Device Details view of the Orion Web Console:

Recent Configurations

Recent Configuration Changes

Node Configuration History

Last 10 Conf Changes

Last X Config Changes

Last XX Configurations

Additionally, if NCM is integrated with NPM, you gain this resource on the Config Summary view:

Find Connected Port for End Host

Orion Alerts Integration

With the SolarWinds NCM integration module you can use a default NCM alert in the Orion Alert Manager; and you can specify NCM actions to run when this alert triggers, viewing the results of those actions along with the notification.

Device Configuration Change Templates

You can use templates to generate an appropriate sequence of CLI commands for all relevant devices for which you need to make a specific configuration change.

Device Configuration Change Management

You can setup a request and approval system for processing the workflow of device configuration changes.

How Does SolarWinds NCM Work?

SolarWinds Network Configuration Manager utilizes a scripting engine that parses individual commands across several different platforms. Combining this scripting engine 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 NCM database and accessible from the SolarWinds NCM application console and the Orion Web Console.

Chapter 2

Installing SolarWinds Network Configuration Manager

SolarWinds NCM version 7.3.X is a major rearchitecture that merges all Orion Platform and NCM data into a single database.

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

You have two options for either installing or upgrading the NCM version 7.3.X software.

Single Server Standalone

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

Single Server Integrated

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

Installing or upgrading NCM involves these processes:

- Installing the NCM software
- Configuring the database, website, and services
- Discovering network devices
- Migrating data from an existing NCM database (upgrade only)

Notes on Installation and Upgrade:

- A separate server deployment is not supported with NCM 7.3.X. If you are upgrading an NCM separate server deployment, you must convert to a single server deployment. In an existing separate server standalone deployment, you do that by installing the NCM 7.3.X software on the host where the NCM Web software is currently running.

- When you upgrade NCM to version 7.3.X, the installer migrates config and other data from your existing NCM database into the Orion Platform database that currently holds your node data. The time needed to complete the migration varies depending on how much and what data you are migrating. See the section “Preparing to Upgrade SolarWinds Network Configuration Manager” for more information.
- Whether you are installing or upgrading NCM, in order to ensure its best performance on your server host, specifically exclude these file paths from anti-virus software scans:

  ```
  %USERPROFILE%\AppData\Local\Temp

  %ALLUSERSPROFILE%\Application Data\Solarwinds

  %Program Files (x86)%\SolarWinds\Orion

  %Program Files (x86)%\SolarWinds\Orion\NCM

  C:\Windows\System32\msmq\storage
  ```

You can find SolarWinds NCM 7.3.X installation software in your customer portal.

Installing NCM Software

Information in this section guides you in installing NCM software—includng software common to all Orion Platform products—on a single host, either with or without another Orion Platform product.

An Orion Platform product is one whose features and functions can be accessed and managed through the Orion Web Console. Integrating NCM with another Orion Platform product on a single host gives you the benefits of having features of multiple products available from the same Orion Web Console.

When the SolarWinds Configuration Wizard prompts you to create the database,. SolarWinds highly recommends that you create your database on a separate SQL Server host—not on a SQL Server instance that cohabits the NCM host. SolarWinds especially recommends using a remote SQL Server host if you are installing SolarWinds NCM on the same host with SolarWinds NPM; as you will gain a number of performance enhancements through this deployment scenario,.

If after installing the NCM software in a standalone deployment, you want to install and integrate another Orion Platform product with NCM at a future time, you can do so only on the NCM host. The other Orion Product would share the Orion Platform database that you have already established with your installation of NCM.

You cannot integrate NCM with an Orion Platform product already installed on a different host. Conversely, you cannot separate NCM from another Orion Platform product once you have integrated them; since both share a single database.

Supported Products for Integration

Here is the current list Orion Platform products and version with which SolarWinds NCM version 7.3.X can integrate. You must upgrade to an appropriate version of the other Orion Platform product(s) for NCM integration to function.

- SolarWinds Network Performance Manager (NPM) version 10.11
- SolarWinds Server and Application Monitor (SAM) versions 6.0.x, 6.1.x
- EOC: 1.4, 1.5, 1.6
- SolarWinds IP Address Manager (IPAM) version 4.0, 4.1
- SolarWinds User Device Tracker (UDT) version 3.0.x
- SolarWinds IPSLA (VNQM) version 4.0.1, 4.1, 4.2
- Toolset: 10.9, 11.0

Note: Because SolarWinds NCM 7.x shares common components with all Orion Platform products, the process of installing and configuring SolarWinds NCM involves shutting down and restarting all Orion services. Choose a time to install SolarWinds NCM 7.x when your IT operation can tolerate a short period of downtime for Orion Platform products.

About the Orion Platform Database

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

The following procedures assume that, if you are integrating NCM with another Orion Platform product, your other product is already installed on the host and has been upgraded to a version compatible with SolarWinds NCM version 7.3.X. These procedures also assume that the hardware of the host on which you install NCM meet the appropriate requirements; see the section on “Requirements” for details.

To install SolarWinds Network Configuration Manager:

1. Login on with a local administrator account to the host on which you want to install NCM.

   Note: To ensure that SolarWinds Network Configuration Manager runs properly, do not install SolarWinds Network Configuration Manager on a domain controller.

2. Navigate to your download location and launch the executable.

3. If you are willing to send us usage statistics, select **Send usage statistics to SolarWinds to help us improve our products**.
4. Accept the License Agreement and click Next.
5. Accept the default target directory (/Program Files/SolarWinds/NCM) for your installation or set another that you prefer.
6. Click Next to start copying files.
7. Click Finish.

   The SolarWinds 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 authentication method (Windows or SQL Server Authentication) used to communicate with the instance, and then click **Next**.

    Notes:

    The SQL Server instance must support SQL authentication or mixed mode.

    If you are using a local instance of SQL Server Express, use the following syntax to use the default instance: `(local)\SQLEXPRESS`.

    If you select SQL Authentication, provide an account with sufficient rights to create new databases on the server instance. For example, specify the SQL administrator (**sa**) account.
11. Select your existing Orion Platform database database, and then click **Next**.
12. Select an existing account with administrator rights on the database, and then click **Next**.

    Note: You must supply a strong password. For more information about strong passwords, see http://msdn.microsoft.com/en-us/library/ms143705.aspx
13. Click Next to setup the website with default settings or adjust the settings as needed.
14. Click Yes if you are informed that a website already exists with the same settings.
15. Click Next after reviewing the settings that will be configured.
16. Click Next after reviewing the overview configuration plan for the Database, Website, and Services.

The dual blue bars show progress and annotations of the wizard's current actions.

17. Click Finish when the wizard completes.

18. ***If you are prompted to license SolarWinds NCM***, click **Enter Licensing Information** and then complete the following procedure to license your SolarWinds NCM installation:

    If you have both an activation key and access to the internet, select the first option, I have internet access and an activation key…, enter your Activation Key, and then click Next.

    Note: ***If you are using a proxy server to access the internet,*** select **I access the internet through a proxy server**, and then provide the **Proxy address** and **Port**.

    If you do not have access to the internet from your designated SolarWinds NCM server, select **This server does not have internet access…**, click **Next**, and then complete the steps provided..

    You need a customer ID and password to successfully install the key. For more information, see the section "Obtaining a Software License Key".

19. Enter registration information, including your name and a valid email address, and click Finish.

    If licensing failed for some reason the software should automatically mark the installation as an evaluation. You will have 30 days to enter valid license information.

    Orion Web Console launches.

20. Enter an appropriate username and password.

    The default credentials are 'admin' with no password.

21. Click DISCOVER MY NETWORK under NCM Nodes to discover the nodes for SolarWinds NCM to manage.

    The software navigates to the Network Sonar Wizard.

22. Review and accept the defaults (public/private) for the SNMP read-only and read-write community strings; or click the pencil icon to edit a credential. Click Next when you are finished.

    These default strings are tried first the software interactively requests a credential during node discovery.

23. Select **Add to NCM** to make the discovered nodes part of the set on which you will perform NCM operations (for example, downloading and uploading configs).

You manage NCM nodes through Nodes resource on the HOME page. For more information, see “Managing NCM Nodes”

24. Click Add New Credential under Windows Credentials as needed.

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

25. Define an IP range, subnet, or a list of specific nodes for the wizard to use in discovering nodes; and click **Next** when you are finished.
26. Review and adjust discovery settings. Click **Ignore nodes…** if you want to ignore nodes that provide no SNMP or WMI information.
27. Click Next when you are finished.
28. Click DISCOVER to start discovering nodes.

    The Discovery Results Wizards opens to report the discovery results.

29. Click Next when you are ready import the devices types discovered.
30. Click Next when you are ready import the volume types discovered.
31. Click Import after you have reviewed and adjusted (as needed) the list of devices and volumes.

    Details and progress of the import operation is shown in real-time in the Import Results window.

32. Click Finish when the import operation is done.

    The software navigates to Discovery Central.

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

    The nodes managed in NCM are the results of the Network Sonar Wizard session just finished. In discovering these nodes, the software has automatically added the nodes to the database.

34. Click CONFIGS in the Orion Web Console to access NCM features.

Preparing to Upgrade SolarWinds Network Configuration Manager

You have two options for upgrading the NCM version 7.3.X software.

Single Server Standalone

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

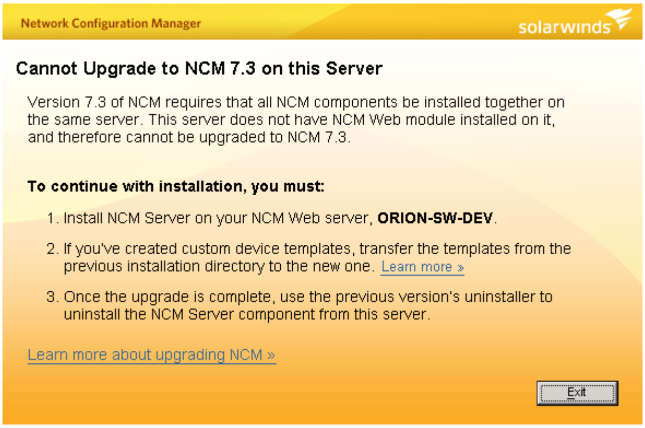
Single Server Integrated

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

Existing Separate Server Deployments

A separate server deployment is not supported with NCM 7.3.X. If you are upgrading an NCM separate server deployment, you must convert to a single server deployment. In an existing separate server standalone deployment, you do that by installing the NCM 7.3.X software on the host where the NCM Web software is currently running (Administrative Tools > Services as "**SolarWinds Orion NCM – NPM integration V7.x.x**").

If you begin upgrade on the current NCM Server host of a separate server deployment, then NCM shows you this screen:



Cannot Upgrade to NCM 7.3 on this Server

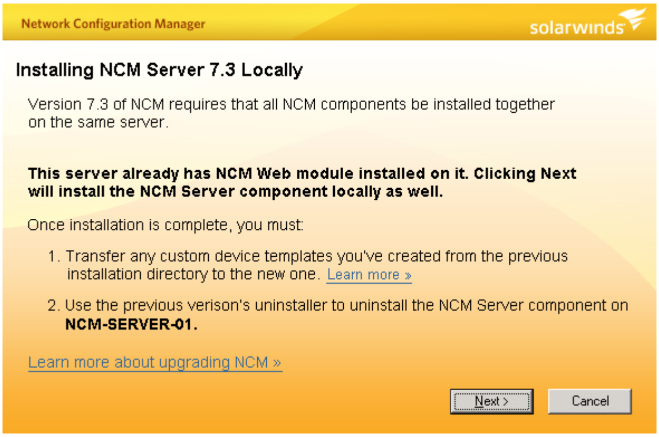
Version 7.3 of NCM requires that all NCM components be installed together on the same server. This server does not have NCM Web module installed on it, and therefore cannot be upgraded to NCM 7.3.

To continue with installation, you must:

1. Install NCM Server on your NCM Web server, **ORION-SW-DEV**.
2. If you've created custom device templates, transfer the templates from the previous installation directory to the new one. Learn more »
3. Once the upgrade is complete, use the previous version's uninstaller to uninstall the NCM Server component from this server.

Learn more about upgrading NCM »

You must exit the NCM Installer and begin the upgrade on the appropriate host; in this case, the software tells you to find the host ORION-SW-DEV. When you are upgrading on the correct host, NCM shows you this screen:



Installing NCM Server 7.3 Locally

Version 7.3 of NCM requires that all NCM components be installed together on the same server.

This server already has NCM Web module installed on it. Clicking Next will install the NCM Server component locally as well.

Once installation is complete, you must:

1. Transfer any custom device templates you've created from the previous installation directory to the new one. Learn more »
2. Use the previous verison's uninstaller to uninstall the NCM Server component on **NCM-SERVER-01.**

Learn more about upgrading NCM »

If you click Next the NCM Installer begins the process of upgrading as covered in the section “Upgrading NCM Software”.

Migrating NCM Data into the Orion Platform Database

Upgrading NCM to version 7.3.X involves migrating NCM data from your existing NCM database into the Orion Platform database that currently holds your node data. The time needed to complete the installation varies depending on how much and what data you are migrating.

Here are the guidelines:

- **Migrating all data (4-6 Hours)**

  This option migrates NCM node data, device inventories, your config archive, and the cache of compliance data. SolarWinds recommends this option.

  Note: NCM installs a standard set of device templates. Even if you select this option, you must move all of your **custom** device templates (%Program Files%\SolarWinds\Orion\NCM\Device Types) from your previous primary to your new NCM server. You can do that before or after migrating NCM data.

- **Do not migrate data that can be re-collected Later (2-4 Hours)**

  This option migrates NCM node data and your config archive. SolarWinds does not recommend this option.

  After this data is migrated, you must make new inventories of your devices.

  Rebuilding the compliance cache occurs automatically each night or when you click “Update All” on the Compliance Reports page.

- **Migrate the minimum amount of data possible (not recommended) (0-2 Hours)**

  This option migrates NCM node data only. Assuming you do not have configs backed up in some other way, you will lose your config data. And after node data is migrated, you must make inventories of your devices. Rebuilding the compliance cache occurs automatically each night or when you click “Update All” on the Compliance Reports page..

Caveats:

1. If you are an existing customer, and your current version does not qualify for a direct upgrade to SolarWinds NCM version 7.3.X, you first need to install the versions of SolarWinds NCM that at least bring your installation to SolarWinds NCM version 7.2.

   For example, if you were running SolarWinds NCM version 6.0, you would need to install SolarWinds NCM versions 7.0 and 7.2 before you can install SolarWinds NCM 7.3.X. Additionally, in this case, should you want to gain access to the latest NCM/NPM integration features, you would need to upgrade your SolarWinds Network Performance Manager software to version 10.7.
2. If you need previous versions of SolarWinds NCM, Contact Customer Service and Support (customerservice@solarwinds.com).

Estimating Free Space on the SQL Server Host

NCM cannot write to its database while it is being merged with the Orion Platform database. Disabling NCM services during the upgrade process prevents this from happening.

Note: SolarWinds strongly recommends that you do not use a SQL Server Express instance as the target for your merged database during NCM version 7.3.X upgrade. If the NCM Installer detects that a SQL Server Express instance that you select for a data migration target does not have sufficient space, the installer forces you to stop the NCM software upgrade process until you have readied an appropriate version of SQL Server software on an available host.

Please keep in mind that, to accommodate merged database, ***you may need as much as twice the size of your current NCM database available*** on the target SQL Server host (where your Orion Platform database currently resides).

NCM estimates the free space needed your Orion Platform database's SQL Server host by discovering and doubling the size of NCM database files on the NCM database SQL Server host.

NCM cannot determine the space available in your Orion Platform database deployment with complete certainty; any estimate would be blind to your actual physical disks available and their storage states. Many environments have a SQL Server host setup to use logical units in a large disk array, for example.

Rather than providing a potentially flawed programmatic estimate, we instead defer to your expertise in using the tools you trust to manage your database environment. As a result, though NCM attempts to detect your free space on the Orion Platform database, you must explicitly confirm the space estimate in order to procede with the database merge operation.

Use a tool you trust to confirm that your Orion Platform database SQL Server host contains the required free space. Keep in mind that different tools give different space information. For example, Properites of a local SQL Server drive may show different available space than SQL Server Management Studio or SolarWinds Orion Database Manager. In a more complex environment, in which you have your SQL Server setup to use logical units of a disk array, you most likely need to use tools related to managing the array to get a reliable estimate of the free space avaible to your Orion Platform database. If you see a big discrepancy among different indications of free space, use the most conservative estimate.

If you discover that you need to free-up space on the Orion Platform database, consider shrinking the Orion Platform database. You can use SQL Server Management Studio or another database management application to do the database shrink operation. Shrinking a large Orion Platform database can take as long as 10-20 minutes.

Orion Platform Products: Integration Support

An Orion Platform product is one whose features and functions can be accessed and managed through the Orion Web Console.

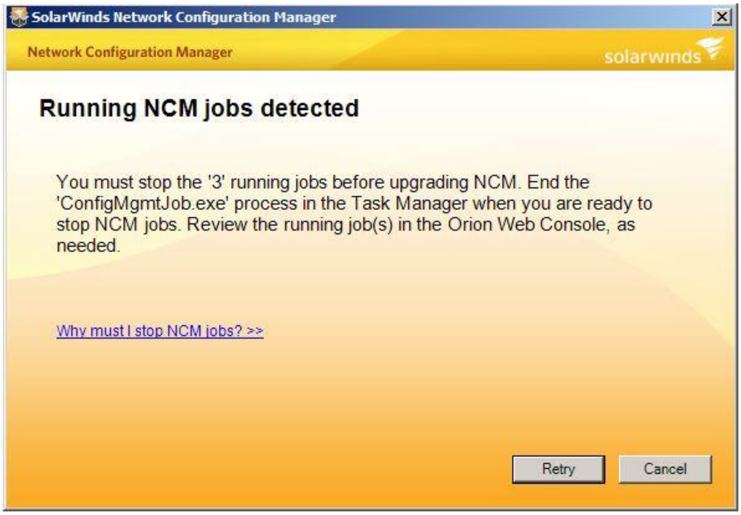
Here is the current list Orion Platform products and version with which SolarWinds NCM version 7.3.X can integrate. You must upgrade to an appropriate version of the other Orion Platform product(s) for NCM integration to function.

- SolarWinds Network Performance ManageSASAMr (NPM) version 10.11
- SolarWinds Server and Application Monitor (SAM) versions 6.0.x, 6.1.x
- EOC: 1.4, 1.5, 1.6
- SolarWinds IP Address Manager (IPAM) version 4.0, 4.1
- SolarWinds User Device Tracker (UDT) version 3.0.x
- SolarWinds IPSLA (VNQM) version 4.0.1, 4.1, 4.2
- Toolset: 10.9, 11.0

Note: Because SolarWinds NCM 7.x shares common components with all Orion Platform products, the process of installing and configuring SolarWinds NCM involves shutting down and restarting all Orion services. Choose a time to install SolarWinds NCM 7.x when your IT operation can tolerate a short period of downtime for Orion Platform products.

Stopping NCM Jobs

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


SolarWinds Network Configuration Manager
Network Configuration Manager
solarwinds

Running NCM jobs detected

You must stop the '3' running jobs before upgrading NCM. End the 'ConfigMgmtJob.exe' process in the Task Manager when you are ready to stop NCM jobs. Review the running job(s) in the Orion Web Console, as needed.

Why must I stop NCM jobs? >>
Retry
Cancel

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

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

To end running NCM jobs:

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

Stopping the SCP Server Tray

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

To end this application:

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

Upgrading NCM Software

In upgrading to NCM version 7.3.X, you cannot preserve an existing deployment of NCM on separate hosts. Assuming you are running such a deployment, and you currently run NCM as integrated with another Orion Platform product, you must convert to a single server deployment by installing the NCM 7.3.X software on the host where the NCM Web (see Administrative Tools > Services > **SolarWinds Orion NCM – NPM integration V7.x.x)** and other Orion Platform product software are currently running. For more information see the section “Existing Separate Server Deployments”.

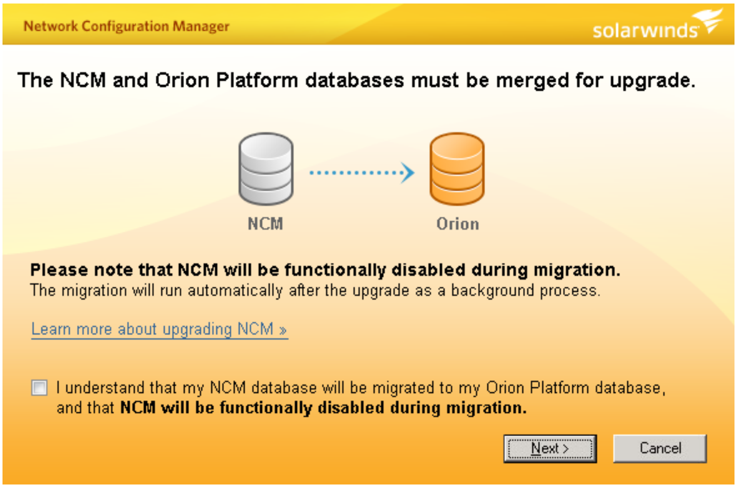
The section assumes that, if you are integrating with another Orion Platform product, your other product is already installed on the host and has been upgraded to a version compatible with SolarWinds NCM version 7.3.X; see “Orion Platform Products: Integration Support” for information on product compatibility.

To upgrade SolarWinds Network Configuration Manager:

1. Using an account with administrator permissions, log in on the computer on which you want to install SolarWinds Network Configuration Manager along with the other Orion Platform product.

   Note: To ensure that SolarWinds Network Configuration Manager runs properly, do not install SolarWinds Network Configuration Manager on a domain controller.

2. Navigate to your download location and launch the executable.



The NCM and Orion Platform databases must be merged for upgrade.

Please note that NCM will be functionally disabled during migration.
The migration will run automatically after the upgrade as a background process.

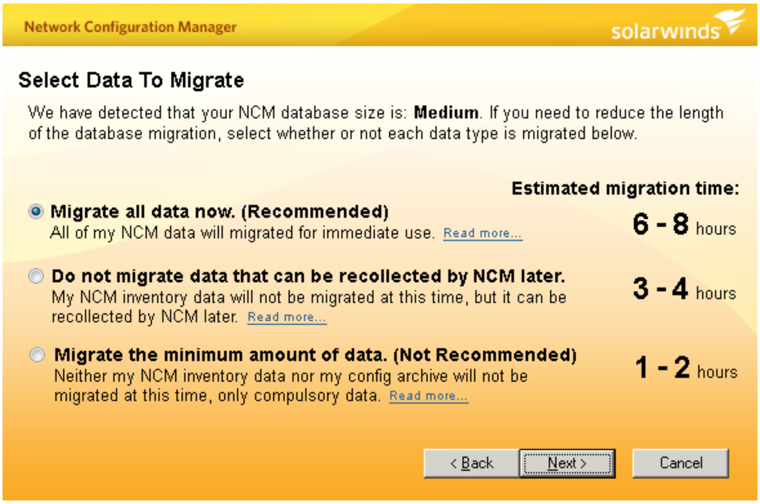
Learn more about upgrading NCM »

□ I understand that my NCM database will be migrated to my Orion Platform database, and that **NCM will be functionally disabled during migration.**

3. When you sufficiently have reviewed the information, select **I understand…** and click Next.

   For more information about upgrading see the subsections under “Preparing to Upgrade SolarWinds Network Configuration Manager”

   The Select Data to Migrate screen appears.



Select Data To Migrate

We have detected that your NCM database size is: **Medium**. If you need to reduce the length of the database migration, select whether or not each data type is migrated below.

Estimated migration time:

● **Migrate all data now. (Recommended)** 6 - 8 hours
All of my NCM data will migrated for immediate use. Read more...

○ **Do not migrate data that can be recollected by NCM later.** 3 - 4 hours
My NCM inventory data will not be migrated at this time, but it can be recollected by NCM later. Read more...

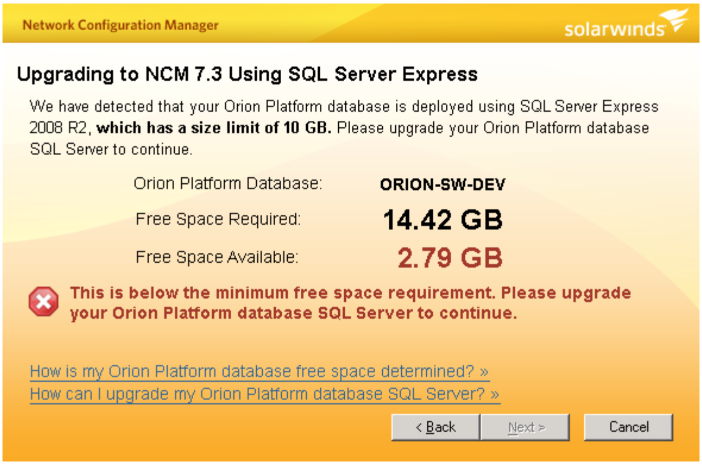
○ **Migrate the minimum amount of data. (Not Recommended)** 1 - 2 hours
Neither my NCM inventory data nor my config archive will not be migrated at this time, only compulsory data. Read more...

4. Select your NCM data migration option and then click Next.

   For more information see the section ”Migrating NCM Data into the Orion Platform Database”.

The Database Free Space Required screen appears with a message that NCM estimates that your Orion Platform database either does or does not have enough space to handle the merging of NCM data into the Orion Platform database.

For more information see “Estimating Free Space on the SQL Server Host”.



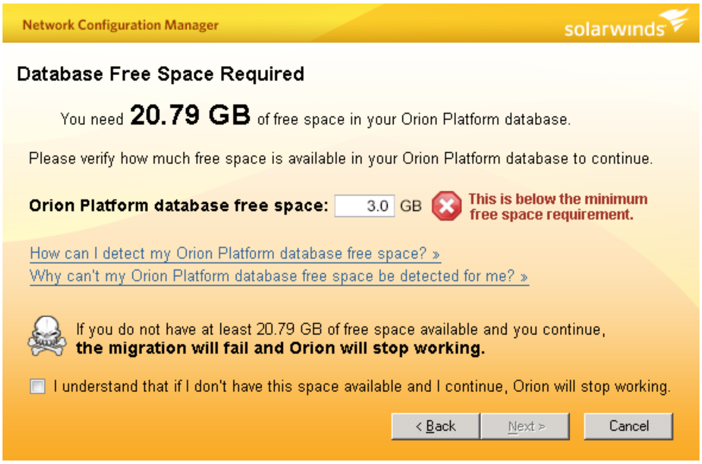
Upgrading to NCM 7.3 Using SQL Server Express

We have detected that your Orion Platform database is deployed using SQL Server Express 2008 R2, **which has a size limit of 10 GB.** Please upgrade your Orion Platform database SQL Server to continue.

Orion Platform Database:	**ORION-SW-DEV**
Free Space Required:	**14.42 GB**
Free Space Available:	**2.79 GB**

This is below the minimum free space requirement. Please upgrade your Orion Platform database SQL Server to continue.

How is my Orion Platform database free space determined? »
How can I upgrade my Orion Platform database SQL Server? »



Database Free Space Required

You need **20.79 GB** of free space in your Orion Platform database.

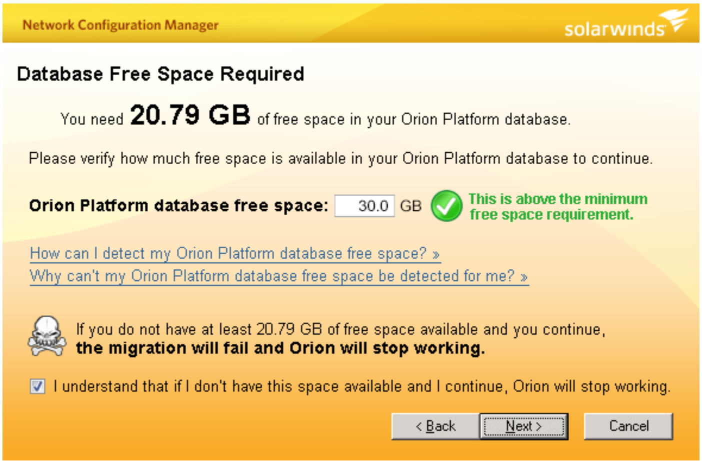
Please verify how much free space is available in your Orion Platform database to continue.

Orion Platform database free space: 3.0 GB **This is below the minimum free space requirement.**

How can I detect my Orion Platform database free space? »
Why can't my Orion Platform database free space be detected for me? »

If you do not have at least 20.79 GB of free space available and you continue, **the migration will fail and Orion will stop working.**

□ I understand that if I don't have this space available and I continue, Orion will stop working.



Database Free Space Required

You need **20.79 GB** of free space in your Orion Platform database.

Please verify how much free space is available in your Orion Platform database to continue.

Orion Platform database free space: 30.0 GB **This is above the minimum free space requirement.**

How can I detect my Orion Platform database free space? »
Why can't my Orion Platform database free space be detected for me? »

If you do not have at least 20.79 GB of free space available and you continue, **the migration will fail and Orion will stop working.**

☑ I understand that if I don't have this space available and I continue, Orion will stop working.

5. When you sufficiently have reviewed the information, and you can proceed with the upgrade, select **I understand…** click Next.

   The Setup Wizard begins your software upgrade.

6. If you are willing to send us usage statistics, select **Send usage statistics to SolarWinds to help us improve our products**.

7. Type **Yes** after creating your database back-up, and then click Next.

   See the section on “Managing and Migrating a Database with SQL Server Management Studio” for detailed information on backing up your database.

8. Accept the license agreement displayed on the License Agreement window, and then click Next.

9. If prompted, accept the default directory for the installation or Browse to another, then click Next.

10. Click Next to have the Setup Wizard start copying files.

    You should see the blue progress bar advancing with annotations of which files are being copied.

11. Click Finish when the Setup Wizard completes its copying.

    The SolarWinds Configuration Wizards starts.

12. In the SolarWinds Configuration Wizard, verify that Database, Website, and Services are selected, and then click Next.

13. Specify the SQL Server instance on which your Orion Platform database is installed.\

    If you do not have credentials to access the Orion Platform database’s SQL Server host, you must consult a system administrator for that host or for the SQL Server instance to obtain an appropriate set of SQL Server credentials.

    Keep in mind that you are upgrading from a version of NCM that has both an Orion Platform database and an NCM database. Those may or may not both reside on the same instance of SQL Server. In this case, you need to identify the SQL Server that hosts your Orion Platform database.

14. Enter the authentication method (Windows or SQL Server Authentication) used to communicate with the SQL Server instance, and then click **Next**.

    Notes:

    The SQL Server instance must support SQL authentication or mixed mode.

If you are using a local instance of SQL Server Express, use the following syntax to use the default instance: `(local)\SQLEXPRESS`.

If you select SQL Authentication, provide an account with sufficient rights to create new databases on the instance. For example, specify the SQL administrator (**sa**) account.

15. Select the appropriate existing Orion Platform database and then click **Next**..
16. Select an account (with administrator rights) on the database you selected, and then click **Next**.

    Note: You must supply a strong password. For more information about strong passwords, see http://msdn.microsoft.com/en-us/library/ms143705.aspx
17. Click Next to setup the website with default settings or adjust the settings as needed.
18. Click Yes if you are informed that a website already exists with the same settings.
19. Click Next after reviewing the settings that will be configured.
20. Click Next after reviewing the overview configuration plan for the database, website, and services.

    The dual blue bars show progress and annotations of the wizard's current actions.
21. Click Finish when the wizard completes.
22. ***If you are prompted to license SolarWinds NCM, click Enter* Licensing Information** and then complete the following procedure to license your SolarWinds NCM installation:

    If you have both an activation key and access to the internet, select the first option, **I** have internet access and an activation key…, enter your Activation Key, and then click Next.

    Note: ***If you are using a proxy server to access the internet,*** select **I access the internet through a proxy server**, and then provide the **Proxy address** and **Port**.

    If you do not have access to the internet from your designated SolarWinds NCM server, select **This server does not have internet access…**, click **Next**, and then complete the steps provided..

    You need a customer ID and password to successfully install the key. For more information, see the section "Obtaining a Software License Key".

23. Enter registration information, including your name and a valid email address, and click Finish.

    If licensing failed for some reason the software should automatically mark the installation as an evaluation. You will have 30 days to enter valid license information.

    Orion Web Console launches.

24. Enter an appropriate username and password.

    The default credentials are ‘admin’ with no password.

25. Click CONFIGS in the Orion Web Console toolbar.

    The banner displays a status message about the database migration. Though you cannot use NCM features while the migration is underway, Orion Platform services and services related to other Orion Platform products run normally.

Additional Polling Engine and Web Console

According to your needs in managing the devices in your network 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 back-up of device configs.

Installing an Additional Poller

If you are upgrading to SolarWinds NCM 7.3.X, before you attempt to install an additional poller on another host, you must first upgrade the NCM Server software . Consult the section “Preparing to Upgrade SolarWinds Network Configuration Manager” for details on upgrading to NCM version 7.3.X.

There is no distinction between the Orion Platform poller and the NCM poller in NCM version 7.3.X. All pollers perform NCM operations-- updating inventory, downloading and uploading configs, executing scripts, scheduling jobs—in addition to all normal node monitoring operations the Orion Platform performs on its (sub)set of managed nodes.

As a capacity planning guideline, if you divide managed nodes among the main poller and additional pollers, then you should expect each poller to handle all relevant node-polling, NCM-related work (scheduled config downloads, etc.), and other work related to the Orion Platform modules (NPM, NTA, etc.) installed on the additional polling host.

Also, as part of setting up additional pollers in your environment, so that device templates are available on the relevant poller hosts, you must install the NCM Additional Poller software on each additional poller host. You may also need to open firewall ports on the additional poller hosts to enable the NCM software to operate successfully.

To upgrade your additional NCM poller:

1. Launch the executable (SolarWinds-Orion_AdditionalPoller.exe) from the location where you downloaded it on the server that will host your additional poller.
2. Visit the Customer Portal to obtain the file if you do not already have it.
3. Click Next on the Welcome screen.
4. Click to accept the end user agreement, then click Next.
5. Click Next to accept the default installation directory or use Browse to adjust it.
6. Click Next to start copying files.

   The software copies the files, including the Orion Platform components needed for your server to communicate with the main poller.

7. Click Finish when the files are finished being copied.

8. If you are prompted to license the additional poller, click Enter Licensing Information and then complete the following procedure to license your installation:

   a. If you have both an activation key and access to the internet, select the first option, I have internet access and an activation key…, enter your Activation Key, and then click Next.

   Note: If you are using a proxy server to access the internet, select I access the internet through a proxy server, and then provide the Proxy address and Port.

   b. If you do not have access to the internet from your designated SolarWinds NCM additional poller host server, select This server does not have internet access…, click Next, and then complete the steps provided..

   You need a customer ID and password to successfully install the key. For more information, see the section “Obtaining a Software License Key”.

9. Review the Welcome text, click Next.

10. Specify the SQL Server instance—where the Orion Platform database is located—and enter the authentication method (Windows or SQL Server Authentication) used to communicate with the instance. Click Next when you are ready.

    The SQL Server instance must support SQL authentication or mixed mode.

    Notes:

    If you are using a local instance of SQL Server Express, use the following syntax to use the default instance: (local)\SQLEXPRESS.

    If you select SQL Authentication, provide an account with sufficient rights to create new databases on the server instance. For example, specify the SQL administrator (sa) account.

11. Click Use an existing database, select the Orion Platform database in the dropdown list, and then click Next.

12. Click Use and existing account and select the account credentials from the dropdown list. Click Next when you are ready.

13. Click Next after reviewing the services to install.

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

15. Click Next after reviewing the Database and Services to be configured.

16. The green progress bars and descriptive text explain what is being done and how far along it is.
17. Click Launch Orion Web and Finish to complete configuration and bring up the website on your additional poller.

Installing an Additional Website

If you are upgrading to SolarWinds NCM 7.3.X, before you attempt to install an additional website on another host, you must first upgrade the NCM Server software . Consult the section “Preparing to Upgrade SolarWinds Network Configuration Manager” for details on upgrading to NCM version 7.3.X.

Follow the steps in this section to install or upgrade your additional website.

To upgrade your additional NCM website:

1. Launch the executable (SolarWinds-Orion_WebOnly.exe) from the location where you downloaded it on the server that will host your additional poller.
2. Visit the Customer Portal to obtain the file if you do not already have it.
3. Enter the hostname or IP address and the Orion administrator credentials of your NCM Server host in the Orion Compatibility Checker.
4. Click Next on the Welcome screen.
5. Click I accept… and Next to accept the License Agreement.
6. Click Next to accept the default location for installing the files or first use Browse to adjust the location.
7. Click Next to start copying files.
8. The software copies the files, including the Orion Platform components needed for your server to communicate with the NCM Server host.
9. Click Finish when the files are finished being copied.
10. When you are prompted to license the additional poller, click Enter Licensing Information and then complete the following procedure to license your installation:

    a. If you have both an activation key and access to the internet, select the first option, I have internet access and an activation key…, enter your Activation Key, and then click Next.

    Note: If you are using a proxy server to access the internet, select I access the internet through a proxy server, and then provide the Proxy address and Port.

b. If you do not have access to the internet from your designated SolarWinds NCM additional poller host server, select This server does not have internet access…, click Next, and then complete the steps provided..

You need a customer ID and password to successfully install the key. For more information, see the section “Obtaining a Software License Key”.

11. Click Next on the Welcome screen of the SolarWinds Configuration Wizard.
12. Specify the SQL Server instance—where the Orion Platform database is located—and enter the authentication method (Windows or SQL Server Authentication) used to communicate with the instance. Click Next when you are ready.

    The SQL Server instance must support SQL authentication or mixed mode.

    Notes:

    If you are using a local instance of SQL Server Express, use the following syntax to use the default instance: (local)\SQLEXPRESS.

    If you select SQL Authentication, provide an account with sufficient rights to create new databases on the server instance. For example, specify the SQL administrator (sa) account.
13. Click Use an existing database, select the Orion Platform database in the dropdown list, and then click Next.
14. Click Use and existing account and select the account credentials from the dropdown list. Click Next when you are ready.
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 Next after reviewing the services to install.
18. Click Next after reviewing the Database, Website, and Services to be configured.

    The green progress bars and descriptive text explain what is being done and how far along it is.
19. Click Launch Orion Web and Finish to complete configuration and bring up the Orion Web Console.

Limiting NCM Resource Consumption

Since NCM and other Orion Platform products use the same database, you may want to adjust NCM settings to reduce potential contention for CPU cycles on the Orion Platform server host and for data processing requests on the SQL Server host where the Orion Platform dataase resides.

Here is a table of NCM components and their characteristic use of CPU and SQL Server resources.

Functional Area	Resource Impact	Risk	Start Type	Configurable	Resource Consumption Strategy
Compliance cache	CPU, DB		Manual, Schedule	N	Schedule off peak and increase interval.
Config transfer	CPU	CPU pinning.	Manual, Schedule	Y	Decrease simultaneous transfers.
Device Inventory	CPU, DB		Manual, Schedule	Y	Decrease simultaneous inventories.
FTS index update	DB		Schedule	Y	Increase update interval or disable.
Jobs	CPU, DB	Multiple jobs may consume all resources.	Manual, Schedule	N	Avoid run-time overlapping.
Purge configs	DB	Executes complex SQL script.	Manual, Schedule	N	Schedule off peak and increase interval.
Reports	DB	Executes complex SQL script.	Manual, Schedule	N	Schedule off peak and increase interval.

Repairing SolarWinds Network Configuration Manager

If your installation is behaving abnormally, you can repair it by launching the SolarWinds Configuration Wizard. Start it from the SolarWinds Orion program group in the Start menu.

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

To repair SolarWinds Network Configuration Manager:

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

   The SQL Server instance must support SQL authentication or mixed mode.

   Notes:

   If you are using a local instance of SQL Server Express, use the following syntax to use the default instance: (local)\SQLEXPRESS.

   If you select SQL Authentication, provide an account with sufficient rights to create new databases on the server instance. For example, specify the SQL administrator (sa) account.
4. Select the appropriate existing Orion Platform database, and then click Next.
5. Select a appropriate existing account for the database.

   Note: You must supply a strong password. For more information about strong passwords, see http://msdn.microsoft.com/en-us/library/ms143705.aspx.
6. Click Next. I
7. Review the services the wizard will install, and then click Next
8. Read the summary of what the configuration wizard will configure, and then click Next.
9. Review the Configuration Summary as needed, and then click Finish.

Removing SolarWinds Network Configuration Manager

If for whatever reason you need to remove SolarWinds NCM from a server, you must remove both SolarWinds Orion Network Configuration Manager and SolarWinds Orion NCM-NPM Integration.Failing to remove both component will result in a failure to installl and configure another version of NCM on the server whenever you might you choose to do that.

To remove SolarWinds Network Configuration Manager:

1. Open Add and Remove Programs in Windows.
2. Select SolarWinds Orion Network Configuration Manager and click Remove.
3. If you have integrated NCM with NPM, select SolarWinds Orion NCM-NPM Integration and click Remove.
4. Reboot the server.

Using SSL Communication with SolarWinds NCM

SolarWinds NCM supports the use of Secure Sockets Layer certificates to enable secure communications with the Orion Web Console.

Notes:

- Secure SSL communications are conducted over port 443.
- The following procedure does not detail the process of either obtaining a required certificate or generating a certificate signing request for a third-party certificate authority. It is assumed that the required SSL certificate has already been installed on your SolarWinds NCM server. For more information about acquiring and installing a required server certificate for SSL communications, see http://support.microsoft.com/kb/298805, from which this procedure was adapted.

The following procedures enable SSL connections to the Orion Web Console.

To enforce SSL connections to the Orion Web Console:

1. Login on as an administrator to your SolarWinds NCM Server host.
2. Click Start > Control Panel > Administrative Tools > Computer Management.
3. Expand Services and Applications > Internet Information Services (IIS) Manager > Web Sites.
4. Right click SolarWinds NetPerfMon, then click Properties.

5. Click the Web Site tab.
6. Confirm that SSL port is set to 443, and then click Apply.
7. Click Advanced.
8. If the Multiple SSL identities for this Web site field does not list the IP address for the Orion Web Console with SSL port 443, complete the following steps:

   a. Click Add, and then select the IP address of the Orion Web Console.

   Note: As it was set initially in the Configuration Wizard, this option is usually set to (All Unassigned). If the IP address of the Orion Web Console was not initially set to (All Unassigned), select the actual, configured IP address of the Orion Web Console.

   b. Type 443 as the TCP port, and then click OK.
9. Click the Directory Security tab.
10. Click Edit in the Secure communications section.
11. Select Require secure channel (SSL), and then click OK.
12. Click Apply, and then click OK to exit.

Setting Node Communication Defaults

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

On the Global Device Defaults page (Settings > NCM Settings > Global Device Defaults), the settings you enter under **Device Login Information**, **Communication Transfer Protocol**, and **Transfer Ports** are treated as values for global macros that apply to all managed devices when you select **Reset all devices to use Global Settings** beside a category of settings.

Note: NCM supports SNMPv3 with AES-256.

To set node communication default parameters:

1. Open the Orion Web Console.
2. Click Settings > NCM Settings.
3. Navigate to and expand Global Device Defaults.
4. Enter and confirm credentials under Device Login Information.
5. Enable Level and Enable Password set the level of permission at which the entered password is valid.
6. Select the desired protocol for transfer operations.

These settings apply to command/script, config request, and config transfer operations. TELNET is the default.

The available protocol options are: TELNET, SSH1, SSH2, and SSHAuto.

Select the port the Telnet (default: 23) and SSH (default: 22) will use.

7. Click Submit.

To override default settings for a particular node:

1. Login to the Orion Web Console.
2. Click Settings.
3. Click Manage Nodes under Node & Group Management.
4. Use the Group by list to organize the node list.
5. Select the relevant node in the list.
6. Click Edit Properties.
7. Scroll down to NCM Properties.
8. Edit the login and communication information.
9. Click Submit.

Using Multiple Connection Profiles

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

To create or edit a connection profile:

1. Open NCM Settings (Settings > NCM Setttings) in the Orion Web Console.
2. If you want to create a new connection profile, click Create New.
3. If you want to edit an existing connection profile, select the profile and click Edit.
4. Enter the appropriate values.
5. Clcik Submit when you are finished.

The settings you enter fall into the categories of **Device Login Information**, **Communication Transfer Protocol**, and **Transfer Ports** are treated as values for any node to which you apply the connection profile.

Device Login Information

Enter the Username, Password, Enable Level and Enable Password to set the level of permission at which access to the device is valid for this connection profile.

Communication Transfer Protocol
You can select a different protocol for command/script, config request, and config transfer operations. The available protocol options are: TELNET, SSH1, SSH2, and SSHAuto.

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

Setting Communication Limits

As part of setting up communication defaults you can define timeout values and retry number for ICMP, SNMP, Telnet, and SSH communication.

To set communication timeouts and retries :

1. Open the Orion Web Console.
2. Click Settings > NCM Settings.
3. Click Protocol Settings under Network.
4. Enter timeout settings for each protocol.
5. ICMP has a default timeout of 2500 milliseconds.

   Enter the data portion of the ICMP packet. The default is SolarWinds Network Configuration Manager Version 7.1.

   SNMP has a default timeout of 1000 milliseconds with 1 retry.

   Telnet/SSH both have default connection timeouts of 45 seconds and prompt timeouts of 15 seconds.
6. Click Submit.

Configuring Event Logging

Logging events associated with a specific function of SolarWinds Network Configuration Manager allows you to keep a detailed record of events and helps you troubleshoot any anomalies you may encounter.

A number of functional areas within SolarWinds NCM provide verbose logging options, including the following:

Scheduled Jobs

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

Inventory Monitor

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

Database Updates

Logs database events, including backup and connectivity events.

Real-time Config Change Detection

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

Security

Logs security events, including login failures, account modifications, and global security setting changes.

To enable logging for SolarWinds Network Configuration Manager events:

1. Open Orion Web Console.
2. Click Settings > NCM Settings.
3. Click Advanced .
4. Select all log types for which you want to keep verbose log information.

   Such information aids in trouble-shooting a problem with NCM..

   Note: Logs are stored in the Logging folder found in your installation directory. By default, the Logging folder can be found in \Program Files\SolarWinds\Configuration Management\Logging\
5. If you want to trouble communication node by node, click Enable Session Tracing to create a log file of each telnet session.
6. When you are finished making selections, click Submit.

Moving SolarWinds Network Configuration Manager

These procedures assume that you have already upgraded to NCM 7.3.X and have decided to move the NCM software from an existing host to another host.

To move SolarWinds Network Configuration Manager:

1. Using an account with administrator permissions, log in on the computer on which SolarWinds Network Configuration Manager is installed.

   Note: To ensure that SolarWinds Network Configuration Manager runs properly, do not install SolarWinds Network Configuration Manager on a domain controller.

2. Navigate to your download location and launch the executable.
3. If you are willing to send us usage statistics, select **Send usage statistics to SolarWinds to help us improve our products**.
4. Type **Yes** after creating your database back-up, and then click Next.

   See the section on “Managing and Migrating a Database with SQL Server Management Studio” for detailed information on backing up your database.

5. Run License Manager to reset your current license, making it available for your new implementation.
6. Using an account with administrator permissions, log in on the computer to which you want to move SolarWinds Network Configuration Manager.
7. Accept the license agreement displayed on the License Agreement window, and then click Next.
8. If prompted, accept the default directory for the installation or Browse to another, then click Next.
9. Click Next to have the Setup Wizard start copying files.

   You should see the blue progress bar advancing with annotations of which files are being copied.

10. Click Finish when the Setup Wizard completes its copying.

    The SolarWinds Configuration Wizards starts.

11. In the SolarWinds Configuration Wizard, verify that Database, Website, and Services are selected, and then click Next.
12. Specify the SQL Server instance on which your Orion Platform database is installed.
13. Enter the authentication method (Windows or SQL Server Authentication) used to communicate with the SQL Server instance, and then click **Next**.

    Notes:

    The SQL Server instance must support SQL authentication or mixed mode.

    If you are using a local instance of SQL Server Express, use the following syntax to use the default instance: `(local)\SQLEXPRESS`.

If you select SQL Authentication, provide an account with sufficient rights to create new databases on the instance. For example, specify the SQL administrator (**sa**) account.

14. Select the appropriate existing Orion Platform database and then click **Next**.
15. Select an account (with administrator rights) on the database you selected, and then click **Next.**

    Note: You must supply a strong password. For more information about strong passwords, see http://msdn.microsoft.com/en-us/library/ms143705.aspx
16. Click Next to setup the website with default settings or adjust the settings as needed.
17. Click Yes if you are informed that a website already exists with the same settings.
18. Click Next after reviewing the settings that will be configured.
19. Click Next after reviewing the overview configuration plan for the database, website, and services.

    The dual blue bars show progress and annotations of the wizard's current actions.
20. Click Finish when the wizard completes.
21. ***If you are prompted to license SolarWinds NCM***, click **Enter Licensing Information** and then complete the following procedure to license your SolarWinds NCM installation:

    If you have both an activation key and access to the internet, select the first option, I have internet access and an activation key…, enter your Activation Key, and then click Next.

    Note: ***If you are using a proxy server to access the internet,*** select **I access the internet through a proxy server**, and then provide the **Proxy address** and **Port**.

    If you do not have access to the internet from your designated SolarWinds NCM server, select **This server does not have internet access…**, click **Next**, and then complete the steps provided..

    You need a customer ID and password to successfully install the key. For more information, see the section "Obtaining a Software License Key".
22. Enter registration information, including your name and a valid email address, and click Finish.

If licensing failed for some reason the software should automatically mark the installation as an evaluation. You will have 30 days to enter valid license information.

Orion Web Console launches.

23. Enter an appropriate username and password.

    The default credentials are ‘admin’ with no password.

24. Click CONFIGS in the Orion Web Console toolbar.

Moving Reports

If you have created any custom reports, it will be necessary to copy them to the new computer. Complete the following procedure to move your reports.

To move reports to new hardware:

1. Login on the old computer.
2. Copy the files in the Reports folder. By default, this folder is located at C:\Program Files\SolarWinds\Orion\NCM.
3. Paste the files into the Reports folder on the new server. By default, this folder is located at C:\Program Files\SolarWinds\Orion\NCM.

Moving Device Command Templates

If you have created any custom device command templates, it will be necessary to copy them to the new computer. Complete the following procedure to move your templates.

To move device command templates to new hardware:

1. Login on the old computer.
2. Copy the files in the DeviceTypes folder. By default, this folder is located at C:\Program Files\SolarWinds\Orion\NCM.
3. Paste the files into the DeviceTypes folder on the new server. By default, this folder is located at C:\Program Files\SolarWinds\Orion\NCM.

Requirements

The requirements for SolarWinds Network Configuration Manager vary based on a number of factors, including the following:

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

The following table provides the general requirements for an SolarWinds Network Configuration Manager installation.

<table>
<tr><th>Software/Hardware</th><th colspan="2">Requirements</th></tr>
<tr><td>Operating System</td><td colspan="2">Windows 2003 Server SP2 (32-bit and 64-bit) including R2 SP2, and with IIS installed and running in 32-bit mode.
Windows 2008 Server Enterprise or Standard (32-bit or 64-bit) including R2, with IIS installed and running in 32-bit mode, and Server 2008 R2 SP1
Windows Server 2012
SolarWinds supports installing NCM on operating systems setup in these languages: English, German, Japanese, and Simplified Chinese.
NCM does not support using locales outside the group of supported operating system languages.
For evaluation purposes only:
Windows 7, Windows 7 SP1, and Windows 8
<b>Note:</b> SolarWinds does not support installation of SolarWinds NCM on a Windows Domain Controller.</td></tr>
<tr><td rowspan="3">SolarWinds NCM Server Hardware</td><td>CPU Speed</td><td>3GHz dual core dual processor</td></tr>
<tr><td>Memory</td><td>3GB</td></tr>
<tr><td>Hard Drive Space</td><td>30GB
<b>Note</b>: This version of NCM holds a searchable config index on local disk that adds 6-10GB additional disk space to the previous requirement.</td></tr>
<tr><td>Installing Windows Account</td><td colspan="2">Requires administrator permission on the target server</td></tr>
<tr><td>File System Access Permissions</td><td colspan="2">Ensure the Network Service account has modify access to the system temp directory (<code>%systemroot%\temp</code>).</td></tr>
<tr><td>SolarWinds Orion Syslog Server</td><td colspan="2">If you want real-time change detection triggered through devices sending Syslog messages, the executable must have read-write access to the Orion Platform database. For more information, see “Enabling Real-time Configuration Change Detection” and “Monitoring SNMP”.</td></tr>
</table>

Software/Hardware	Requirements
SolarWinds Orion Trap Service	If you want real-time change detection triggered through devices sending SNMP traps, the executable must have read-write access to the Orion Platform database. For more information, see “Enabling Real-time Configuration Change Detection” and “Monitoring SNMP”.
Microsoft SNMP Trap Service	Must be installed if you want real-time change detection triggered through devices sending SNMP traps. For more information, see “Enabling Real-time Configuration Change Detection” and “Monitoring SNMP” in the SolarWinds NCM Administrator Guide.
Microsoft IIS	Version 6 or later. DNS specifications require hostnames to be composed of alphanumeric characters (A-Z, 0-9), the minus sign (-), and periods (.). Underscore characters (_) are not allowed. For more information, see *RFC 952*. **Note:** 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.
Microsoft ASP .NET 2.0 Ajax Extension	Version 1 or later (if this is not found on the target computer, the setup program downloads and installs the component)
Microsoft .NET Framework	Versions 3.5 SP1 and 4.0 (if these are not found on the target computer, the setup program downloads and installs them)
Database	**Note**: You must create the SolarWinds Orion Platform database with the SolarWinds Configuration Wizard. Creating the database in another way is not supported. SolarWinds supports using NCM with database servers setup in these languages: English, German, Japanese, and Chinese; but only supports storing characters in the UTF8 set. The following database servers are supported as the SolarWinds Network Configuration Manager datastore: • SQL Server 2012 with/without SP1 Standard or Enterprise • SQL 2008 R2 without SP, 2008 R2 SP1, 2008 R2 SP2 • SQL 2008 without SP, 2008 SP1, 2008 SP2, 2008 SP3 • SQL Server 2005 SP1, 2005 SP2, 2005 SP3, 2005 SP4 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 Your database server must support mixed-mode authentication or SQL authentication and have the following protocols enabled: • Shared memory

Software/Hardware	Requirements
	• TCP/IP • Named Pipes SQL Server 2005 Express Edition does not enable these protocols. The following x86 components must be installed (if the components are not found on the target computer, the setup program downloads and installs the components): • SQL Server System Common Language Runtime (CLR) Types • Microsoft SQL Server Native Client • Microsoft SQL Server Management Objects
Ports	The following ports that may be needed for Orion Web Console and depending on how Orion NCM is setup to download and upload configurations. • 20: FTP data transfer • 21: FTP control (setup/teardown) • 22: SSH/SCP default for NCM to transfer configs • 23: TELNET default for NCM to transfer configs • 25: SMTP email default that NCM uses for notifications • 25: SSL/TLS for email alert actions should be enabled on it • 69: TFTP server listens on it • 80: HTTP default for Orion Web Console • 161: SNMP statistics collection, NCM's default for polling • 162: UDP trap messages listened for and received by Trap Server • 514: UDP Syslog messages arrive for Orion Syslog Service • 17777 – SolarWinds Information Service for Orion Web Console • 17778 – SolarWinds Information Service for Orion Web Console • 17779 – SolarWinds Information Service for Orion Web Console • 1801: TCP used for MSMQ WCF binding (More information: http://support.microsoft.com/kb/183293)

Software/Hardware	Requirements
Browser	To access the SolarWinds Network Configuration Manager website, use one of the following browsers: • Microsoft Internet Explorer 7, 8, 9, 10 standard mobile views • Mozilla Firefox 10.0.9, 16.0.2 • Google Chrome v22.0.1229.96**,** 23.0.1271.64

Notes:

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

Scalability

NCM 7.X was tested for scalability in a standalone deployment of three servers: One server hosts the main NCM server and the other two servers each host an NCM additional polling engine. The main NCM server manages up to 10K NCM nodes, as do each NCM additional polling engine. The deployment therefore supports up to 30K nodes total.

And while using the Orion Web Console in a normal way, with the Orion Platform on the main NCM polling for node status at the default rate, this tested deployment supports 2 NCM operations (inventory update, configuration download) being performed per day on all 30K nodes.

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

Server Sizing

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

Should scalability issues arise, consider adjusting the following variables:

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

In larger environments, inventory jobs may run longer than expected. To remedy this situation, consider breaking large inventory jobs into smaller jobs that do not include as many nodes and spacing these jobs over a larger period of time. Adjusting server CPU and memory will enhance user interface performance and job execution speed.

Licensing SolarWinds Network Configuration Manager

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

The following list provides the different types of SolarWinds Network Configuration Manager licenses available

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

Obtaining a Software License Key

If you are prompted for your name, email address, phone number, customer ID, and password, complete the following procedure.

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

To license your product:

1. From the appropriate server in your deployment, navigate to http://www.solarwinds.com/customerportal and enter the requested information to obtain your Activation Key.

   4. ***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 you are integrating SolarWinds NCM on one machine with SolarWinds NPM on another, you would install your SolarWinds NCM license on the machine that is hosting SolarWinds NPM.

   5. ***If you are deploying SolarWinds NCM standalone or on a single integrated server***, then you must install the SolarWinds NCM license on that server.

2. ***If you have both an activation key and access to the internet*****,** select the first option, **I have internet access and an activation key…**, enter your **Activation Key**, and then click Next.

   Note: ***If you are using a proxy server to access the internet,*** select **I access the internet through a proxy server**, and then provide the **Proxy address** and **Port**.

3. ***If you do not have access to the internet from your designated SolarWinds NCM server,*** select **This server does not have internet access…**, click **Next**, and then complete the steps provided.

Reviewing Your License

You can review the licenses associated with your NCM server at any time from the Orion Web Console.

To review SolarWinds license details:

1. Open the Orion Web Console.
2. Click **Settings**.
3. Click **NCM Settings**.
4. Click **Node Licensing**.

Resetting Your License

You can easily install the SolarWinds License Manager, a free utility that gives you the ability to easily migrate Orion licenses from one computer to another without contacting SolarWinds Customer Service.

Note: You must install License Manager on a computer with the correct time. If the time on the computer is off 5 minutes, in either direction, from Greenwich Mean Time, you will be unable to reset licenses. Time zone settings do not affect and do not cause this issue.

Installing License Manager

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

To install License Manager:

1. Click **Start > All Programs > SolarWinds > SolarWinds License Manager Setup**.
2. Click **I Accept** to accept the SolarWinds EULA.
3. Click **Install**. After installation completes, the program launches.

Using License Manager

You must run License Manager on the computer where the currently licensed SolarWinds product is installed.

To deactivate currently installed licenses:

1. Click **Start > All Programs > SolarWinds > SolarWinds License Manager**.

2. Select the products you want to deactivate on this computer.
3. Click **Deactivate**.
4. Specify your SolarWinds Customer ID and password when prompted, and then click **Deactivate**.

   Note: Deactivated licenses are now available for activation on a new computer.

When you have successfully deactivated your products, Login on the computer on which you want to install your products and begin the installation procedure. When asked to specify your licenses, provide the appropriate information. The license you deactivated earlier is assigned to the new installation.

Warnings:

- The following characters cannot be included in the database name: asterisk (*), closing square bracket (]), colon (:), semicolon (;), single quote ('), double quote ("), backward slash (\), forward slash (/), less than (<), greater than (>), and question mark (?).
- Do not include the single quote (') or the semicolon (;) in the username or password of the database account.

SNMP Communication

SolarWinds Network Configuration Manager takes advantage of SNMP communication to collect inventory information. Ensure all devices from which you want to collect detailed information have SNMP properly configured.

Chapter 3

Managing Nodes

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

- Adding Nodes
- Managing NCM Nodes **Error! Reference source not found.**
- Using the Network Sonar Discovery Results Wizard
- Unmanaging and Remanaging Nodes
- Managing End of Support and End of Sales (EOS)**Error! Reference source not found.**

Adding Nodes

You can add nodes using the SolarWinds Network Sonar, add them individually, or import a list of IP addresses or hostnames from a file. The following sections guide you through these methods:

- Adding Nodes with the Network Sonar Discovery
- Adding an Individual Node
- Managing NCM Nodes
- Using the Network Sonar Discovery Results Wizard

Adding Nodes with the Network Sonar Discovery

SolarWinds Network Sonar Discovery is a high performance network discovery engine that allows you to build a database of the structure and devices found in your TCP/IP network.

In discovering nodes, the Network Discovery Sonar software identifies network devices to manage within the Orion Platform database. Use the **Add to NCM** checkbox if you want to add discovered nodes to NCM. Otherwise, after discovery is done, you will need to manually select the nodes in the Network Sonar Discovery Results Wizard that you want NCM to manage.

For more information on importing the results of your discovery, see “Using the Network Sonar Discovery Results Wizard”.

Caveat:

If you discover more nodes than your NCM license limit, and you import all of them through the Network Sonar Discovery Results Wizard, then the software will import only as many nodes into the database as you have licenses available; and when the license limit is reached, the software will generate an error informing you that all nodes were not added. The result in this case is that some of the nodes managed in NCM may not be the nodes on which you want to perform NCM actions.

There are two ways to address this issue. You can simply take care to select nodes for importing into the database only those nodes you want to manage in NCM. To do this follow the steps in “Using the Network Sonar Discovery Results Wizard”.

As an alternative, you can turn off the option to automatically manage discovered nodes in NCM.

To discover nodes:

1. Login on Orion Web Console.
2. Click Settings.
3. Click Network Sonar Discovery under Getting Started with Orion.
4. If you want to create a new discovery, click Add New Discovery, click Add New Discovery.
5. If you have already defined a network discovery, a number of options are available on the Network Sonar Discovery tab. Select one of the following:

- ***If you want to edit an existing discovery before using it,*** select the discovery you want to edit, and then click **Edit**.
- ***If you want to use an existing discovery to rediscover your network,*** select the discovery you want to use, click **Discover Now**, and then complete the Network Sonar Results Wizard after discovery completes. For more information about network discovery results, see “Using the Network Sonar Discovery Results Wizard”.
- ***If you want to import some or all devices found in a defined discovery that you may not have already imported for monitoring,*** select a currently defined discovery, and then click **Import All Results**. For more information about network discovery results, see “Using the Network Sonar Discovery Results Wizard”.
- ***If you want to import any newly enabled devices matching a defined discovery profile,*** select a currently defined discovery, and then click **Import New Results**. For more information about network discovery results, see “Using the Network Sonar Discovery Results Wizard”.
- ***If you want to delete an existing discovery profile,*** select a currently defined discovery and then click **Delete**.

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

   Notes:

   Repeat the following procedure for each new community string. To speed up discovery, highlight the most commonly used community strings on your network, and then use the arrows to move them to the top of the list.

   NCM supports SNMPv3 with AES-256.

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

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

c. If you are adding an SNMPv3 credential, provide the following information for the new credential:

d. User Name, Context, and Authentication Method

e. Authentication Password/Key, Privacy/Encryption Method and Password/Key, if required.

f. Click Add.

8. Click Next on the SNMP Credentials view.
9. Select **Add to NCM** to make the discovered nodes part of the set on which you will perform NCM operations (for example, downloading and uploading configs).

   You manage NCM nodes through Nodes resource on the HOME page. For more information, see “Managing NCM Nodes”
10. If you want to add Windows credentials for WMI collections, click Add New Credential.:

a. Choose a credential.

b. Name the credential.

c. Enter the relevant user name (with privileges to accomplish WMI polling).

d. Enter and confirm the user account password.

e. Click Add.

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

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

a. Click IP Ranges in the Selection Method menu, and then, for each IP range, provide both a Start address and an End address.

b. Note: Scheduled discovery profiles should not use IP address ranges that include nodes with dynamically assigned IP addresses (DHCP).

c. If you want to add another range, click Add More, and then repeat the previous step.

d. Note: If you have multiple ranges, click X to delete an incorrect range.

e. If you have added all the IP ranges you want to poll, click Next.

12. If you want to discover devices connected to a specific router or on a specific subnet of your network, complete the following procedure:

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

    a. Click Subnets in the Selection Method menu.

    b. If you want to discover on a specific subnet, click Add a New Subnet, provide both a Subnet Address and a Subnet Mask for the desired subnet, and then click Add.

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

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

    Notes:

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

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

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

    e. Confirm that all networks on which you want to conduct your network discovery are selected, and then click Next.

13. If you already know the IP addresses or hostnames of the devices you want to discover and include in the Orion database, complete the following procedure:

a. Click Specific Nodes in the Selection Method menu.

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

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

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

d. If you have provided all the IPv4 addresses and hostnames you want to discover, click Next.

14. Configure the options on the Discovery Settings view, as detailed in the following steps. Provide a Name and Description to distinguish the current discovery profile from other profiles you may use to discover other network areas.

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

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

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

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

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

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

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

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

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

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

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

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

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

16. If multiple Orion polling engines are available in your environment, select the Polling Engine you want to use for this discovery.
17. Click Next.
18. If you want the discovery you are currently defining to run on a regular schedule, select either Custom or Daily as the discovery Frequency, as shown in the following steps:

    Notes:

    Scheduled discovery profiles should not use IP address ranges that include nodes with dynamically assigned IP addresses (DHCP).

    Default Discovery Scheduling settings execute a single discovery of your network that starts immediately, once you click **Discover**.

    Results of scheduled discoveries are maintained on the Scheduled Discovery Results tab of Network Discovery.

    a. If you want to define a custom discovery schedule to perform the currently defined discovery repeatedly in the future, select Custom and then provide the period of time, in hours, between discoveries.
    b. If you want your scheduled discovery to run once daily, select Daily, and then provide the time at which you want your discovery to run every day, using the format HH:MM AM/PM.

19. If you do not want to run your network discovery at this time, select No, don’t run now, and then click Save or Schedule, depending on whether you have configured the discovery to run once or on a schedule, respectively.
20. If you want your Network Sonar discovery to run now, click Discover to start your network discovery.

    Note: Because some devices may serve as both routers and switches, the total number of Nodes Discovered may be less than the sum of reported Routers Discovered plus reported Switches Discovered.

Adding an Individual Node

The following procedure details the steps required to add a device and its interfaces and volumes for monitoring in the Orion Web Console.

To add a single node:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings in the top right of the web console.
3. Click Manage Nodes in the Node Management grouping of the Orion Website Administration page.
4. Click Add Node on the Node Management toolbar.
5. Provide the hostname or IP Address of the node you want to add in the Hostname or IP Address field.
6. If you only want to use ICMP to monitor node status, response time, or packet loss for the added node, select Status Only (ICMP).
7. If you want to add an External node to monitor a hosted application with Orion Platform products (for example, Orion APM), select External.

   Note: SolarWinds NCM does not collect or monitor any network performance data from nodes designated as External. The External status is reserved for nodes hosting application that you want to monitor with Orion Application Performance Monitor.
8. If you want to use SNMP to monitor the added node, confirm that ICMP (Ping only) is cleared, and then complete the following steps:

   a. Select the SNMP Version for the added node.

   Notes:

   SolarWinds NPM uses **SNMPv2c** by default. If the device you are adding supports or requires the enhanced security features of SNMPv3, select **SNMPv3.**(NCM supports SNMPv3 with AES-256.)

   If SNMPv2c is enabled on a device you want SolarWinds NCM to monitor, by default, SolarWinds NCM will attempt to use SNMPv2c to poll for performance information. If you only want SolarWinds NCM to poll using SNMPv1, you must disable SNMPv2c on the device to be polled.

   b. If the SNMP port on the added node is not the Orion Platform product default of 161, provide the actual port number in the SNMP Port field.If the added node supports 64 bit counters and you want to use them, select Allow 64 bit counters.

   Note: Orion Platform products support the use of 64-bit counters; however, these high capacity counters can exhibit erratic behavior depending on manufacturer implementation. If you notice peculiar results when using these counters, use the Node Details view to disable the use of 64-bit counters for the device and contact the hardware manufacturer.
9. If you want Orion Platform products to use SNMPv2c to monitor the added node, provide valid community strings for the added node.

Note: The Read/Write Community String is optional, but Orion Platform products require the public Community String, at minimum, for node monitoring.

10. If you want Orion Platform products to use SNMPv3 to monitor the added node, provide the following SNMP Credentials, Authentication, and Privacy/Encryption settings:

    SNMPv3 Username and Context

    SNMPv3 Authentication Method and Password/Key

    SNMPv3 Privacy/Encryption Method and Password/Key

11. If you are using SNMP to communicate with your added node, click Validate SNMP after entering all credentials to confirm your SNMP settings.

12. Click Next.

13. Select the interfaces, volumes, and interface charts for the added node that you want Orion to monitor. The following options are available in the selection toolbar:

    Clicking **All** selects all listed devices and charts for monitoring.

    Clicking **None** clears any selected interfaces, volumes, or interface charts that have been selected for monitoring.

    Clicking **All Active Interfaces** selects only currently active interfaces and the associated interface charts for monitoring.

    Clicking **All Volumes** selects all listed volumes for monitoring.

    Clicking **All Interfaces** selects all listed interfaces for monitoring.

14. After you have selected interfaces, volumes, or interface charts for monitoring, click Next.

15. If you want to edit the default polling settings for your added node, change the Node Status Polling or Collect Statistics Every values in the Polling area of the Change Properties page, as appropriate.

    Note: The Node Status Polling value refers to the number of seconds, between the node status checks Orion Platform products perform on the added node. The Collect Statistics Every value refers to the period of time between the updates Orion Platform products make to displayed statistics for the added node.

16. If you have defined any custom properties for monitored nodes, provide appropriate values for the added node in the Custom Properties area of the Change Properties page.

Note: The Custom Properties area is empty if you have not defined any custom properties for monitored nodes. For more information on how to add custom properties, see Creating Custom Properties.

17. Click Add Node to NCM to manage the node as part of NCM.
18. Click OK, Add Node when you have completed properties configuration.
19. If you have successfully added the node, click OK on the dialog.

Managing NCM Nodes

All SolarWinds NCM nodes must be managed in the Orion Platform database, which all Orion Platform products share.

Use these procedures to find, add, edit, or remove Orion nodes to and from the NCM node list.

Note: If you remove a node from NCM all data associated with the node (configs, inventory data, etc.) is also removed.

To add or remove a specific node from NCM:

1. Login on the Orion Web Console with an administrator account.
2. Click Manage Nodes in the All Nodes resource.
3. Select a desired grouping in the left pane or select ‘No Grouping’.
4. Select the node and then click Edit Properties.
5. search for the node under Search NodesSelect the node in the list of the Node resource and then click Manage Node.
6. Scroll down to the last section with the property **Manage node(s) with NCM**.
7. ***If you do not want the node managed with NCM***, select No.
8. ***If you want to manage the node with NCM***, select Yes.

   The NCM Properties listed with their current values.
9. Adjust the values as needed and then click Submit.
10. Consult the Licensed by NCM column to review node status.

To edit the properties of an NCM node:

1. Login on the Orion Web Console with an administrator account.
2. Click Manage Nodes in the All Nodes resource.
3. Select a desired grouping in the left pane or select ‘No Grouping’.
4. Select the node and then click Edit Properties.

5. search for the node under Search NodesSelect the node in the list of the Node resource and then click Manage Node.
6. Scroll down to the last section with the property **Manage node(s) with NCM**.
7. Select Yes.

   The NCM Properties listed with their current values.
8. Adjust the values as needed and then click Submit.

Using the Network Sonar Discovery Results Wizard

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

The following steps detail the selection of discovered objects for monitoring in SolarWinds NCM.

To select the results of a network discovery for monitoring in SolarWinds NCM:

1. On the Device Types to Import page, select the device types you want SolarWinds NCM to monitor, and then click Next.

   Note: If you are not sure you want to monitor a specific device type, select the device type in question. If, later, you do not want to monitor a selected device, simply delete the device using Web Node Management.
2. On the Volume Types to Import page, select the volume types you want SolarWinds NCM to monitor, and then click Next.

   Note: If you are not sure you want to monitor a specific volume type, select the volume type in question. If, later, you do not want to monitor any volume of the selected type, delete the volume using Web Node Management.
3. If there are any devices on the Import Preview that you do not ever want to import, select the device to ignore, and then click Ignore. Selected nodes are added to the Discovery Ignore List.
4. Confirm that the network objects you want to monitor are selected on the Import Preview page, and then click Import.
5. After the import completes, click Finish.

   Note: Imported devices display in the All Nodes resource.

Unmanaging and Remanaging Nodes

When you need to perform maintenance on nodes, such as upgrading firmware, installing new hardware, or updating security, you may want SolarWinds Network Configuration Manager to discontinue downloading configurations and reporting information about the nodes while the devices are down. Unmanaging nodes while node maintenance is being performed helps maintain the accuracy of your data and prevents unnecessary and inaccurate reports.

Another reason to unmanage a node is if you want to keep configuration files for a decommissioned device. Configuration data for unmanaged nodes will remain in Orion Platform database.

To unmanage nodes:

1. Login on the Orion Web Console with an administrator account.
2. Click Manage Nodes on the All Nodes resource.
3. Select the nodes you want to unmanage in the nodes list, and then click Unmanage.

When nodes are unmanaged, SolarWinds Network Configuration Manager will not perform actions on the nodes such as downloading configuration files, running scheduled jobs on the nodes, including the unmanaged nodes in reports.

To remanage nodes:

1. Login on the Orion Web Console with an administrator account.
2. Click Manage Nodes on the All Nodes resource.
3. Select the nodes you want to unmanage in the nodes list, and then click Remanage.

Managing End of Support and End of Sales (EOS)

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

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

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

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

Refreshing EOS Dates

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

To refresh suggested EOS dates for your NCM devices:

1. Login to the Orion Web Console and access the EOS view (CONFIG > EOS).
2. Select the devices for which you want updated data (if available). Use the Group by options as needed.
3. Click Refresh Suggested Dates.'

Assigning EOS Dates

If you want to apply known EOS dates for a vendor model to one or more of you NCM devices, follow these steps.

To assign EOS dates for your NCM devices:

1. Login to the Orion Web Console and access the EOS view (CONFIG > EOS).
2. Select the devices for which you want updated data (if available). Use the Group by options as needed.
3. Click Assign Dates.'
4. You should see a list of your selected devices on the Assign EOS Data screen under Node Selected. If a device is missing, click Add More Nodes, select the appropriate nodes, and then click OK.
5. Search the table for the model of your selected NCM nodes in the Choose Dates table. If you find it, select that row.
6. Search the table for the model of your selected NCM nodes in the Set EOS Dates table. If you find it, select that row.

   The dates listed for a model or series have indications in the Reliability column: High, Medium, Low, Confirmed. 'High' indicates that the date(s) are unambiguous. 'Medium' indicates that the date(s) remains ambiguous due to other incomplete or conflicting information. 'Low' indicates that the date(s) are tentative. And 'Confirmed' indicates that the date(s) were confirmed by an NCM user.

7. If you did not find the model of your selected NCM nodes, but you want to assign dates anyway, select Option 2 and set the End of Support and/or End of Sales dates.
8. Add comments as needed.
9. Click Assign.

Ignoring Devices in EOS Management

If you do not want NCM to track EOS dates for one or more of you NCM devices, follow these steps.

To ignore EOS dates for NCM devices:

1. Login to the Orion Web Console and access the EOS view (CONFIG > EOS).
2. Select the devices for which you want updated data (if available). Use the Group by options as needed.
3. Click Ignore Devices.’
4. You should see a list of your selected devices on the Assign EOS Data screen under Node Selected. If a device is missing, click Add More Nodes, select the appropriate nodes, and then click OK.
5. Search the table for the model of your selected NCM nodes in the Choose Dates table. If you find it, select that row.
6. If you did not find the model of your selected NCM nodes, but you want to assign dates anyway, select Option 2 and set the End of Support and/or End of Sales dates.
7. Add comments as needed.
8. Click Assign.

Exporting EOS Information

If you want NCM to export EOS data for one or more of you NCM devices, follow these steps.

To export EOS data for NCM devices:

1. Login to the Orion Web Console and access the EOS view (CONFIG > EOS).
2. Select the devices for which you want updated data (if available). Use the Group by options as needed.
3. Click Export and select the format.’
4. Select a location.

5. Click OK.

Deleting EOS Data

If you want NCM to drop EOS data for one or more of you NCM devices, follow these steps.

To delete EOS data for NCM devices:

1. Login to the Orion Web Console and access the EOS view (CONFIG > EOS).
2. Select the devices for which you want updated data (if available). Use the Group by options as needed.
3. Click Delete EOS Data.’
4. Click OK.

How to Filter EOS Data

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

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

Setting filters is especially useful in seeing which devices reach End of Support or End of Sales at the same time (for example, in the “Next 3 months”); to see the EOS status for devices from the same vendor; or to see the EOS status on devices in the same subnet.

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

Assigning EOS Dates

You can apply assigned or suggested EOS dates to any NCM device, regardless of what EOS currently displays in the EOS table.

Follow these steps to assign dates to NCM nodes:

1. Select the relevant nodes in the End of Support & Sales resource. Alternatively, if you are on the Assign EOS Dates resource, and you have one or nodes selected, but you want to select more, click Add More Nodes.
2. Select an option of assigning dates.

   a. If your device(s) pertain to a model for which EOS dates are listed in Option 1, click the relevant date ranage for that model.
   b. Click More details to see the source of the EOS information.If you want to manually enter EOS dates, select Option 2 and enter either an End of Support date, an End of Sales date, or both.
3. Enter EOS comments as needed.
4. Click Assign.

Understanding NCM Macros

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

All NCM macros are enclosed in '${   }'; the macro for system name, for example, is '${SysName}'. NCM User can concatenate any number of macros in each editable node field. For example, the macros ${SysName}${Vendor} would involve both the system name and vendor in the field.

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

NCM supports several types of macros:

Nodes Macros

Macros which point to another column in Nodes table. For example: ${SysName} will point to 'SysName' column of Nodes table. Node macros are unique to each Node.

Global Macros

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. Serveral global macros—such as ${GlobalCommunitySting}—are predefined; and users can also create custom global macros.

Built-in Macros

Macros such as ${Date}, ${Time} that currently are not supported by the Orion Web Console, which uses the .NET macro parser. Only the NCM desktop application supports this type of macro.

Device Template Macros

Macros related to a device vendor and stored in device templates. For example: ${ConfigType}.

Menu-based Macros

Macros defined to operate with menu-base devices. For Example: ${DownArow} will simulate sending of DownArrow key while connection to device.

Using Custom Macros

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

To create a custom macro:

1. Click Add New in the Custom Macros resource.
2. Enter a name and value for the new macro.

   For example, if you want to define a macro to track the provision date and location of devices, you might use ProvisionAustin1 as the name for devices in Austin TX provisioned on a certain date and use the city and date as the value; Macro Name: ProvisionedAustin1; Macro Value: Austin 05/10/2012.
3. Click Submit.

To edit a custom macro:

1. Select the macro and click Edit in the Custom Macros resource.
2. Modify the value of the macro.
3. Click Submit.

To delete a custom macro:

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

Searching for Network Addresses

SolarWinds Network Configuration Manager provides the ability to search the entire database (Nodes table, IP Address table, ARP tables, BridgePorts andMAC Forwarding tables, Interfaces) for specific network addresses.

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

Consult these topics as needed:

Finding IP Addresses

Finding MAC Addresses

Finding Hostnames

Understanding How Addresses are Found

Finding IP Addresses

It can be important to find an IP address in SolarWinds Network Configuration Manager. For example, you may need to search all of your nodes to see if a node to which you need to make changes is managed by SolarWinds Network Configuration Manager.

To find an address:

1. Open the SolarWinds Network Configuration Manager application.
2. Click Edit > Find IP Address.
3. To ensure that the most complete results are available, click Update Inventory at the bottom of the Find Address tab to rescan all nodes in the database for any updated information. For more information on performing inventory scans, see “Managing Inventory” on page 225.
4. Type the address pattern you want to find in the IP Address Pattern field.
5. Click Find.

Finding MAC Addresses

It can be necessary to find an MAC address in SolarWinds Network Configuration Manager. For example, you may need to search all of your configuration files to see if a MAC address is included in any black lists.

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

To find a MAC address:

1. Open the SolarWinds Network Configuration Manager application.
2. Click Edit > Find MAC Address.
3. To ensure that the most complete results are available, click Update Inventory at the bottom of the Find Address tab to rescan all nodes in the database for any updated information. For more information on performing inventory scans, see “Managing Inventory” on page 225.
4. Type the address pattern you want to find in the MAC Address Pattern field.
5. Click Find.

Finding Hostnames

For convenience, if you network supports DNS, you can search for NCM nodes by hostname.

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

To find a hostname:

1. Open the SolarWinds Network Configuration Manager application.
2. Click Edit > Find Hostname
3. To ensure that the most complete results are available, click Update Inventory at the bottom of the Find Address tab to rescan all nodes in the database for any updated information. For more information on performing inventory scans, see “Managing Inventory” on page 225.
4. Select Hostname from the Type of Address list if it is not already in focus.
5. Type a fully qualified hostname in the Hostname field.
6. Click Find.

Understanding How Addresses are Found

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

Nodes Table

Stores a list of all nodes managed by SolarWinds NCM, along with the declared node properties.

IpAddresses Table

Stores a list of IP addresses mapped to interface and node IDs.

Interfaces Table

Stores a list of interfaces, interface indices, interface types, and interface descriptions mapped to node IDs.

BridgePorts Table

Stores a list of bridge ports, spanning tree status, spanning tree state, VLAN type, and VLAN ID mapped to node IDs.

MACForwarding Table

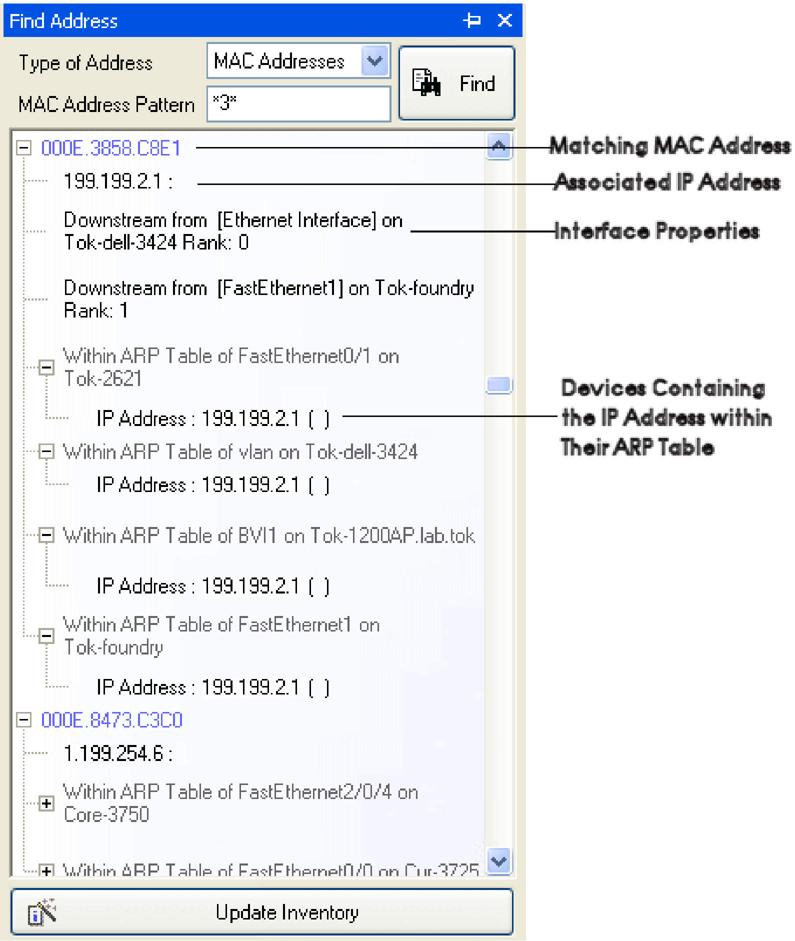
Stores a list of MAC addresses, ports, and how the address was mapped to node IDs.

ARPTables

> 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.

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.

The following screen capture illustrates a typical search result.



Find Address

Type of Address: MAC Addresses

MAC Address Pattern: *3*

```
⊟ 000E.3858.C8E1
    199.199.2.1 :
    Downstream from [Ethernet Interface] on
    Tok-dell-3424 Rank: 0
    Downstream from [FastEthernet1] on Tok-foundry
    Rank: 1
  ⊟ Within ARP Table of FastEthernet0/1 on
    Tok-2621
      IP Address : 199.199.2.1 ( )
  ⊟ Within ARP Table of vlan on Tok-dell-3424
      IP Address : 199.199.2.1 ( )
  ⊟ Within ARP Table of BVI1 on Tok-1200AP.lab.tok
      IP Address : 199.199.2.1 ( )
  ⊟ Within ARP Table of FastEthernet1 on
    Tok-foundry
      IP Address : 199.199.2.1 ( )
⊟ 000E.8473.C3C0
    1.199.254.6 :
  ⊞ Within ARP Table of FastEthernet2/0/4 on
    Core-3750
  ⊞ Within ARP Table of FastEthernet0/0 on Cur-3725
```

Matching MAC Address

Associated IP Address

Interface Properties

Devices Containing the IP Address within Their ARP Table

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

Notes:

- If you are searching for a MAC address that is part of a VLAN, the returned 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.

Find Connected Port for a Host (SolarWinds NPM Integration)

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

Besides having NCM integrated with NPM, for this feature to function, you must also manage both nodes and both 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, which is specified at the top of the table in which search results are presented, in this form:

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

You can search for connected ports by these node properties:

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

To search for connected ports:

1. Login to the Orion Web Console with administrator privileges.
2. Note: If you do not have administrator privileges you may not be able to see some results.
3. Click Configs.
4. Locate the Find Connected Port for End Host resource.
5. Select the Search By filter and enter an appropriate value in Find.
6. Use the Edit button to adjust the columns of data to include in your search results.
7. Click Find.

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

Column	Description
(For Wired Devices)	
Node	Vendor and model of context node
IP Address	Of the context node
MAC Address	Of the context node
Connected Via Interface	On the context node
To This Interface	On a connection point
On This Node	Vendor and model of device supporting the connection point
IP Address	Of a connection point
MAC Address	Of a connection point
(For Wireless Devices)	
Mapped Host Name	Vendor and model of context node
Mapped MAC Address	Of context node
Mapped Device Type	Of context node
Source Interface	Of the wireless access point
Controller Source IP Address	Of the wireless access point
Controller Description	Of the wireless access point
Controller Host Name Source SSID	Of the wireless access point
Source Channel	Of the wireless access point
Source Interface Alias	Of the wireless access point
Source Radio Type	Of the wireless access point
Source Host Name	Of the wireless access point
Source Device Type	Of the wireless access point
Source IP Address	Of the wireless access point

Chapter 4

Managing Web Accounts

Orion Web Console user accounts, permissions, and views are established and maintained with the Manage Accounts option. Use the following sections of this chapter to work with Orion accounts.

- Creating a New Account
- Editing an Orion User Account
- Creating Account Limitations

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

Creating a New Account

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

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

The following procedure creates a new web console user account.

To create a new user account:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings in the top right of the web console.
3. Click Manage Accounts in the Accounts grouping of the Orion Website Administration page.
4. Click Add New Account.
5. Select the type of account you want to add, and then click Next.
6. If you selected Windows individual account, complete the following steps:

a. Provide the User Name and Password for a user that has administrative access to your Active Directory or local domain.

b. In the Search for Account area, enter the User name of the Active Directory or local domain user for whom you want to create a new web console account, and then click Search.

c. In the Add Users area, select the users for whom you want to create new web console accounts, and then click Next.

7. If you selected Windows group account, complete the following steps:

   a. Provide the User Name and Password for a user that has administrative access to your Active Directory or local domain.

   b. In the Search for Account area, enter the Group name of the Active Directory or local domain group for which you want to create a new web console account, and then click Search.

   c. In the Add Users area, select the users for whom you want to create new web console accounts, and then click Next.

8. If you selected Orion individual account, complete the following steps:

   a. Provide a User Name and a Password for the Orion individual account.

   b. Confirm the password, and then click Next.

   c. Define user settings and privileges, as appropriate.

   For more information, see “Editing an Orion User Account” on page 70.

   By default a new Orion account is created with the WebUploader role. To adjust the NCM role for an account, expand Network Configuration Manager Settings and select the appropriate role for the account you are creating.

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

9. Click Submit to create the account.

   Note: Accounts are enabled by default, and disabling an account does not delete it. Account definitions and details are stored in the Orion database in the event that the account is enabled at a later time.

Editing an Orion User Account

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

Note: You must be an Orion platform administrator to create and manage jobs. However, if you are an Orion platform administrator with account limitations that are designed to limit your area of operation to a specific set of nodes, but you use NCM job editing controls to limit the nodes upon which a specific job acts, NCM will not honor those node limitations. Any job you create or edit will affect all nodes to which your Orion platform Administrator account gives you access.

The following sections and procedures detail the configuration of user accounts.

Note: To reset a password, click **Change Password** at the bottom of the page.

- Setting User Account Access
- Configuring User Login and Device Access Security
- Setting Account Limitations
- Creating Account Limitations
- Setting Default Account Menu Bars and Views
- Configuring Audible Web Alerts

Setting User Account Access

The following procedure is a guide to setting Orion user account access.

By default, 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. If you select None as the NCM role, and this account might be used for node discovery, you should unselect "Enable Import from Discovery" (in Settings > NCM Settings > Manage Nodes) to prevent this and similar account users from adding licensed nodes to NCM.

To edit an Orion user account:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings in the top right of the web console.
3. Click Manage Accounts in the Accounts grouping of the Orion Website Administration page.
4. Select the account that you want to edit, and then click Edit.
5. Set Account Enabled to Yes or No, as appropriate.

   Note: Accounts are enabled by default, and disabling an account does not delete it. Account definitions and details are stored in the Orion database in the event that the account is enabled at a later time.

6. If you want the account to expire on a certain date, click Browse (…) next to the Account Expires field, and then select the account expiration date using the calendar tool.

   Note: By default, accounts are set to Never expire. Dates may be entered in any format, and they will conform to the local settings on your computer.

7. If you want to allow the user to remain logged-in indefinitely, select Yes for the Disable Session Timeout option.

   Note: By default, for added security, new user accounts are configured to timeout automatically.

8. If you want to grant administrator rights to the selected account, set Allow Administrator Rights to Yes.

   Notes:

   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 Admin page information.

9. If you want to allow the user to manage nodes directly from the Orion Web Console, set Allow Node Management Rights to Yes.

   Note: By default, node management rights are not granted. For more information about node management in the Orion Web Console, see “Managing Devices in the Web Console”.

10. If you want to allow the user to customize views, set Allow Account to Customize Views to Yes.

    Note: 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.

11. Designate whether or not to Allow Account to Clear Events and Acknowledge Alerts.

12. Select whether or not to Allow Browser Integration.

    Note: Browser integration can provide additional functionality, including access to right-click menu options, depending on client browser capabilities.

13. If you want to enable audible alerts through the client browser, select a sound 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.

14. Provide the maximum Number of items in the breadcrumb list.

    Note: If this value is set to 0, all available items are shown in breadcrumb dropdown lists.

15. Set account limitations as needed under Account Limitations.

16. Set menu bars and views (Default Menu Bars and Views) as you want them displayed by default in the Orion Web Console.

17. 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 a CONFIGS tab and all the NCM views.

    For details see “Setting Default Account Menu Bars and Views”.

18. Set an NCM role for the account under Network Configuration Manager Settings.

    By default, Orion administrator accounts are given the NCM administrator role; it does not make sense to assign an Orion admin anything other than an NCM admin role.

    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. If you select None as the NCM role, and this account might be used for node discovery, you should unselect "Enable Import from Discovery" (in Settings > NCM Settings > Manage Nodes) to prevent this and similar account users from adding licensed nodes to NCM.

    A user with the NCM role None cannot access the SolarWinds Network Configuration Manager application and will not see any NCM resources in non-NCM views and tabs on the Orion Web Console. For example, such a user sees no Pending Approval List on the Summary view under HOME.

    Though this user would be able to complete the process of adding NCM resources through Customize Page, the resources do not display when the target view loads. And though this user may have privileges to add nodes into Orion, the user cannot add nodes to NCM (the “Add Node to NCM” option does not appear); and NCM properties are hidden when the user edits any selected Orion node.

If an account user with NCM role None sets up an NCM Alert Action the software displays an error in alert details.

19. 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 NCM view settings (Settings > Manage Accounts > Edit [User] Account) . If you do not set them to None, and you select None as the NCM role for the account, the user will still see a CONFIGS tab and all the NCM views.
20. Use the settings under General Orion Settings to define how you want information to be displayed when a specific node, volume, or group is viewed.
21. Click Submit when you are finished adjusting account settings.

Configuring User Login and Device Access Security

Security settings enable you to govern the handling of account credentials, using encryption and masking when appropriate.

To set user authentication and device access:

1. Open the Orion Web Console.
2. Click Settings.
3. Click NCM Settings.
4. Click Security under Security.
5. Select the desired password security settings:

   Hide SNMP Community Strings

   Selecting this setting hides your SNMP community strings in any area of the application where they would otherwise show.

   Hide Login User Names

   Selecting this setting hides a username during login.

   Encrypt User Names in Database

   Selecting this setting encrypts usernames in the Orion Platform database so that a database viewer cannot see plain text values.

   Encrypt Passwords in the Database

   Selecting this setting encrypts passwords in the Orion Platform database so that a database viewer cannot see plain text values.

6. Click the credential set to be used in managing devices.

Global—Device Level

This option defaults the device login to the global setting.

Individual—User Level

This option defaults the device login to the NCM user account. (SolarWinds recommends this option so that access to network devices takes advantage of the security inherent in NCM roles.)

7. Click Submit.

Setting User Level Login Credentials

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

To set user level credentials:

1. Open the Orion Web Console.
2. Click Settings.
3. Click NCM Settings.
4. Click Manage User Level Login Credentials under Security.
5. Enter a valid NCM user credentials (Username/Password).
6. Select an Enable Level if you want the account to a specific level of access on relevant network devices.
7. If you select an Enable Level, enter the password that pertains to this level.
8. Click Submit.

Setting Account Limitations

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

Note: You must be an Orion platform administrator to create and manage jobs. However, if you are an Orion platform administrator with account limitations that are designed to limit your area of operation to a specific set of nodes, but you use NCM job editing controls to limit the nodes upon which a specific job acts, NCM will not honor those node limitations. Any job you create or edit will affect all nodes to which your Orion platform Administrator account gives you access.

The following procedure sets user account limitations.

To set user account limitations:

1. Log in to the Orion Web Console as an administrator.

2. Click Settings in the top right of the web console, and then click Manage Accounts in the Accounts group of the Orion Website Administration page.
3. If you want to limit an individual user account, complete the following steps:

   a. On the Individual Accounts tab, select the account you want to limit.

   b. Click Edit.

   c. Click Add Limitation in the Account Limitations section.

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

   Notes:

   Because SolarWinds NCM initially caches account limitations, it may take up to a minute for account limitations related to NCM to take effect in the web console and application.

   Account limitations defined using the Account Limitation Builder display as options on the Select Limitation page. Account limitations can be defined and set using almost any custom properties. For more information, see “Creating Account Limitations”.

   e. Define the limitation as directed on the Configure Limitation page that follows. For more information about defining pattern-type limitations, refer to “Defining Pattern Limitations”.
4. If you want to limit an group account, complete the following steps:

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

   a. On the Groups tab, select the group account you want to limit.

   b. Click Edit.

   c. Click Add Limitation in the Account Limitations section.

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

   Notes:

   Because SolarWinds NCM initially caches account limitations, it may take up to a minute for account limitations related to NCM to take effect in the web console and application.

   Account limitations defined using the Account Limitation Builder display as options on the Select Limitation page. Account limitations can be defined and set using almost any custom properties. For more information, see “Creating Account Limitations”.

    e. Define the limitation as directed on the Configure Limitation page that follows. For more information about defining pattern-type limitations, refer to “Defining Pattern Limitations”.

5. Click Add Limitation in the Account Limitations section.

6. Select the type of limitation to apply from the list, and then click Continue.

   Notes:

   Account limitations defined using the Account Limitation Builder display as options on the Select Limitation page. Account limitations can be defined and set using almost any custom properties. For more information, see “Creating Account Limitations”.

   Because SolarWinds NCM initially caches account limitations, it may take up to a minute for account limitations related to NCM to take effect in the web console and application.

7. Define the limitation as directed on the Configure Limitation page that follows. For more information about defining pattern-type limitations, refer to “Defining Pattern Limitations”.

Creating Account Limitations

The Account Limitation Builder application allows you to create and customize account limitations for the Orion Web Console. These limitations ensure that users of the web console can only view the network objects that are pertinent to their job duties. The following are but a few examples of the uses of account limitation in the Orion Web Console:

- 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

SolarWinds NCM provides predefined account limitations that use built-in SolarWinds NCM property to limit user access. For greater flexibility, however, you can use the Account Limitation Builder to create your own account limitations based on predefined or custom properties. For more information about enabling account limitations in the Orion Web Console, see “Setting Account Limitations”. For more information about custom properties, see “Creating Custom Properties”.

Note: You must be an Orion platform administrator to create and manage jobs. However, if you are an Orion platform administrator with account limitations that are designed to limit your area of operation to a specific set of nodes, but you use NCM job editing controls to limit the nodes upon which a specific job acts, NCM will not honor those node limitations. Any job you create or edit will affect all nodes to which your Orion platform Administrator account gives you access.

Using the Account Limitation Builder

Before you can use the Account Limitation Builder, you must have first created the custom property that you want to use to limit the Orion Web Console view. For more information, see “Creating Custom Properties”. After you have defined custom properties and populated them with data, you may use the Account Limitations Builder as directed in the following procedure.

Creating an Account Limitation

The following steps create an account limitation.

To create an account limitation:

1. Click Start > All Programs > SolarWinds Orion > Grouping and Access Control > Account Limitation Builder.
2. Click Start on the splash screen.
3. Click Edit > Add Limitation.
4. Select a Custom Property.

   Notes:

   If Custom Property is empty, you need to define a custom property. For more information, see “Creating Custom Properties”.

   The remaining boxes are populated automatically, based upon your selection.
5. Choose a Selection Method.

   Note: This is the selection format that will appear when you are choosing values for the account limitation through the web Account Manager. For more information, see “Setting Account Limitations”.
6. If you want to include your own description of your account limitation, type your description over the default text provided in the Description field.
7. Click OK.

Your newly defined account limitation is added to the top of the table view. You may now use the new limitation in the Orion Web Console Account Manager. For more information, see “Setting Account Limitations”.

Deleting an Account Limitation

The following steps delete an account limitation using the Account Limitation Builder utility.

To delete an account limitation:

1. Click Start > All Programs > SolarWinds Orion > Grouping and Access Control > Account Limitation Builder.
2. Click Start on the splash screen.
3. Click the row of the limitation that you want to delete.

   Note: Use Shift+click to highlight multiple consecutive rows or Ctrl+Click to highlight multiple non-consecutive rows.
4. Click Edit > Delete Selected Limitations.

   Note: Although Orion deletes the selected limitations from the table, ensuring that they will no longer be available through the web Account Manager, if you delete a limitation using the Account Limitation Builder, all accounts that have been assigned that limitation will remain limited. Deleting a limitation simply makes it unavailable for future use in the Orion Web Console.

Defining Pattern Limitations

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

Note: Patterns are not case sensitive.

- `foo` matches only objects named "foo".
- `foo_` matches all objects with names consisting of the string "foo" followed by only one additional character, like `foot` or `food`, but not `seafood` or `football`.
- `foo*` matches all objects with names starting with the string "foo", like `football` or `food`, but not `seafood`.
- `*foo` matches all objects with names ending with the string "foo", like `bigfoot` or `seafood`, but not `food`.
- `*foo*` matches all objects with names containing the string "foo", like `seafood` or `Bigfoot`.
- `*foo* OR *soc*` matches all objects containing either the string "foo" or the string "soc", including `football`, `socks`, `soccer`, and `food`.

- `*foo* AND *ball*` matches all objects containing both the string "foo" and the string "ball", including `football` but excluding `food`.
- `*foo* NOT *ball*` matches all objects containing the string "foo" that do not also contain the string "ball", including `food` but excluding `football`.
- `*foo* EXCEPT *ball*` matches all objects containing the string "foo" that do not also contain the string "ball", including `food` but excluding `football`.

You 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`.

Setting Default Account Menu Bars and Views

The Default Menu Bar and Views section provides several options for configuring the default menu bar and views for your user account. The following procedure is a guide to setting these options.

To set default menu bar and view options:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings in the top right of the web console, and then click Manage Accounts in the Accounts grouping of the Orion Website Administration page.
3. Select the account that you want to configure, and then click Edit.
4. Scroll down to Default Menu Bar and Views.
5. Select a Home Tab Menu Bar from the available list.

   Note: This is the default menu bar displayed when you click Home in the Orion Web Console. If you are editing a user account that must have administrator privileges, set the Home Tab Menu Bar to Admin.
6. Select a Network Tab Menu Bar from the available list.

   Note: This is the default menu bar displayed when you click Network in the Orion Web Console. If you are editing a user account that must have administrator privileges, select Admin.
7. Select a Virtualization Tab Menu Bar from the available list.

   Note: This is the default menu bar displayed when you click Virtualization in the Orion Web Console. If you are editing a user account that must have administrator privileges, select Admin.
8. If you have installed any additional Orion modules, select an Orion Module Tab Menu Bar from each available list.

Note: This step configures the default menu bar displayed when you click the tab corresponding to an installed module in the Orion Web Console. If you are editing an account that must have administrator privileges, select Admin.

9. Select a Home Page View.

    Note: If no Home Page View is specified, the default is designated to be the same as the page that is specified in the Default Summary View field below.

10. If the Home Page View you have selected refers to a specific network device, select a Default Network Device by clicking Edit and selecting from the list of available devices on the next page.

    Note: If the Home Page View you have selected does not require a specific network device, Orion will select a device to display, automatically.

11. Select a Default Summary View for the account.

    Note: This is typically the same as the Home Page View.

12. If you want all reports to be available for the account, select \Reports from the Report folder list in the Default Menu Bars and Views area.

    Note: If you are creating a new user, you must designate the Report Folder the new account is to use to access Orion reports. By default, no report folder is configured for new users. The Reports directory is located in the SolarWinds NCM installation directory:
    C:\Program Files\SolarWinds\Orion\.

13. If you want to designate default Node, Volume, and Group Details Views for this account, expand Orion General Settings, and then select appropriate Node Detail, Volume Detail, and Group Detail Views.

14. If you want to designate default Virtualization Summary Manager, Cluster Details, and Datacenter Details Views for this account, expand Integrated Virtual Infrastructure Monitor Settings, and then select appropriate default views.

15. Click Submit.

Configuring Audible Web Alerts

When browsing the Orion Web Console, audible alerts can be sounded whenever new alerts are generated. When enabled, you will receive an audible alert the first time, after login, that an alert is displayed on the page. This alert may come from either an alert resource or the Alerts view. You 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 in the top right of the web console.
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.

Chapter 5

Managing Configuration Files

Configuration files can be downloaded, edited, compared, and uploaded using SolarWinds Network Configuration Manager. The following procedures guide you through various tasks that simplify configuration file management.

Note: The **Config Transfers** setting (Settings > NCM Settings > Configs) limits the number of lines required for a config file to be recognized as valid for download. The default setting is 11 lines. In the case of a multi-node upload/download operation, keep in mind that the Simultaneous Downloads/Uploads setting can be used as a throttle; by default it's set to run 10 Sessions simultaneously. Similarly, to avoid unusually long download sessions, you can set the SNMP config transfer timeout (default: 4 minutes).

Downloading Configuration Files

You can download configuration files to view the current configuration of your device, compare the current to a previous configuration, or just to archive configuration files for backup purposes. SolarWinds Network Configuration Manager can transfer files using both direct and indirect transfers. Complete the following procedure to download configuration files from your devices.

Notes:

- On some Nortel devices, you may need to enable CLI mode before the command templates supplied with SolarWinds NCM work correctly. Most BayStack devices allow you to choose command line from the system menu and type `cmd-interface cli` to enable CLI mode. For more information, see your Nortel device documentation.
- 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, and you can perform all SNMP operations except transferring configurations. You can execute scripts, upload, and download configuration files on IPv6 addresses; Telnet and SSH communication are supported.
- The **Config Transfers** setting (Settings > NCM Settings > Configs) limits the number of lines required for a config file to be recognized as valid for download. The default is 11 lines.

Download Configs (Single Node)

This resource allows you to download the startup, running, or custom configuration from the current node.

To download a config:

1. Login to the Orion Web Console with an account that has the WebDownloader, WebUploader, Engineer, or Administrator role..
2. Click CONFIGS > Config Summary.
3. Click a node in the nodes list.
4. Click the Config tab.
5. Select the config type in the Download Config resource, and then click Download.
6. Click OK.
7. For details on the transfer click Transfer Details.

Downloaded configuration files are stored on your server in an archive in the location specified in the NCM Settings (Settings>NCM Settings>Configs).

Notes:

If NCM cannot turn-off pagination for a managed device, then configs downloaded from the device via Telnet or SSH most likely will include blank or other unexpected lines.

The **Config Transfers** setting (Settings > NCM Settings > Configs) limits the number of lines required for a config file to be recognized as valid for download. The default setting is 11 lines. In the case of a multi-node download operation, keep in mind that the Simultaneous Downloads/Uploads setting can be used as a throttle; by default it’s set to run 10 Sessions simultaneously.

Download Configs (Multiple Nodes)

This resource allows you to download the startup, running, or custom configuration from the current node.

To download a config:

1. Open the Orion Web Console and navigate to the NCM Jobs view (CONFIGS > Jobs).
2. Click Create New Job, select Download Configs from Devices, and give the job a title.
3. Select the schedule type.

   Basic gives you Once, Daily, Weekly, and Monthly schedule settings (start, end, recurrence). .

   Advanced gives you more granular control over the schedule, supporting more complex patterns defined with cron expressions.

4. If you are creating a Basic schedule, select the frequency of the job.

   Once: enter a day and time (at least 15 minutes from current NCM server time).

   Daily: Select Every Day or Every Week Day, enter a Start time, and then select start and end dates

   Weekly: Select the days, enter a Start time, and then select start and end dates.

   Monthly: Select the months, days of the month, enter a Start time, and then select start and end dates

5. If you are creating an Advanced schedule, use the five fields to create the appropriate cron expression.

   For example, if you want the job to run once a week over every month at midnight on Sunday morning, the values for the fields would be 0 0 * * 0.

   This transliterates as telling NCM to run the job at 0 minutes and 0 hours, on all valid days of month, in all valid months, on Sunday".

6. Add a comment as needed and then click Next.

7. Select the NCM nodes to target with this job.

   Select Nodes: Click Select Nodes and select the NCM nodes you want the job to target.

   All Nodes: Selects all NCM nodes as targets for the the job.

   Dynamic Selection: Define the criteria that NCM will use to determine the selection of NCM nodes as targets for the job.

   Nodes defined in legacy job scheduling system: Select the option and then click Yes, change selection.

   Note: Use this option to target the node group of all wireless access points in the Orion Platform database.

8. Select an email notification option.

   a. If you select Email Results, then enter the email from/to information.

   b. Enter the email server address and port number.

   c. If the email server expects credentials, then select Password.

   d. Enter the username and password.

9. Click Next.

10. Select the configuration types you want to download.

11. If you want to be notified when the downloaded configuration file is different from the last configuration, select Last downloaded config file.

12. If you want to be notified when the downloaded configuration file is different from the baseline configuration, select Baseline config file.
13. If you want to be notified when the downloaded configuration file is different from the startup configuration, select Startup config file.
14. Select Send config change notification details in a separate text email and Send config change notification details in a separate HTML email as appropriate. These options allow you to separate change details from change notification.
15. If you only want to save the configuration file when changes are found, select Only save Configs that have changed.
16. Click Next.
17. Review the settings for the job.
18. When you are done reviewing the settings, click Finish.

    Notes:

    The Config Transfers setting (Settings > NCM Settings > Configs) limits the number of lines required for a config file to be recognized as valid for download. The default setting is 11 lines. In the case of a multi-node download operation, keep in mind that the Simultaneous Downloads/Uploads setting can be used as a throttle; by default it’s set to run 10 Sessions simultaneously.

    If NCM cannot turn-off pagination for a managed device, then configs downloaded from the device via Telnet or SSH most likely will include blank or other unexpected lines.

Enabling a New Config Type

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

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

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

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

To enable a new config type for your device:

1. Open the Orion Web Console.
2. Click Settings > NCM Settings.
3. Click Configs.
4. Click Add New under Config Types.
5. Enter a name for the new config type.
6. Click Submit.
7. Follow these procedures to modify your relevant device template with an appropriate statement.

Note: NCM uses the ‘show’ command to download configurations. In modifying each relevant device template model your new statement on the statements that define the ‘startup’ and ‘running’ configs as valid types of config to use with ‘show’.

Enabling the Config Cache

By default, if you enable config caching, the config cache is automatically updated at 11:55 pm every evening.

Enabling the policy and config caches occurs with the same control.

To enable the config cache:

1. Open the Orion Web Console.
2. Click Settings.
3. Click NCM Settings.
4. Click Advanced Settings.
5. Select Enable Config and Policy Caches under Cache Settings.
6. Click Submit.

Editing Configuration Files

When you need to update access lists, modify community strings, or make any other configuration changes, you will need to edit the configuration files you have already downloaded with SolarWinds Network Configuration Manager. Complete the following procedure to edit a configuration file.

To edit an existing configuration file:

1. Login to the Orion Web Console with an account that has the WebDownloader, WebUploader, Engineer, or Administrator role..
2. Click CONFIGS > Config Summary.

3. Click a node in the nodes list.
4. Click the Config tab.
5. Select a config in the Config List resource and click Edit config.
6. Retitle this version of the config, if desired.
7. Click Edit Config text and make your changes.
8. Make comments under Comments, as needed, and then click Submit..

   Note: The revision is saved in the Config List with the indication that it is an ‘Edited’ config of its type.
9. If you are ready to upload the edited config, verify that the edited config is selected in the Upload Config resource (it is selected by default), and then click Upload For more information, see "Uploading Configuration Changes".

Executing a Script

You can execute a script against the selected node or a list of nodes.

The script you execute needs to be saved as a text file that can be browsed to on the client computer. The results of your script can be found on the Configuration Management view by clicking **Transfer Status** in the left navigation pane. Transfer Status provides the most resent status of an action taken on a node through SolarWinds NCM. Click **Script Results** to view the results of executing your script.

This resource is available to users with the WebUploader, Engineer, or Administrator role. For more information, see "Configuring User Access Control" in the *SolarWinds NCM Administrator Guide*.

These procedures assume that you have already created a script to be uploaded and stored it on the NCM host.

To execute a script:

1. Login to the Orion Web Console with an account that has the WebDownloader, WebUploader, Engineer, or Administrator role..
2. Click CONFIGS > Config Summary.
3. Select a node or nodes in the nodes list.
4. Click Execute Script.
5. Create a script in Enter a script to execute or click Load Script.

   Notes:

NCM automatically manages device connection session; you do not need to include a command for terminating the session in which your script executes.

You can specify delay inside script in seconds– time NCM wait before sending next command:${Delay:20} - wait 20 seconds before sending next command. So a script that includes the delay looks like this:

{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.

6. Select Execute Script in Config Mode if you want NCM to put the device into config mode before executing the script.

   Note: This is the function for Telnet/SSH. For TFTP or SCP, the script sends a config file to the device, not a line-by-line script. Whether or not the target device merges the script with the existing config (for example, by appending it) or overwrites the config file varies according to device; check your device documentation for details.
7. Select the config type to which the script will be uploaded.
8. If you want to write the config to NVRAM after upload, select that option and then click Next.
9. If you want to reboot the device after executing the script, select Reboot Device
10. Click Execute.
11. If you created a new script, click Save Script to File to store it.
12. If you want to add the script to the product repository on thwack, click Download/Share Script.
13. Click Close when you are finished working with the script.

Uploading a Config

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

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.

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

To upload a config:

1. Open Orion Web Console.

   Note: 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. Click CONFIGS > Configuration Management.
3. Select the node(s) in the node list to which you want to upload the config.
4. Click Upload Config.
5. Find (+) and select a config under a node in the list.

   The config loads in the right pane.

6. Make changes as needed.
7. Click Advanced.
8. If you want to write the config to NVRAM after upload, select Write to NRAM.
9. If you want to reboot the device after executing the script, select Reboot Device/
10. If you want to reboot the device after upload, select Reboot Device.
11. If you created a new script, click Save Script to File to store it.
12. Click Upload.
13. Click Close.

Decrypting Cisco Type 7 Passwords

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

To decrypt Cisco Type 7 passwords:

1. Open the SolarWinds Network Configuration Manager application.

2. Click on the configuration file in the left pane, and then click Configs > Edit Configs.

3. Click Actions, and then click Decrypt Type 7 Passwords.

   Notes:

   All passwords that have been decrypted will appear in green text.

   Decrypting Type 7 Passwords alters the text of the configuration file. If the configuration file is saved after decrypting the passwords, the passwords will be saved without encryption.

Defining Comparison Criteria

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

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

The regular expressions you create and enable in the Comparison Criteria resource are used throughout SolarWinds NCM—for example, in performing scheduled jobs—wherever the software needs to compare config files as part of its work.

Use the following procedures to create, edit, enable/disable, or delete a regular expression pattern.

To create a new regular expression statement:

1. Open the Orion Web Console.
2. Click Settings > NCM Settings > Comparison Criteria.
3. Click Add New.
4. Enter the appropriate information.
   a. Give the pattern a distinctive name. For example, if the purpose of the pattern is to have NCM ignore hex data, you might call this pattern ‘hex data’.
   b. Write the regular expression.

   See “Comparison Criteria (Exclusion Examples)” for basic guidelines on writing regular expressions to ignore lines in config files when performing config comparisons; and see “Regular Expression Pattern Matching” for details on the range of regular expression operations supported in creating comparison criteria.

c. Provide a comment so that others know your intent in creating this RegEx pattern.

d. Click Enable this RegEx pattern during config compares to activate this pattern. You can always edit the pattern later and enable it if you choose to leave the pattern disabled now.

e. Click OK.

To edit a regular expression statement:

1. Open the Orion Web Console.
2. Click Settings > NCM Settings > Comparison Criteria.
3. Select a regular expression (Title) and click Edit.
4. Modify the information as needed.

    a. Select Enable this RegEx pattern during config compares to activate this pattern or unselect it to disable.

    b. Provide a descriptive for a title. For example, if the purpose of the pattern is to have NCM ignore hex data, you might call this pattern ‘hex data’.

    c. Revise the regular expression. Consult Regular Expression Pattern Matching for details on regular expression statements supported in creating comparison criteria.

    d. Revise or add the comment so that others know your intent in creating this RegEx pattern.

    e. Click OK.

To enable or disable a regular expression pattern:

Select the relevant item (Title) and click Enable or Disable.

To delete a regular expression pattern:

Select the relevant item (Title) and click Delete.

Comparison Criteria (Exclusion Examples)

The following are examples of regular expression pattern combinations that SolarWinds Network Configuration Manager 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.

Exclusions specified with regular expressions are global, and used for all comparison operations throughout SolarWinds NCM, including scheduled jobs. For more information about regular expression patterns, see “Regular Expression Pattern Matching”.

Comparing Configurations

SolarWinds Network Configuration Manager provides the ability to compare configuration files. Configuration files can be compared between two nodes; or older configurations can be compared with the current configuration.

In making your comparison, you can select comparison criteria for excluding lines that contain a specific string pattern.

To compare two configurations:

1. Open the Orion Web Console.
2. Create and enable exclusion filters, as needed. See “Defining Comparison Criteria” for details.
3. Click CONFIGS > Configuration Management.
4. Select the node(s) whose configs you want to compare.

   Ifyou want to compare configs from two different nodes, select both nodes.

   Ifyou want to compare two configs from the same node, select the single node.
5. Select the configs you want to compare.

   The dropdown list includes the configs available on the node(s) you selected.
6. Review the configs for changes (yellow highlights), added lines (green highlights), and missing lines (pink highlights).
7. Click Edit Config above either config if you need to make changes.
8. Click Set/Clear Baseline on either config to make it the baseline against which NCM should alert you to future config changes.

9. If either config is obsolete and should be removed, click Delete Config, double-check the config name to verify this is the config to remove, and then click Yes.
10. Click Export to PDF if you want a PDF of the config comparison.
11. Close Close.

Importing Configuration Files

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

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

To import a configuration file (NCM web console):

1. Open the SolarWinds Web Console
2. Click CONFIGS > Configuration Management
3. Select a node from the node list.
4. Click Config.
5. Click Import a Config in the Config List resource.
6. Browse to the config file.
7. Add comments as needed and then click Submit.

To import a configuration file (NCM application):

8. Open the SolarWinds Network Configuration Manager application.
9. Select the node in the node list to which you want to import a configuration file.
10. Drag the file from the Windows Explorer to the SolarWinds Network Configuration Manager node list.
11. Type a name for the configuration file, and then click OK.

Understanding Baselines

A baseline is a configuration file that is known to be good for a particular application. When making node configuration changes, it is a good idea to establish a *known-good* configuration as a baseline.

Setting a Baseline

Follow these procedures to mark a downloaded config as the baseline against which to compare future downloads.

To set an existing configuration file as a baseline:

1. Open Orion Web Console.

   Note: 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. Click CONFIGS > Configuration Management.
3. Select the node(s) in the node list.
4. Click Config.
5. Select the config in the Config List resource and click Set/Clear Baseline.

   Note:

   Currently the NCM application is the best way to set a new baseline. When you do this in the application NCM regenerates cache data used to update the "Overall Baseline Vs Running Config Conflict" chart, always keeping it up to date. Resetting a baseline through the web console does not regenerate cache data, so there may be some delay before the chart displays the most current data.

   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 previous downloaded configuration file.

Removing a Baseline

Follow these procedures to clear a downloaded config as the baseline against which to compare future downloads.

To remove an existing configuration file as a baseline:

1. Open Orion Web Console.

Note: 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. Click CONFIGS > Configuration Management.
3. Select the node(s) in the node list.
4. Click Config.
5. Select the config that is the current baseline in the Config List resource and click Set/Clear Baseline.

Baselining Your Entire Network

In some situations, it may be appropriate to establish a baseline configuration for every node managed by SolarWinds Network Configuration Manager on your network. You can use either of the following options to create your baseline:

- Set to the last configuration file downloaded
- Set to the configuration files downloaded on a specific date

To create a baseline for your entire network:

1. Open the Orion Web Console and navigate to the NCM Jobs view (CONFIGS > Jobs).
2. If you are creating a new job, click Create New Job, select the appropriate job type, give the job a title.
3. If you want to edit an existing job, click Edit.
4. Select the schedule type.

   Basic gives you Once, Daily, Weekly, and Monthly schedule settings (start, end, recurrence). .

   Advanced gives you more granular control over the schedule, supporting more complex patterns defined with cron expressions.
5. If you are creating a Basic schedule, select the frequency of the job.

   Once: enter a day and time (at least 15 minutes from current NCM server time).

   Daily: Select Every Day or Every Week Day, enter a Start time, and then select start and end dates

   Weekly: Select the days, enter a Start time, and then select start and end dates.

   Monthly: Select the months, days of the month, enter a Start time, and then

6. If you are creating an Advanced schedule, use the five fields to create the appropriate cron expression.

   For example, if you want the job to run once a week over every month at midnight on Sunday morning, the values for the fields would be 0 0 * * 0.

   This transliterates as telling NCM to run the job at 0 minutes and 0 hours, on all valid days of month, in all valid months, on Sunday".

7. Add a comment as needed and then click Next.

8. Select the NCM nodes to target with this job.

9. Select Nodes: Click Select Nodes and select the NCM nodes you want the job to target.

   All Nodes: Selects all NCM nodes as targets for the the job.

   Dynamic Selection: Define the criteria that NCM will use to determine the selection of NCM nodes as targets for the job.

   Nodes defined in legacy job scheduling system: Select the option and then click Yes, change selection.

   Note: Use this option to target the node group of all wireless access points in the database.

10. Select an email notification option.

    a. If you select Email Results, then enter the email from/to information.

    b. Enter the email server address and port number.

    c. If the email server expects credentials, then select Password.

    d. Enter the username and password.

11. Click Next.

12. If you want to use the last config downloaded from each device as your baseline, select Set the Network Baseline to the last Config downloaded from each Node.

13. If you want to set the Network Baseline to a spefic date, select Set the Network Baseline to a specific date and select a date.

14. If instead of setting the baseline you want to remove existing baselines, select Clear all Baselines.

15. Click Next.

16. Review the settings for the job.

17. When you are done reviewing the settings, click Finish.

Clearing All Baselines

Follow these procedures to clear all baselines from the Orion Platform database.

To remove all baselines from your database:

1. Open the Orion Web Console and navigate to the NCM Jobs view (CONFIGS > Jobs).
2. If you are creating a new job, click Create New Job, select the appropriate job type, give the job a title.
3. If you want to edit an existing job, click Edit.
4. Select the schedule type.

   Basic gives you Once, Daily, Weekly, and Monthly schedule settings (start, end, recurrence). .

   Advanced gives you more granular control over the schedule, supporting more complex patterns defined with cron expressions.
5. If you are creating a Basic schedule, select the frequency of the job.

   Once: enter a day and time (at least 15 minutes from current NCM server time).

   Daily: Select Every Day or Every Week Day, enter a Start time, and then select start and end dates

   Weekly: Select the days, enter a Start time, and then select start and end dates.

   Monthly: Select the months, days of the month, enter a Start time, and then select start and end dates
6. If you are creating an Advanced schedule, use the five fields to create the appropriate cron expression.

   For example, if you want the job to run once a week over every month at midnight on Sunday morning, the values for the fields would be 0 0 * * 0.

   This transliterates as telling NCM to run the job at 0 minutes and 0 hours, on all valid days of month, in all valid months, on Sunday”.
7. Add a comment as needed and then click Next.
8. Select the NCM nodes to target with this job.

   Select Nodes: Click Select Nodes and select the NCM nodes you want the job to target.

   All Nodes: Selects all NCM nodes as targets for the the job.

   Dynamic Selection: Define the criteria that NCM will use to determine the selection of NCM nodes as targets for the job.

Nodes defined in legacy job scheduling system: Select the option and then click Yes, change selection.

Note: Use this option to target the node group of all wireless access points in the database.

9. Select an email notification option.
   a. If you select Email Results, then enter the email from/to information.
   b. Enter the email server address and port number.
   c. If the email server expects credentials, then select Password.
   d. Enter the username and password.
10. Click Next.
11. Select Clear all Baselines.
12. Click Next.
13. Review the settings for the job.
14. When you are done reviewing the settings, click Finish.

Running Change Reports

A change report shows all modifications made to each configuration file over a specific time period. Change reports can show you changes made during a specific date range, or all differences between the latest downloaded configuration file and the baseline configuration file.

To run a config change report:

1. Open the SolarWinds Network Configuration Manager application.
2. Click Configs > Config Change Report.
3. Select the type of change report to generate:

Compare most recent download to the last running config

Displays all differences between the most recent running configuration and the latest downloaded configuration file.

Compare most recent download to the last startup config

Displays all differences between the most recent startup configuration and the latest downloaded configuration file.

Compare most recent download to the last baseline config

Displays all differences between the most recent baseline and the latest downloaded configuration file.

Compare the most recent download to the configuration on date

Displays all differences between the most recent downloaded configuration file and a configuration file from the specified date.

Note: If no configuration file was downloaded on the specified date, the configuration file following that date is used.

Show changes made over the past ## days

Displays all changes made over the specified number of days.

Show changes made between dates

Displays all the changes made through the specified date range.

Note: Keep in mind that generating a Config Change Report with these procedures differs from generating a Config Change Report from the Device Details resources of a specific node. In the current case, the report runs based on the criteria selected on the 'Show the following config changes' section of report. In contrast, from node details (right-click node > Configuration History > Config Change Report) the software performs a comparison of all configs from the bottom of the list (the oldest, essentially) upward (to the newest) and displays only those which actually have the changes during the last 60 days.

4. If you want the config change report to ignore specific changes, complete the following procedure:
   a. Click Edit Comparison Criteria.
   b. Select the appropriate exclusions.
   c. If you want to create a new exclusion, see “Creating New Config Change Report Exclusions” on page 100.
   d. Click Done.
5. If you want to see detailed changes between each configuration file, click ︽, and then select Show detailed changes. This shows each change from one configuration file to the next. For example, if there were 14 configuration changes made during a specific date range, the report will show the differences in the first configuration file as compared to the second configuration, and then show the differences in the second configuration file as compared to the third, and so on.
6. Click Generate Report.

Creating New Config Change Report Exclusions

When viewing config change reports, some changes can be ignored. For example, the `!Last Configuration change` line in Cisco configuration files can safely be ignored.

To specify sections of configuration files that can be ignored, SolarWinds Network Configuration Manager uses regular expression patterns. The following are some of the regular expression pattern combinations SolarWinds Network Configuration Manager recognizes:

```
^! 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.

Exclusions specified with regular expressions are global, and used for all comparison operations throughout SolarWinds NCM, including scheduled jobs. For more information about regular expression patterns, see "Regular Expression Pattern Matching".

To create a new exclusion:

1. Select Configs > Config Change Report in the SolarWinds Network Configuration Manager application.
2. Click Edit Comparison Criteria in the Config Change Report resource.
3. Click Add Pattern.
4. Type a name for the new comparison criteria in the Title field.
5. Type the regular expression pattern in the RegEx Pattern field you want SolarWinds Network Configuration Manager to ignore when running change reports.
6. Type any comments you have in the Comment field.

Creating Config Snippets

A config snippet is a string of text that can be saved to a file, allowing you to easily merge sections of configuration files. For example, a config snippet is created from a router with the string `snmp-server community 123@dm1n RO`. When editing another router configuration, the config snippet can be reused. Config snippets can be used to edit an existing configuration file, or they can be uploaded directly to a node or group of nodes. For more information, see "Uploading a Config Snippet" on page 105.

To create a new Config snippet:

1. Open the SolarWinds Network Configuration Manager application.

2. Click Configs > Config Snippets.
3. Click New Snippet.
4. Type a name in the Snippet field.
5. Type configuration lines for the new config snippet in the large text box provided, and then click Save Changes.

Uploading Configuration Changes

After editing your configuration files, you can easily upload changes to a node or group of nodes. There are three different ways to upload configuration changes:

- Upload an entire configuration
- Upload selected lines
- Upload a config snippet.

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

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

Uploading an Entire Configuration

Complete the following procedure to upload an entire configuration file.

Notes: In the case of a multi-node upload/download operation, keep in mind that the Simultaneous Downloads/Uploads setting can be used as a throttle; by default it's set to run 10 Sessions simultaneously.

To upload an entire configuration file:

1. Open the Orion Web Console and navigate to the NCM Jobs view (CONFIGS > Jobs).
2. Click Create New Job, select the appropriate job type, give the job a title.
3. Select the schedule type.

Basic gives you Once, Daily, Weekly, and Monthly schedule settings (start, end, recurrence). .

Advanced gives you more granular control over the schedule, supporting more complex patterns defined with cron expressions.

4. If you are creating a Basic schedule, select the frequency of the job.

   Once: enter a day and time (at least 15 minutes from current NCM server time).

   Daily: Select Every Day or Every Week Day, enter a Start time, and then select start and end dates

   Weekly: Select the days, enter a Start time, and then select start and end dates.

   Monthly: Select the months, days of the month, enter a Start time, and then select start and end dates

5. If you are creating an Advanced schedule, use the five fields to create the appropriate cron expression.

   For example, if you want the job to run once a week over every month at midnight on Sunday morning, the values for the fields would be 0 0 * * 0.

   This transliterates as telling NCM to run the job at 0 minutes and 0 hours, on all valid days of month, in all valid months, on Sunday".

6. Add a comment as needed and then click Next.

7. Select the NCM nodes to target with this job.

   Select Nodes: Click Select Nodes and select the NCM nodes you want the job to target.

   All Nodes: Selects all NCM nodes as targets for the the job.

   Dynamic Selection: Define the criteria that NCM will use to determine the selection of NCM nodes as targets for the job.

   Nodes defined in legacy job scheduling system: Select the option and then click Yes, change selection.

   Note: Use this option to target the node group of all wireless access points in the database.

8. Select an email notification option.

   a. If you select Email Results, then enter the email from/to information.
   b. Enter the email server address and port number.
   c. If the email server expects credentials, then select Password.
   d. Enter the username and password.

9. Click Next.
10. If you want to select config changes from a config in the database, click Load Script, browse to your command script file, and then click OK.
11. If you want to select a config snippet, click Select Config Changes from Snippet, and copy the relevant snippet from the Select Config Snippet box.

    For more information on config snippets see "Uploading a Config Snippet".
12. If you want to select config changes from a config in the database, click Select Config Changes from Database, locate the config in the node tree, and the click OK.
13. Verify the config information in the Upload Changes to Devices Job box is what you want NCM to upload.
14. Select Write config to NVRAM after upload if you want the upload to reside in RAM.
15. Click Next.
16. Review the settings for the job.
17. When you are done reviewing the settings, click Finish.

Uploading Selected Lines

There are times when you only need to upload part of a configuration file. SolarWinds Network Configuration Manager includes the ability to upload specific lines of a configuration.

To upload specific lines:

1. Open the SolarWinds Network Configuration Manager application.

   Note: If you do not have administrator privileges you may not be able to see some nodes or settings.
2. Click a configuration file under the node in the node list (left pane), and then click Configs > Edit Configs.
3. Select the lines you want to upload, and then click Actions > Upload Selected Lines.

   Note: Additional nodes can be added or removed from the list by using the associated buttons below the list of nodes.

4. If you want to write the configuration to memory, select Write Config to NVRAM.
5. If you need to reboot your device following the upload, select Reboot Device.

   Warning: Rebooting a device may cause momentary connectivity outages.

6. Click Create Upload Script.
7. Click Execute Command Script.
8. If you want to save the results of the script when the upload finishes, click Save Results.

Uploading a Config Snippet

Complete the following procedure to upload a config snippet. For information on how to create config snippets, see “Creating Config Snippets” on page 101.

Caveat: Regarding upload of config snippets to your device, some devices are setup by default to overwrite the startup config with a config received via TFTP. If in doubt about the way your device is setup, do not use TFTP as your protocol to upload config snippets.

To upload a Config Snippet:

1. Open the Orion Web Console.

   Note: If you do not have administrator privileges you may not be able to see some nodes or settings.

2. Click Settings.
3. Click NCM Settings and then click Global Device Defaults.
4. Adjust the transfer protocol under Communication Transfer Protocol > Transfer Configs as needed, and then click Submit.

   Note: Upload of config snippets to your device, some devices are setup by default to overwrite the startup config with a config received via TFTP. If in doubt about the way your device is setup, do not use TFTP to upload config snippets.

5. Open the SolarWinds Network Configuration Manager application in the program group on your computer.
6. Click Configs > Config Snippets.

7. Click the snippet in the Config Snippets window, and then right-click Upload to Devices.
8. Use the associated buttons to add or delete nodes from the list or to group them together for easier oversight during your operation.
9. On the Upload Config tab do the following as needed:
10. If you want to write the configuration to memory, select Write Config to NVRAM on the Upload Config tab.
11. If you need to reboot your device following the upload, select Reboot Device.

    Warning: Rebooting a device may cause momentary connectivity outages.
12. Click Upload.
13. If you want to save the results of the script when the upload finishes, click Save Results.

Configuring a Config Archive

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

To configure a configuration archive:

1. Open the Orion Web Console.

   Note: If you do not have administrator privileges you may not be able to see some nodes and settings.
2. ***If you want to store your Config Archive on a network share***, instead of a local directory on the NCM Server host, do the following:
   a. Open NCM Advanced Settings (Settings > NCM Settings > Advanced Settings).
   b. Select **Use custom credentials** to give NCM write access, provide a username and password valid for the network share, and click Validate Credentials to verify your entries.
3. Open NCM Settings (Settings > NCM Settings).
4. Click Configs.
5. Select **Save a copy of each Config to the Config-Archive directory when it is downloaded**.
6. To save space on your storage target, if you need only the immediately past version in addition to the current config, select **When configs are edited, only retain the last version**.

7. Type the path of the local directory or network share in which you want to store the NCM Config Archive.

   Note: By default, NCM sets the directory for your Config Archive as %Program Files (x86)\SolarWinds\Orion\NCM\Config-Archive. As preparation for a growing archive, SolarWinds recommends that you move the Config Archive from this location.

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

9. Click Submit.

Enabling Real-time Configuration Change Detection

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

Requirements

To utilize real-time configuration change detection you will need the following items.

- 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.
- Both the SolarWinds Syslog and Trap Services must be configured to run as administrator so that their scheduled jobs are processed correctly. For detailed steps, see “Running Syslog and Trap Services as Administrator”.
- Ensure the SNMP Trap Service is running. If the SNMP Trap Service is not listed as a running service in the service control manager (`services.msc`), you can enable Simple Network Management Protocol in the Management and Monitoring Tools through Add/Remove Windows Components in the Add/Remove Programs application.

Configuring Real-time Configuration Change Detection

Complete the following procedure to enable real-time configuration change detection using SolarWinds SolarWinds Network Configuration Manager.

Notes:

- Both the SolarWinds Syslog and Trap Services must be configured to run as administrator so that their scheduled jobs are processed correctly. For detailed steps, see Running Syslog and Trap Services as Administrator.
- Cisco devices send trap messages when a user enters config mode but not when the user exits. As a result, if you make changes to the config on your device, you will receive a trap about those changes only when you again enter config mode, which usually is not until another change to the config needs to be done. In short, due to this behavior, SolarWinds recommends that you use the syslog option for setting up real-time change detection.
- SolarWinds Kiwi Server Syslog Server setup instruction appear in Step 8 if you are using that product for syslog server notifications.

To enable real-time configuration change detection:

1. Open the Orion Web Console.
2. Click Settings.
3. Click NCM Settings.
4. Click Configure Real-time Change Detection.

   You must complete all 6 steps for Real-time Change Detection features and functions to operate correctly.
5. On the Real-Time Change Detection setup page, complete the pre-requisite (Step 1) by manually configuring your devices to send syslog or trap messages.when configuration changes are detected.

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

   Note: You can remove device configurations by running a given command with ‘no’ in front of it; for example, no set logging server ip_address removes that target from the remote logging stream.

   a. Open Orion Web Console if it’s not already open.
   b. Click Configuration Management under CONFIGS.
   c. Click Execute Command Script.in the list of options on the left.
   d. Paste in the commands from the example, changing the IP address to match your device.

   Syslog (IOS)

   config terminal

   logging 10.199.3.43

   logging trap 6

```
end
```

Syslog (CatOS)

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

Traps (IOS)

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

Taps (CatOS)

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

e. Click Next.

f. Select the node(s) on which to run the script.

g. Click Execute.

h. Click OK .

i. Click Results under STATUS/DETAILS.

Note: Steps 6 through 9 pertain to the NCM Process section (Step 2) on the Real-Time Change Detection setup page.

6. For your Cisco devices that send change notifications using Syslog messages, complete the following procedure.

   a. Open the Syslog Viewer (SolarWinds > Syslog and SNMP Traps).

   b. Click View > Alerts/Filter Rules.

   c. Select NCM Rule: Cisco IOS - Change Notifications.

   d. Click OK.

7. If your devices are not Cisco devices and send change notifications using Syslog messages, complete the following procedure:

a. Click Start > All Programs > SolarWinds > Syslog and SNMP Traps > Syslog Viewer.

b. Click View > Alerts/Filter Rules.

Note: For the upgrade to NCM 7.1.x, if you setup rules in the SolarWinds NCM Syslog Server in a previous version of SolarWinds NCM, you can open that application (SolarWinds Network Configuration Manager > SolarWinds NCM Syslog Server) to find your previous setup. Use those previously defined rules for recreating your logic here in the SolarWinds Syslog Viewer.

c. Click Add New Rule.

d. Provide the appropriate information on the General tab and DNS Hostname tab.

e. Click the Message tab, and then type the message pattern to look for in the Message Type Pattern field. The message pattern will vary by device type. For example, when a change is made to a Cisco router, a syslog message containing SYS-5-CONFIG_I: is sent. For more information about what messages are sent, see the documentation provided by the vendor of your device.

f. Click the Alert Actions tab, and then click Add New Action.

g. Select Execute an external program, and then click OK.

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

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

Where:

Path

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

${IP}

Variable that includes the IP of the triggering device.

RealtimeNotification

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

${DateTime}

Variable that includes the current date and time, this is equivalent to the Windows control panel defined Short Date and Short Time format.

${Message}

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

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

i. Click OK.

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

8. If your devices send change notifications using SolarWinds Kiwi Syslog Server, complete the following procedure:

   a. Click Start > All Programs > SolarWinds Kiwi Syslog Server > SolarWinds Kiwi Syslog Server Console.

   b. Click File > Setup.

   c. Click Filter, and then right-click New Filter to give it a better name (for example, RTNMessage).

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

   e. Right-click Actions and.change New Action to a name that servers better. For example, call it ‘RTN’.

   f. Type the following in the Program file name field:

      Path\Orion\SolarWinds.NCM.RTNForwarder.exe

      Where:

      Path

      Declares the location of the Orion folder. For example, “C:\Program Files (x86)\SolarWinds”. If the path contains spaces, enclose the path section of the statement in quotation marks (“).

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

   h. Click ApplyOK.

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

9. If your device sends change notifications using SNMP Trap messages, complete the following procedure:

a. Click Start > All Programs > SolarWinds > Syslog and SNMP Traps > Trap Viewer.

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

b. Click View > Alerts/Filter Rules.

Note: For the upgrade to NCM 7.1.x, if you setup rules in the SolarWinds NCM Trap Server in a previous version of SolarWinds NCM, you can open that application (SolarWinds Network Configuration Manager > SolarWinds NCM Trap Server) to find your previous setup. Use those previously defined rules for recreating your logic here in the SolarWinds Trap Viewer.

c. Click Add Rule.

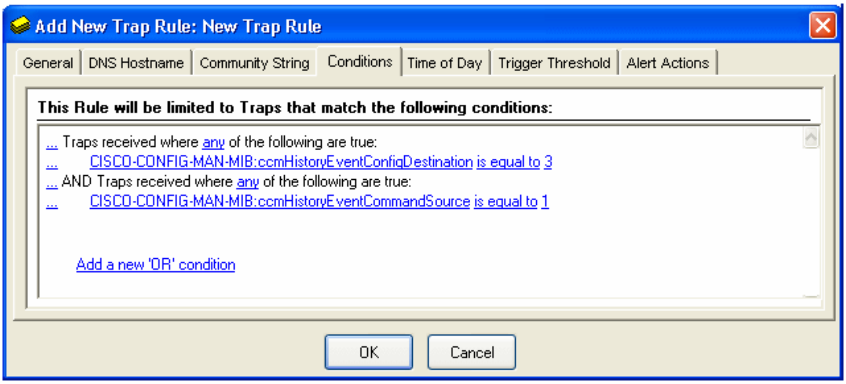
d. Provide the appropriate information on the General tab and DNS Hostname tab.

e. Click the Conditions tab, and then click Add a condition.

f. Click SNMPv2-MIB:snmpTrapOID, and then browse to the MIB that contains the trap message. For example, browse to CISCO-CONFIG-MAN-MIB:ccmHistoryEventConfigDestination (1.3.6.1.4.1.9.9.43.1.1.6.1.5).

g. Click the asterisk, and then type the message pattern to match. For example, when a change is made to the running config the HistoryEventMedium is 3. Changes to the startup config are designated by the integer 4.

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



This Rule will be limited to Traps that match the following conditions:

... Traps received where any of the following are true:
...   CISCO-CONFIG-MAN-MIB:ccmHistoryEventConfigDestination is equal to 3
... AND Traps received where any of the following are true:
...   CISCO-CONFIG-MAN-MIB:ccmHistoryEventCommandSource is equal to 1

Add a new 'OR' condition

i. Click the Alert Actions tab, and then click Add Action.

j. Select Execute an external program, and then click OK.

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

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

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

l. Click OK.

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

10. If your device sends change notifications to a system other than SolarWinds Network Configuration Manager, complete the following procedure:

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

    b. Setup an alert that executes an external program.

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

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

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

       ${IP}

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

    d. Save the alert and ensure it is enabled.

11. For NCM Process (Step 3), Enter Windows account credentials and device login information.

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

13. Click Config Changes under NCM Process (Step 3) on the Real-Time Change Detection setup page.

14. Each syslog or trap that triggers RTCD immediately results in the download of the latest running config on the relevant device(s). To do this the Orion software uses the Windows Task Scheduler, which requires an account to create and run the relevant job(s).

a. Define the Windows account you will use to create and run RTCD-related download jobs.

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

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

c. Click a desired setting for how to handle simultaneous Real-Time Notification download operations.

d. If you choose More than one at a time, then the NCM software runs as many as are allowed by the Simultaneous Downloads/Uploads setting (Settings > NCM Settings > Configs > Config Transfer). The default is 10 concurrent sessions.

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

f. Click Submit.

15. Click Config Downloads and Notification Settings (under Step 4) on the Real-Time Change Detection setup page to specify config download details.

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

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

c. Select the relevant Email Notification Options

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

e. Click Submit.

16. Click Config NCM SMTP Server (under Step 5) on the Real-Time Change Detection setup page to specify config download details.

a. Enter the mail server’s FQDN or IP address.

b. Enter the relevant port number on which the mail server handles messages.

c. Enter an access authentication option (either Password or None).

d. Enter a valid username by which the mail server will identify your RTN recipient.

e. If you are requiring password authentication, type and confirm the password for the username.

f. Click Submit.

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

For information on config change approvals, see Chapter 13, “Approving Device Configuration Changes”.

17. Click Enable (Step 6, Real-Time Detection setup page) to turn on Real-Time Change Detection.
18. Click Submit.

Limiting Real-time Notification Download Operations

In some cases the config downloads in response to syslog and trap information flowing in from your network devices can threaten to pin resources on your NCM server.

Complete the following procedure to limit the number of simultaneous Real-time notification download operations that can be performed.

To limit Real-time notification download operations:

1. Open the Orion Web Console.
2. Click Settings.
3. Click NCM Settings.
4. Click Config.
5. Use the slider to adjust the number of Simultaneous Download/Uploads. The default number of concurrent sessions is 10.
6. Click Submit.

Running Syslog and Trap Services as Administrator

Although the SolarWinds Syslog Service and Trap Service are installed and launched with Administrator access, you must manually grant them such access in order for them and their jobs to run correctly.

To grant Administrator access to the SolarWinds Syslog Service and Trap Service:

1. Navigate to the location where SolarWinds software is installed. The default installation path is C:\Program Files\SolarWinds\Orion\....
2. Right click SyslogService.exe in the right pane and select Run as….
3. Click The following user and select Administrator.
4. Click OK.
5. Right click SWTrapService.exe in the right pane and select Run as….
6. Click The following user and select Administrator.
7. Click OK.

Searching for Configuration Files (Web Console)

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

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

To search for text within configuration files:

1. Login on the Orion Web Console.
2. Click CONFIGS.
3. Click Advanced Search under the Search NCM resource.
4. Enter the string and select a search target from the dropdown list.
   a. If you are searching Configs from All Nodes, select the filters for your search.

   Search the last downloaded config from each node only and Search All Configs do as they say.

b. Specify a date range allow you to limit the search to configs downloaded within the past week, month, previous month, or within a range that is accurate to the second.

c. Include the following Config types allows you to limit the search to all the running, startup, or edited config type. (The default setting targets all config types as part of the search.)

d. If you are searching Configs from Selected Nodes, select the relevant nodes in the Selected Nodes list and define the filters for your search.

Search the last downloaded config from each node only and Search All Configs do as they say.

e. Specify a date range allow you to limit the search to configs downloaded within the past week, month, previous month, or within a range that is accurate to the second.

f. Include the following Config types allows you to limit the search to all the running, startup, or edited config type. (The default setting targets all config types as part of the search.)

5. Click Search.
6. To search within the returned search results, click Search in results, enter a relevant string, and click Search again.

Searching for Configuration Files (Application Only)

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

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

To search for text within configuration files:

1. Open the SolarWinds Network Configuration Manager application.

   Note: If you do not have administrator privileges you may not be able to see some nodes or settings.

2. Click Edit > Search Configs in the SolarWinds Network Configuration Manager application.
3. If you want to select which nodes to search, complete the following procedure:

   a. Click Add Devices.

   b. Select the devices you want to search.

   c. Click OK.

4. If you want to search all nodes, click Select Nodes Directly, and then click All Nodes in the Database.
5. If you want to search a group of nodes that meet specific criteria, complete the following procedure:

   a. Click Select Nodes Directly

   b. Click Specify a Selection Criteria.

   c. Click Browse, and then click Add a Simple Condition.

   d. Click the first asterisk, and then click the appropriate field.

   e. If you want to change the comparison operator, click is equal to, and then select the comparison operator you want to use.

   f. Click the second asterisk, and then type the value or select it from the list.

   Note: All values currently in the database for the field are displayed when you browse the list.

6. Type the string of text you want to find in the Find field.
7. If you want to specify a date range for your search, complete the following procedure:

   a. Click ︽ to expand the search criteria pane.

   b. Set the date range for your search.

8. If you want to specify the type of configuration files to search, complete the following procedure:

   a. Click ︽ to expand the search criteria pane.

   b. Select the configuration types you want to search.

9. Click Start Search.
10. If you want to save the results of the search, click Save Results.

Deleting Configuration Files from the Database

As the Orion Platform database grows in size, you can delete existing configuration files from the database. If there is any chance you may need information you want to delete, back up your database.

To purge configs from the database:

1. Open the SolarWinds Network Configuration Manager application.
2. Note: If you do not have administrator privileges you may not be able to see some nodes.
3. Click Configs > Purge Old Configs.
4. If you want to delete configuration files from selected nodes, complete the following procedure:
    a. Click Add Devices.
    b. Select the devices you want to add to the list.
    c. Click OK.
5. If you want to delete configuration files from all nodes, click Select Nodes Directly, and then click All Nodes in the database.
6. If you want to delete configuration files from a group of nodes that meet specific criteria, complete the following procedure:
    a. Click Select Nodes Directly
    b. Click Specify a Selection Criteria.
    c. Click Browse, and then click Add a Simple Condition.
    d. Click the first asterisk and then click the appropriate field.
    e. If you want to change the comparison operator, click is equal to, and then click the comparison operator you want to use.
    f. Click the second asterisk, and then type the value or select it from the list.

    Note: All values currently in the database for the field are displayed when you browse the list.
7. Click the Select Purge Method tab.
8. If you want to remove configuration files older than a specific date, complete the following procedure:
    a. Click Purge all Configs downloaded before.
    b. Type the date or click the arrow to browse.
    c. If you want to specify the time of day, select Include Time, and then type or select a time from the list.
9. If you want to specify the number of configuration files to keep, complete the following procedure:

   a. Click Purge all Configs except the last 10.
   b. Adjust the slider to adjust the number of configuration files that should be kept in the database.

10. Click Purge.
11. When the purge completes, click Purge More Configs to delete more files, or click Done to close the window.

Automating Configuration File Purges

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

To schedule database configuration file purges:

1. Open the Orion Web Console and navigate to the NCM Jobs view (CONFIGS > Jobs).
2. If you are creating a new job, click **Create New Job**, select the appropriate job type, give the job a title.
3. If you want to edit an existing job, click **Edit**.
4. Select the schedule type.

   Basic gives you Once, Daily, Weekly, and Monthly schedule settings (start, end, recurrence). .

   Advanced gives you more granular control over the schedule, supporting more complex patterns defined with cron expressions.
5. If you are creating a Basic schedule, select the frequency of the job.

   Once: enter a day and time (at least 15 minutes from current NCM server time).

   Daily: Select Every Day or Every Week Day, enter a Start time, and then select start and end dates

   Weekly: Select the days, enter a Start time, and then select start and end dates.

   Monthly: Select the months, days of the month, enter a Start time, and then select start and end dates
6. If you are creating an Advanced schedule, use the five fields to create the appropriate cron expression.

For example, if you want the job to run once a week over every month at midnight on Sunday morning, the values for the fields would be 0 0 * * 0.

This transliterates as telling NCM to run the job at 0 minutes and 0 hours, on all valid days of month, in all valid months, on Sunday".

7. Add a comment as needed and then click **Next**.
8. Select the NCM nodes to target with this job.

   Select Nodes: Click Select Nodes and select the NCM nodes you want the job to target.

   All Nodes: Selects all NCM nodes as targets for the the job.

   Dynamic Selection: Define the criteria that NCM will use to determine the selection of NCM nodes as targets for the job.

   Nodes defined in legacy job scheduling system: Select the option and then click Yes, change selection.

   Note: Use this option to target the node group of all wireless access points in the database.
9. Select an email notification option.
   a. If you select Email Results, then enter the email from/to information.
   b. Enter the email server address and port number.
   c. If the email server expects credentials, then select Password.
   d. Enter the username and password.
10. Click **Next**.
11. Select a config purge option..

    If you want to purge configs before a specific date, select Purge all configs that were downloaded before this date, use the calendar tool to adjust the date. Click Include time and select a time if you want the purge to include those configs on the selected date that are timestamped before your selected time.

    If you want to delete all except a specific number of most recently downloaded configs, select Delete all configs except for the last XX current configs and insert an appropriate number.

    If you purge all configs except those falling within a recent time span, select Purge all configs except fort he last XX and select a interval.

    If you want to protect base configs as NCM takes action on your purge setting, select Do not purge any baseline configs.
12. Click **Next**.
13. Review the settings for the job.

14. When you are done reviewing the settings, click **Finish**.

Chapter 6

Modifying Device Templates

It may be necessary to create a new device template or modify a supplied template to add support for your device. Before attempting to create or modify device templates, review the following sections to ensure you have the information you need to succeed.

To configure user level device credentials:

1. Open Device Connectivity Method settings in SolarWinds NCM (File > Settings > Device Connectivity Method).
2. Select the option to manage devices using an individual set of credentials.
3. Under the Global Macro Settings, for Login Information, select Device.
4. Enter appropriate device login credentials (File > Change My Device Login Credentials).

Gathering the Information You Need

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

- What are the Machine Type and System OID values displayed in the Device Details tab of the node properties? You will use this information to save the device template with a unique name SolarWinds NCM recognizes, ensuring its use when connecting to the device.

- What command is used to disable pagination? This command is the value used in the template `RESET` command, for example, `terminal pager 0`.

- What command is used to reboot the device? This command is the value used in the template `Reboot` command, for example, `reload noconfirm`.

- What command is used to enter configuration mode? This command is the value used in the template `EnterConfigMode` command, for example, `config terminal`.

- What command is used to exit configuration mode? This command is the value used in the template `ExitConfigMode` command, for example, `quit`.

- What command is used to specify the startup configuration? This command is the value used in the template `Startup` command, for example, `startup`.

- What command is used to specify the running configuration? This command is the value used in the template `Running` command, for example, `running`.

- What command sequence is used to directly download the configuration using telnet or SSH? This command sequence is the value used in the template `DownloadConfig` command, for example, `show ${ConfigType}`. For more information about variables that can be used in command scripts and device command templates, see “Pre-Command and Command Template Variables” on page 141.

- What command sequence is used to upload the configuration using telnet or SSH? This command sequence is the value used in the template `UploadConfig` command, for example, `${EnterConfigMode}${CRLF}${ConfigText}${CRLF}${ExitConfigMode}`. For more information about variables that can be used in command scripts and device command templates, see “Pre-Command and Command Template Variables” on page 141.

- What command sequence is used to download the configuration using SNMP, that is, indirect transfer? This command sequence is used in the template `DownloadConfigIndirect` command, for example, `copy ${TransferProtocol}://${StorageAddress}/${StorageFilename}${ConfigType}${CRLF}${CRLF}`. For more information about variables that can be used in command scripts and device command templates, see “Pre-Command and Command Template Variables” on page 141.
- What command sequence is used to erase the configuration? This command sequence is used in the template `EraseConfig` command, for example, `write erase ${CRLF}Yes`.
- What command sequence is used to commit a configuration to memory? This command sequence is used in the template `SaveConfig` command, for example, `write memory`.
- What command sequence is used to show the version information? This command sequence is used in the template `Version` command, for example, `show version`.

Device Command Template Best Practices

Consult the following best practices before modifying device command templates.

- Review several device templates and familiarize yourself with the appropriate command syntax before creating a new template.

- Write down a list of all the commands you need to include in the new device template, including whether or not you have to press `Enter` after you type the command to ensure the device recognizes the command.

- Telnet to your device to find the pre-commands you need. A pre-command can be used for any device which requires input before prompting for credentials. A pre-command is used before logging in. For example, when you connect to a router and before you are asked for a password, you must press `Enter` to wake up the connection. Add the following line to the template: `<Command Name="PreCommand" Value="${CRLF}"/>`.

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

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

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

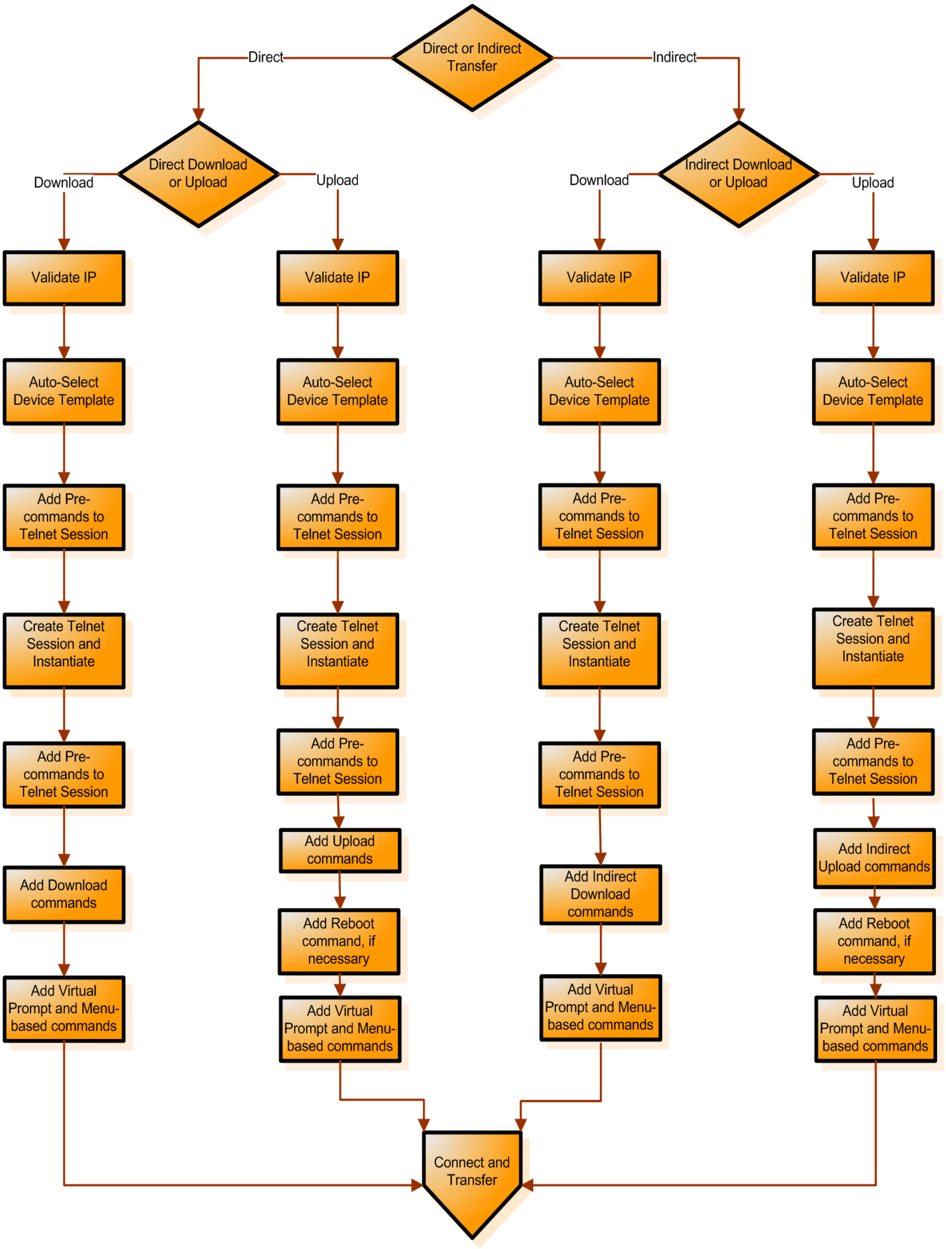
- Ensure that you do not have two command templates with the same System OID.

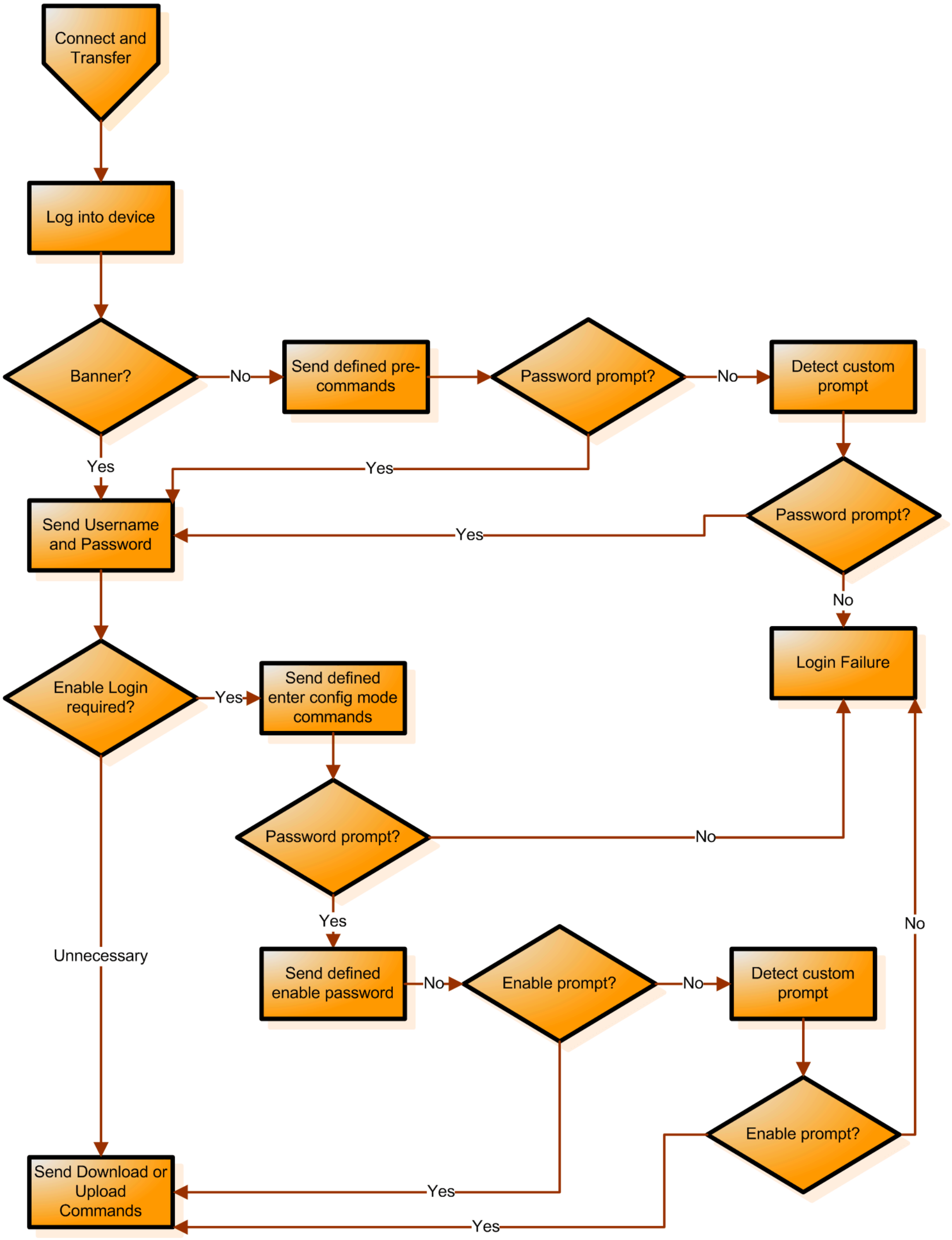
- If the value for the Command Device Template field within the Node Details view is set to Auto Determine, SolarWinds NCM will choose the command template with the System OID value that is closest to the system OID of the device. For example, if the System OID for the device is 1.3.6.1.9.25.5.4, then SolarWinds NCM will start 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 will then look 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, you want to use the full System OID when building templates.

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

- Some 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=""/>`.
- Not all commands are supported on all devices.

Communication Process Diagrams


Direct or Indirect Transfer
Direct
Indirect
Direct Download or Upload
Download
Upload
Indirect Download or Upload
Download
Upload
Validate IP
Validate IP
Validate IP
Validate IP
Auto-Select Device Template
Auto-Select Device Template
Auto-Select Device Template
Auto-Select Device Template
Add Pre-commands to Telnet Session
Add Pre-commands to Telnet Session
Add Pre-commands to Telnet Session
Add Pre-commands to Telnet Session
Create Telnet Session and Instantiate
Create Telnet Session and Instantiate
Create Telnet Session and Instantiate
Create Telnet Session and Instantiate
Add Pre-commands to Telnet Session
Add Pre-commands to Telnet Session
Add Pre-commands to Telnet Session
Add Pre-commands to Telnet Session
Add Download commands
Add Upload commands
Add Indirect Download commands
Add Indirect Upload commands
Add Reboot command, if necessary
Add Reboot command, if necessary
Add Virtual Prompt and Menu-based commands
Add Virtual Prompt and Menu-based commands
Add Virtual Prompt and Menu-based commands
Add Virtual Prompt and Menu-based commands
Connect and Transfer


Connect and Transfer
Log into device
Banner?
No
Send defined pre-commands
Password prompt?
No
Detect custom prompt
Yes
Yes
Send Username and Password
Password prompt?
Yes
No
Login Failure
Enable Login required?
Yes
Send defined enter config mode commands
Password prompt?
No
Yes
Unnecessary
No
Send defined enable password
No
Enable prompt?
No
Detect custom prompt
Enable prompt?
Send Download or Upload Commands
Yes
Yes

Creating or Modifying Device Templates

To add support for additional devices, you may need to create a new device template. You can also modify existing templates to add commands and to accommodate any custom commands your devices may have.

Note: Altering device command templates changes the way that SolarWinds Network Configuration Manager communicates with network devices. SolarWinds does not recommend altering a device command template file unless you have advanced knowledge and experience with device commands and variables.

To create or modify a device command template:

1. Close all SolarWinds Network Configuration Manager applications.
2. Open an existing device command template using a text editor, for example, notepad.exe. The default directory for device command templates is C:\Program Files\SolarWinds\Orion\NCM\DeviceTypes.
3. If you want to modify an existing command, apply the changes where applicable.

   For example, a device shows version information when you type show sys info. The current device command template shows <Command Name="Version" Value="show version"/>. The value needs to be changed to show sys info. The updated command is <Command Name="Version" Value="show sys info"/>.
4. If you want to create a new command, start a new line that opens with a command tag using the following format: <Command Name="CommandName" Value="commands"/>.

   For example, when you are manually logged into a device, you would type config terminal to enter the configuration mode. Therefore, the final command would be: <Command Name="EnterConfigMode" Value="config terminal"/>. For a list of commands and their descriptions, see “Command Template Commands” on page 139.

   Notes:

   Any command you add is available to the execute script engine. If you define some custom actions in the template and name them DO_MY_STUFF, you can use the variable ${DO_MY_STUFF} in a script, and SolarWinds NCM will resolve it to your commands.

   Any unresolved commands are left alone and the macro identifier (${Command}) will be sent to the device, where Command is the name of the command. This will usually cause the device to lock-up or behave erratically.
5. If you are modifying an existing template, save the file.

6. If you are creating a new device command template, save the file with a filename using the following format: DeviceType-SystemOID.ConfigMgmt-Commands. The DeviceType is available under Machine Type within the Node Details screen for SNMP enabled devices. The SystemOID can be found by clicking on the device in the SolarWinds NCM node tree and then clicking MIBs > System Info.

   Note: You can set up cascading templates by creating a series that targets slightly different OIDs. For example:

   1.3.6.1.4.1.9 = Cisco (All)

   1.3.6.1.4.1.9.1.23 = Cisco 2507

   You can specify a specific device with a more exact OID, and SolarWinds NCM will try to find the closest match. If SolarWinds NCM is talking to a device with a system OID of 1.3.6.1.4.1.9.1.25, it will use 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. Open SolarWinds Network Configuration Manager and connect to the device to test the new commands.

   Note: You may need to override the automatically selected template in the Device Details window to one you have customized.

Example CLI Device Command Templates

Two example device command templates for CLI devices are provided below. For a list of commands and their descriptions, see “Command Template Commands” on page 139.

Cisco IOS Example

This is an example device command template for a Cisco IOS device.

File Name

```
Cisco IOS-1.3.6.1.4.1.9.ConfigMgmt-Commands
```

Contents

```
<!--SolarWinds Network Management Tools-->

<!--Copyright 2008 SolarWinds.Net All rights reserved-->

<Configuration-Management Device="Cisco Devices" SystemOID="
1.3.6.1.4.1.9">

      <Commands>

            <Command Name="RESET" Value="terminal width
0${CRLF}terminal length 0"/>
```

```
             <Command Name="Reboot"
Value="reload${CRLF}y${CRLF}y"/>

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

             <Command Name="ExitConfigMode" Value="end"/>

             <Command Name="Startup" Value="startup"/>

             <Command Name="Running" Value="running"/>

             <Command Name="DownloadConfig" Value="Show
${ConfigType}"/>

             <Command Name="UploadConfig"
Value="${EnterConfigMode}${CRLF}${ConfigText}${CRLF}${ExitConfigMo
de}"/>

             <Command Name="DownloadConfigIndirect" Value="copy
${ConfigType}
${TransferProtocol}://${StorageAddress}/${StorageFilename}${CRLF}$
{CRLF}${CRLF}"/>

             <Command Name="UploadConfigIndirect" Value="copy
${TransferProtocol}://${StorageAddress}/${StorageFilename}
${ConfigType}${CRLF}${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

This following example device command template is for a Nortel BayStack 380.

File Name

```
Nortel Baystack380-1.3.6.1.4.1.45.3.45.ConfigMgmt-Commands
```

Contents

```
<!--SolarWinds Network Management Tools-->

<!--Copyright 2008 SolarWinds.Net All rights reserved-->

<Configuration-Management Device="Nortel BayStack 380 Devices"
SystemOID="1.3.6.1.4.1.45.3.45">
```

```
       <Commands>

              <Command Name="RESET" Value="terminal length 0"/>

              <Command Name="Reboot" Value="reload${CRLF}Yes"/>

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

              <Command Name="ExitConfigMode" Value="end"/>

              <Command Name="Startup" Value="configuration"/>

              <Command Name="Running" Value="running-config"/>

              <Command Name="DownloadConfig" Value="show
${ConfigType}"/>

              <Command Name="UploadConfig"
Value="${EnterConfigMode}${CRLF}${ConfigText}${CRLF}${ExitConfigMo
de}"/>

              <Command Name="DownloadConfigIndirect" Value="copy
${ConfigType}
${TransferProtocol}://${StorageAddress}/${StorageFilename}${CRLF}"
/>

              <Command Name="UploadConfigIndirect" Value="copy
${TransferProtocol}://${StorageAddress}/${StorageFilename}
${ConfigType}${CRLF}"/>

              <Command Name="Version" Value="show sys info"/>

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

       </Commands>

</Configuration-Management>\
```

Creating a Menu-Based Command Template

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

Complete the following procedure to create a menu-based device command template.

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 page 139.

Notes: 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}
  ```

  You could instead assign:

  ```
  Value= “1$[ENTER]7$[ENTER]”
  ```
- Login username and password have to be sent as PreCommand values instead of from the NCM Node Details configuration.

To do this:

1. Clear the username and password fields for the node in Login Information, and set Enable to <No Enable Login>.
2. Then use these PreCommands:

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

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

```
<Commands>

        <Command Name="RESET" Value=""/>

        <Command Name="Reboot" Value=""/>

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

        <Command Name="ExitConfigMode" Value=""/>

        <Command Name="Startup" Value=""/>

        <Command Name="Running" Value=""/>
```

```
              <Command Name="DownloadConfigIndirect"
Value="${Downarrow}${Downarrow}${Downarrow}${Downarrow}${Downarrow
}${Downarrow}${Downarrow}${Downarrow}${Downarrow}${CRLF}${CRLF}${S
torageFilename}${CRLF}${DownArrow}${StorageAddress}${CRLF}${DownAr
row} ${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}${DownArrow}${DownArrow}${DownArrow}${DownArrow}${CRL
F}" RegEx="Event Log"/>

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

       </Commands>
```

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 procedure:

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 two times and then press Enter, then 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 will now be: <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 (↓) 9 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 downloading process

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

   ${Downarrow}${Downarrow}${Downarrow}${Downarrow}${Downarrow}

   ${Downarrow}${Downarrow}${Downarrow}${Downarrow}

   ${CRLF}

   ${CRLF}

   ${StorageFilename}${CRLF}

   ${DownArrow}${StorageAddress}${CRLF}

   ${DownArrow} ${CRLF}

Note: For a list of commands and their descriptions, see “Command Template Commands” on page 139.

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

6. Add a delay between keystrokes by adding the following attribute: Delay="300".

7. The complete download command is as follows: <Command Name="DownloadConfigIndirect" Value="${Downarrow}${Downarrow}${Downarrow}${Downarrow}${Downarrow}${Downarrow}${Downarrow}${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 SolarWinds NCM device templates. 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.

Property	**Description**
DownloadConfig	Series of commands used to download a configuration from a device
DownloadConfigIndirect	Series of commands used to download a configuration indirectly from a device using TFTP.
EnableCommand	Allows you to declare a custom enable command for those devices that do not use `Enable` as the command.
EnableIdentifier	Only used when a device does not return the "#" symbol at the end of a prompt to indicate enable mode. Declare the value displayed while in enable mode for a device.
EnterCLI	Specifies the commands to send upon receiving the VirtualPrompt value 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” on page 141.
EnterConfigMode	Series of commands used to enter the configuration mode of a device
ExitConfigMode	Series of commands used to exit the configuration mode of a device
IPAddress	The IP address of the server where SolarWinds Network Configuration Manager is installed

Property	Description
MenuBased	Specifies whether the device is menu or cli based. If a device is menu based and you can switch it to CLI from the menu, use the VirtualPrompt and EnterCLI commands to do so. Valid values are `true` or `false`.
MenuDrivenConfigStart	Allows you to declare a value after which the transmitted data is considered the config requested from the menu-driven device. For example, in the Cisco VPN Concentrator device template, the declared value is `##########`. The information sent after the ten hash signs is saved as the requested configuration file.
More	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.
Precommand	Specifies the device requires a pre-command. For more information and valid pre-command variables, see "Pre-Command and Command Template Variables" on page 141.
Reboot	Series of commands used to reboot the device
RebootAt	Series of commands used to reboot a device at a specified time. Use the variables listed in the "Configuration Archive Variables" section on page 368 to assign the date and time.
RESET	Series of commands used to set the length and pagination of the session
Running	Value used to specify a running configuration type
SaveConfig	Series of commands used to write the configuration to the devices memory
Startup	Value used to specify a startup configuration type.
UploadConfig	Series of commands used to upload a configuration to a device
UploadConfigIndirect	Series of commands used to upload a configuration indirectly to a device using TFTP.
Version	Series of commands used to display the software version of the device.
VirtualEnablePrompt	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, also.
VirtualPrompt	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.

Pre-Command and Command Template Variables

Pre-Command variables are used within command scripts as well as within device command templates. The Pre-Command variables mimic keyboard strokes that are normally entered in the command interface. For more information on creating command scripts, see "Working with Command Scripts" on page 147.

Property	Description
${ConfigType}	Value used to insert the type of configuration
${CR}	Carriage return
${CRLF} or $[ENTER]	Carriage return - linefeed combination
${CTRL+@}	CTRL + @
${CTRL+A}	CTRL + A
${CTRL+B}	CTRL + B
${CTRL+C}	CTRL + C
${CTRL+D}	CTRL + D
${CTRL+E}	CTRL + E
${CTRL+F}	CTRL + F
${CTRL+G}	CTRL + G
${CTRL+H}	CTRL + H
${CTRL+I}	CTRL + I
${CTRL+J}	CTRL + J
${CTRL+K}	CTRL + K
${CTRL+L}	CTRL + L
${CTRL+M}	CTRL + M
${CTRL+N}	CTRL + N
${CTRL+O}	CTRL + O
${CTRL+P}	CTRL + P
${CTRL+Q}	CTRL + Q
${CTRL+R}	CTRL + R
${CTRL+S}	CTRL + S
${CTRL+T}	CTRL + T
${CTRL+U}	CTRL + U
${CTRL+V}	CTRL + V
${CTRL+W}	CTRL + W

Property	Description
${CTRL+X}	CTRL + X
${CTRL+Y}	CTRL + Y
${CTRL+Z}	CTRL + Z
${CTRL+[}	CTRL + [(equivalent to ESC key press)
${CTRL+\}	CTRL + \
${CTRL+]}	CTRL +]
${CTRL+CTRL}	CTRL + CTRL
${CTRL+_}	CTRL + _
${UPARROW}	Up Arrow
${DOWNARROW}	Down Arrow
${RIGHTARROW}	Right Arrow
${LEFTARROW}	Left Arrow
${StorageAddress}	Value used to insert the TFTP server IP address or hostname.
${StorageFilename}	Value used to insert the name generated by SolarWinds NCM for the downloaded configuration file.
${TransferProtocol}	Value used to insert the transfer protocol used during indirect transfer.

Example Pre-Command Device Template Entry

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

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

Note: Device command templates are located in the `DeviceTypes` folder of your installation folder. By default, you can find this folder in the following location: `\Program Files\SolarWinds\Configuration Management\DeviceTypes\`.

Using Command Template Variables to Preclude Pseudoterminal Setup

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

```
<Command Name=”allocatePty” Value=”false”/>
```

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

Using Command Template Variables to Declare a Special Command Prompt

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

```
<Command Name=”MenuBased” Value=”false”/>
```

Specifies that the template logic should run in CLI mode

```
<Command Name=”VirtualPrompt” Value=”CustomPrompt%”/>
```

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

Using Command Template Variables to Switch User Context

If you Login on a device and must switch user context to execute a command,, resulting in a different command prompt, use the following example to guide you in how to handle switching 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 the context of the switch and the new prompt to expect. Use pre-command variables to designate the switch context commands and specify the entire new prompt in the RegEx value.

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

If you Login on a device and perform an action and are then prompted for interaction (for example, you receive a press any key prompt) consult the following example commands in the command template to avoid timing out.

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

Sent when the device does not respond for 3 seconds

```
<Command Name=”PreCommand” Value=”${CTRL+Y}” Delay=”5”/>
```

Sent when the device does not respond for more than 3 seconds

```
<Command Name=”PreCommand” Value=”${CTRL+Y}” Delay=”5”
RegEx=”press any key”/>
```

Sent when the device does not respond for more than 3 seconds and the last received data was `press any key`.

Troubleshooting Device Connections

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

To troubleshoot a device connection issue with a session trace:

1. Open the Orion Web Console.
2. Click Settings.
3. Click NCM Settings.
4. Click Advanced.
5. Select Enable Session Tracing.
6. Perform the steps to recreate the issue you are troubleshooting.
7. Open the session trace file to discover what is causing the error. The default location for session trace files is C:\Program Files\SolarWinds\Orion\NCM\Session-Trace.
8. Apply the necessary changes to the device command template to resolve the issue. For more information, see “Creating or Modifying Device Templates”.

Chapter 7

Working with Command Scripts

SolarWinds Network Configuration Manager allows you to accomplish several tasks through the creation and execution of command scripts. Consider the following tasks you can simplify by using command scripts.

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

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

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

Executing Command Scripts

Complete the following procedure to create and execute a command script.

Note: 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; Telnet and SSH communication are supported.

To create and execute a command script:

1. Click Nodes > Execute Command Script.
2. If you want to select the nodes on which to run the script, complete the following procedure:
   a. Click Add Devices.
   b. Select the devices on which you want to run your command script.
   c. Click OK.
3. If you want to run the script on all nodes, click Select Nodes Directly, and then click All Nodes in the Database.

4. If you want to run the script on a group of nodes that meet specific criteria, complete the following procedure:

   a. Click Select Nodes Directly.

   b. Click Specify a Selection Criteria.

   c. Click Browse, and then click Add a Simple Condition.

   d. Click the first asterisk, and then click the appropriate field.

   e. If you want to change the comparison operator, click is equal to, and then select the comparison operator you want to use.

   f. Click the second asterisk, and then type the value or select it from the list.

   Note: All values currently in the database for the field are displayed when you browse the list.

5. If you want to type a new script, type the script in the Command Script to Execute field.

   Note: Scripts can consist of a single command or list of commands to be executed sequentially. Scripts should mirror commands entered when manually typing instructions from the command prompt. For example, when sending the show version command to a router via a TELNET session, the prompt requires the user to type s version. The command script must mimic this entry. For example, type s version with a carriage return at the end of the line.

6. If you want to load a previously saved script, complete the following procedure:

   a. Click Load Script.

   b. Browse to the script you want to load, and then click Open.

   Note: To view sample scripts, browse to the \Sample Scripts folder.

7. If you want to see results that meet specific criteria, complete the following procedure:

   a. Click ⏫.

   b. Select Filter Results that Match a Pattern.

   c. Type the string you want SolarWinds Network Configuration Manager to use for filtering. For example, adding the word Serial to the filter displays lines that start with the word Serial. For more information on pattern matching, see “Regular Expression Pattern Matching” on page 371.

   Note: The example script Get Serial Number from each Device.txt demonstrates this feature.

8. If you want to write the results of a script to a file, complete the following procedure:
   a. Click ︽.
   b. Select Save Results to a File.
   c. Type or browse to the path and filename for the log file.
9. If you want to hide script commands when the script is executed, complete the following procedure:
   a. Click ︽.
   b. Unselect Show Commands in Output.
10. Click Execute Command Script.
11. If you want to save the results of the script, click Save Results.

    Note: Unselecting Outline View displays results without formatting.
12. If you want to save the script for later use, complete the following procedure:
    a. Click the Execute Script tab.
    b. Click Save Script.
    c. Type a filename, and then click Save.

Using Variables within Scripts

The power of the SolarWinds Network Configuration Manager scripting engine is highlighted by the ability to use variables within scripts. Variables always begin with a dollar sign and a curly brace (`${`) and end with a curly brace (`}`).

Script variables substitute the appropriate commands based on the device type. For example, the variable `${EnterConfigMode}` parses as "config terminal" when communicating with Cisco IOS devices, but parses as "configure" when communicating with an HP Procurve Switch.

For more information about variables that can be used in command scripts and device command templates, see “Command Template Commands” on page 139.

Example Variable Script

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

```
${EnterConfigMode}

no snmp-server community public RO

${ExitConfigMode}
```

```
    ${SaveConfig}
    ${Reboot}
```

Parsed for Cisco IOS devices:

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

Parsed for a Dell PowerConnect Switch:

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

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

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.

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`, and then define another variable that includes the first, `Reveal = show ${ShowInt}`. When you call the Reveal variable, `${Reveal}`, it equals `show running | include interface`. For more information about variables that can be used in command scripts and device command templates, see “Command Template Commands” on page 139.

Chapter 8

Working with Config Change Templates

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

With a single config change template you can generate and execute accurate sets of CLI commands to perform a specific task on many different machine types in a network of variable size.

The following sections introduces, explains, and provides examples of config change template components.

Config Change Template Basics

A change config template enables an NCM user to accomplish a specific device configuration task for a set of NCM managed nodes. In this case the term “template” describes the runtime wizard through which the user selects the NCM nodes/interfaces targeted for the change, and the script behind the wizard the articulates the logic of the configuration change itself.

In terms of configuration change workflow, an IT manager would create the script for a template and other members of the team would use the template’s wizard to perform the specific configuration changes on some set of NCM managed nodes.

Most fundamentally, the framework for creating config change templates depends on the SolarWinds Information Service (SWIS), an API installed with NCM that interacts with inventory data in the 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.

Here are some of the routine config changes you can expedite with config change templates:

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

Preparation and Use of a Template

Every change config template does its work based on NCM device inventory objects (the database “entities” that the SolarWinds Information System accesses in managing NCM’s communication with its database).. As a result, performing an NCM device inventory, and updating device inventories, are the prerequisites for creating and running a config change template.

See the section “SolarWinds Information Services Data Entities” for all the NCM device entities and their properties that you can use in the context of 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. To do that the user must know the basics of writing a script that uses a set of commands, variables, logical structures (foreach loops, if/else conditional statements and operators.

When executed, a config change template exposes a wizard that prompts for imput and uses input values to generate necessary CLI commands needed to accomplish a specific config change on target NCM devices. Based on input, the template's runtime wizard generates a different set of commands for each type of device that the NCM user specifies 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**: A user enters values based on a template's runtime wizard input prompts, reviews the CLI commands the template outputs for each type of targeted device, and tells NCM to execute the commands against targeted NCM devices, making specific config changes.

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

Parts of a Template

Every config change template includes two parts:

- **Parameters**

Through descriptions, parameters tell a user about the template's purpose; and through labels parameters prompt the user for the values (for example, the specific node(s) on which to make the template's specific config change.

- **Commands**

Through arguments, commands declare the input type (int, string, entity) for a variable; and through logical operations (foreach loops,

include arguments and operations needed for NCM to produce a set of CLI commands and execute them 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 use about the template and associate a description or label with a variable in the template's user interface; 2 defining the commands, arguments, and operations that set the input type for variables and lead NCM to generate at runtime the accurate set of CLI statements for each NCM node the template user chooses to target.

Understanding Config Change Template Details

A config change template called “Change VLAN Membership on Ports – Cisco IOS” automatically installs with 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 Port—Cisco IOS” template to make VLAN membership config changes on some hypothetical Cisco device interfaces.

Viewed as parsable code, a config change template consists of two parts:

- **Parameters**

  This part defines names and descriptions of the interface wizard fields associated with the variables that the user delimits when the config change template is executed.

- **Commands**

  This part defines the variables and their data structures on which the `script` command operates when the config change template is executed, and how the relevant data is parsed. Currently variables can be of type int, string, or entity. It is also possible to have a list type of int, string, or entity. The **context node** is the node that is targeted for the config change and of whose inventory data the config change template makes use at runtime.

  This part also includes native CLI commands that are parsed inline.

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, conditional statements (if/else), and logical operators in creating system administration scripts.

Before we discuss the the different parts of a change config template, here is our entire reference template broken up into parameter, command, and output sections.

Reference Template: Parameters

Here are the parameters for the “Change VLAN Membership on Ports – Cisco IOS” template. Notice that the parameters already have values (either a string or a variable) associated with them.

```
/*

.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) you would like to remove. Selecting
VLANs irrelevant to interfaces simply will result in no actions
taken for those interfaces.



.PARAMETER_LABEL @VlanToAssign

        VLAN to assign

.PARAMETER_DESCRIPTION @VlanToAssign

        Select the VLAN you would like to assign.

*/
```

Reference Template: Commands

Here are the commands for the “Change VLAN Membership on Ports – Cisco IOS” template. Notice that there is one instance of the script command and multiple instances of the CLI{ } command and that all variables have declarations.

```
script ConfigureVLANmembershipCiscoIOS (
                            NCM.Nodes @ContextNode,
                            NCM.Interfaces[] @TargetPorts,
                            NCM.VLANs[] @VlansToRemove,
                            NCM.VLANs @VlanToAssign           )
{
  // Enter configuration mode
  CLI
  {
   configure terminal
  }

  // Loop through selected ports
  foreach (@portItem in @TargetPorts)
  {
    CLI
    {
       interface @portItem.InterfaceDescription
    }

    // Loop through list of vlans to remove
    foreach (@vlanRemove in @VlansToRemove)
    {
       CLI
       {
          no switchport access vlan @vlanRemove.VLANID
       }
    }
    CLI
    {
       switchport access vlan @VlanToAssign.VLANID
    }

    CLI
    {
       exit
    }
  }

  // Exit configuration mode
  CLI
  {
    exit
  }
}
```

Reference Template: Output

Here are output commands for the “Change VLAN Membership on Ports – Cisco IOS” template. These are the commands that NCM executes after loggin in on the NCM device(s) selected as the target for the config changes this config change template is designed to make.

Notice that we are changing VLAN membership on one interfaces of two different Cisco swtiches.

NCM Node bgp-2651-03

```
configure terminal
```

```
interface FastEthernet0/0

no switchport access vlan 1004

switchport access vlan 1002

exit

end
```

NCM Node cur-3725

```
Configure terminal

interface FastEthernet0/1

no switchport access vlan 1004

switchport access vlan 1002

exit

end
```

Setting-up Parameters

The parameters of 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 inlcudes at least these 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 (@<variable_name>):

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 runtime 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 runtime wizard itself.

PLATFORM DESCRIPTION

> This parameter defines the type of NCM deivce (for example, “Cisco IOS”) 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 runtime 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 (description of the data) so that the user knows for what the variable is holding a place.

For example, PARAMETER_LABEL is used in every template with the @ContextNode variable whose value the user sets by selecting the 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 in which the NCM nodes are selected in the template's runtime wizard.

A config change template may have as many instances of PARAMETER_LABEL as needed to support the user input needed to do the work for which the template script is designed. See the section XXX for specific examples of how this parameter is used in practice.

PARAMETER_DESCRIPTION

This parameter always appears after PARAMETER_LABEL holds the explanatory text for an input field.

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."

Additionally, some templates may also include:

PARAMETER_DISPLAY_TYPE.

This parameter enables you to create a dropdown list of options. The format for using this parameter is:

```
PARAMETER_DISPLAY_TYPE @VariableName

Listbox:1=String1|2=String2|3=String3
```

Where the pipe character divides the items in the list.

Example: Configuring VLAN Membership

Taking the “Change VLAN membership on ports Cisco IOS” template as our example. here is the section with parameter definitions:

```
/*

.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) you would like to remove. Selecting
VLANs irrelevant to interfaces simply will result in no actions
taken for those interfaces.



.PARAMETER_LABEL @VlanToAssign

        VLAN to assign

.PARAMETER_DESCRIPTION @VlanToAssign

        Select the VLAN you would like to assign.

*/
```

As expected, there is a single CHANGE_TEMPLATE_DESCRIPTION and an actual description that tells us what executing the template does.Similarly, there is one instance each of CHANGE_TEMPLATE_TAGS and PLATFORM_DESCRIPTION that tell us, respectively, how the template can be organized (by Cisco, IOS, VLAN Membership) in the Config Change Template resource in NCM, and that this template is designed for NCM devices that are running Cisco's IOS.

There are three instances of PARAMETER_LABEL in this template, each one associated with a different variable that it labels (NCM Node, Select Ports, VLAN to remove, VLAN to assign). When we run this config change template, we should expect to provide values in the template wizard's runtime interface for the NCM nodes to target for changes, the ports on those nodes, and possibly a VLAN to remove from these ports, and a VLAN to assign to the selected ports.

Basic Commands

There are two commands in a config change template:`script` and `CLI`.

The `script{}`command declares the input type of every variable that the template will use.

The CLI{ } command defines a specific CLI command that NCM will issue on a target device when the config change template is executed by a user.

Script command

`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 )
```

```
where,

data_type can be ‘swis.entity’ (for example, ‘NCM.Nodes’), ‘int’
(integer), or ‘string’.
```

Example for `script`: Configuring VLAN Membership (Cisco IOS)

Again, taking the “Change VLAN membership on ports Cisco IOS” template as our example, here is the single instance of the `script` command:

```
script ConfigureVLANmembershipCiscoIOS (
                                    NCM.Nodes @ContextNode,
                                    NCM.Interfaces[] @TargetPorts,
                                    NCM.VLANs[] @VlansToRemove,
                                    NCM.VLANs[] @VlanToAssign
)
```

Here we see all four variables introduced in the parameter section of the template with an instance of PARAMETER_LABEL given a specific SolarWinds Information Service entity data type. The value of @ContextNode will be determined with data from the NCM.Nodes entity in the database; the value of @TargetPorts will be determined with data from the NCM.Interfaces entity; the value of @VlansToRemove and VlansToAssign will both be determined with data from the NCM.VLANs entity.

Note: Any variable that references an NCM object of which NCM knows through device inventory must take a SolarWinds Information Services entity as its data type. So in this case @ContextNode, @TargetPorts, @VlansToRemove, and @VlanToAssign are all going to work with data that NCM has 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, then NCM will fail to correctly parse your script.

CLI command

The purpose of a CLI { } command 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 brackets { }. At runtime 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.

Example for `CLI{ }`: Entering Config Mode (Cisco IOS)

To enter config mode on Cisco IOS devices you type `configure terminal`. In your config change template script, you would include the command in this form:

```
CLI

  {

   configure terminal

  }
```

In this case 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 runtime:

Example for `CLI{ }`: Configuring VLAN Membership (Cisco IOS)

This second example shows a similar CLI statement but with variables to specify VLAN properties while using the ‘vlan database’ command line editor.

Let’s review the `script` command example in which “Change VLAN membership on ports Cisco IOS” template’s variables are given data types:

```
script ConfigureVLANmembershipCiscoIOS (
                                    NCM.Nodes @ContextNode,
                                    NCM.Interfaces[] @TargetPorts,
                                    NCM.VLANs[] @VlansToRemove,
                                    NCM.VLANs @VlanToAssign)
```

We recall that all the variables are given the SolarWinds Information Service entity data type.

And here is the `CLI{ }` statement that immediately follows:

```
CLI

{

vlan database

vlan @vlanid

description @vlandesc

exit

}
```

For purposes of demonstration, we assume that the variable @vlanid has been set to 1 and @vlandesc has been set to Local-Office. So NCM at runtime 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 admittedly trivial result of a user running the template would be to set the description of vlan 1 to ‘Local Office’ on all NCM nodes selected as targets for the config change.

But the “Change VLAN membership on ports Cisco IOS” config change template actually changes the VLANs associated with targeted NCM node ports. For that we need to introduce some advanced CLI{ } command logic.

Advanced Commands

The scripting framework for change config templates allows you to create `CLI { }` command arguments that include interation loops (foreach), conditional operations (if/else), and functions for manipulating string patterns.

These sections provide explanation for each type of advanced command argument and offers examples for how advanced arguments might play a role in our references template, “Change VLAN Membership on ports Cisco IOS,: which changes VLAN membership for interfaces on selected NCM nodes.

Foreach Loops

A foreach statement iterates through an array of items based on a SWIS entity data type. Foreach statements use the following pattern:

```
foreach (@ItemVaraible in @EntityArrayVariable).
```

A primary purpose of a foreach loop is to allow the template user to select multiple NCM objects for config change; the loop instructs NCM to perform the same config change on all items in scope as determined by the SWIS entity in the database and delimited at runtime by the template user’s selections in the template wizard.

Example for `foreach{ }`: Select Interface(s) for VLAN Membership Changes

In the “Change VLAN Membership on ports Cisco IOS” template we have been using as an extended example, after the script puts the targeted NCM nodes in config mode, and creates the description “Local Office” for VLAN 1, we encounter these lines:

```
  foreach (@portItem in @TargetPorts)

  {
```

```
CLI

{

   interface @portItem.InterfaceDescription

}
```

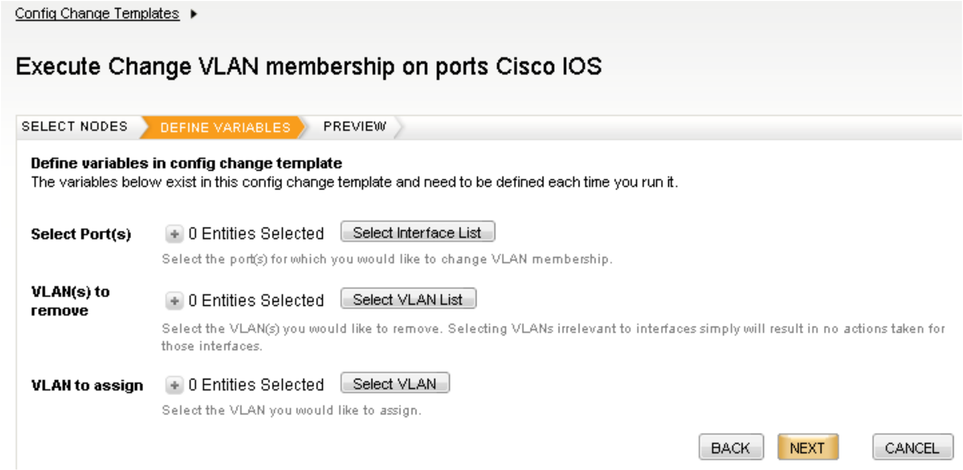
In this case the `foreach ( )` statement creates a set that contains two related variables, @portItem and @TargetPorts.

We know from our example of the `script` command for this template that the variable @TargetPorts holds an array of objects with the data type of a SWIS entity called NCM.Interfaces[ ]. The array will be a set of interfaces on NCM nodes.

We also recall that @TargetPorts is the variable associated with the PARAMETER_LABEL “Select port(s)” and that the template user selects one or more ports at runtime. So 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.

Finally, the @portItem in `foreeach (@portItem in @TargetPorts)` is a dynamic variable that the loop uses during its iterating to hold the value of the current interface from the array of interfaces represented by @TargetPorts. You could use any name for the dynamic variable but in any NCM expects your foreach statement to include one; so that the format of the foreach loop is always `foreach (@ItemVaraible in @ArrayVariable).`

Here is the template wizard screen with which the user must interact:



Config Change Templates ▸

Execute Change VLAN membership on ports Cisco IOS

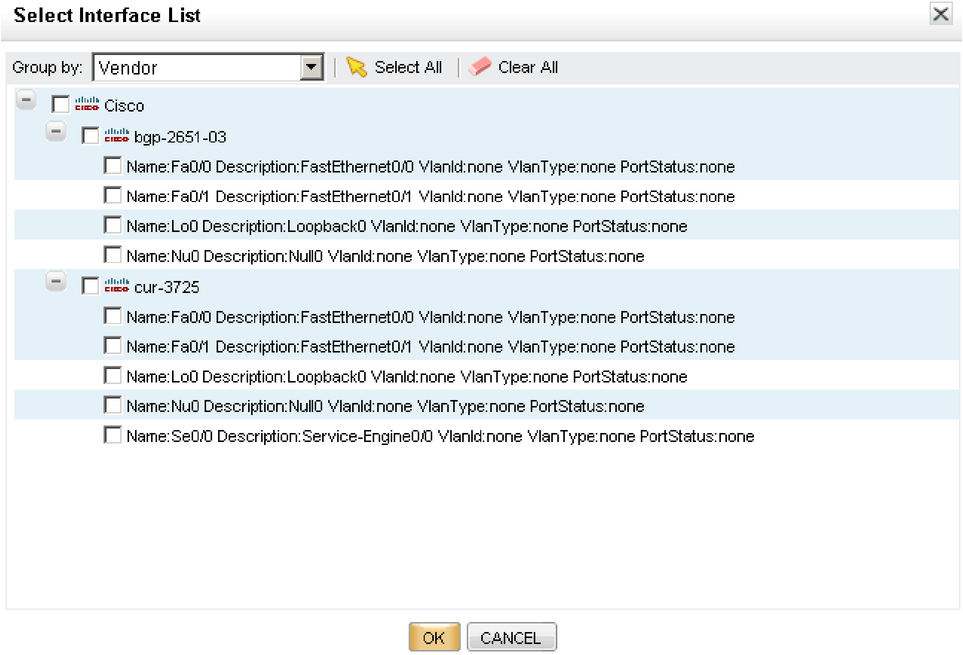
Define variables in config change template
The variables below exist in this config change template and need to be defined each time you run it.

Select Port(s) 0 Entities Selected
Select the port(s) for which you would like to change VLAN membership.

VLAN(s) to remove 0 Entities Selected
Select the VLAN(s) you would like to remove. Selecting VLANs irrelevant to interfaces simply will result in no actions taken for those interfaces.

VLAN to assign 0 Entities Selected
Select the VLAN you would like to assign.

Clicking on Select Interface List brings up a tree that shows the NCM nodes previously selected in the wizard and lists the available interfaces:



Group by: Vendor

- ☐ Cisco
  - ☐ bgp-2651-03
    - ☐ Name:Fa0/0 Description:FastEthernet0/0 VlanId:none VlanType:none PortStatus:none
    - ☐ Name:Fa0/1 Description:FastEthernet0/1 VlanId:none VlanType:none PortStatus:none
    - ☐ Name:Lo0 Description:Loopback0 VlanId:none VlanType:none PortStatus:none
    - ☐ Name:Nu0 Description:Null0 VlanId:none VlanType:none PortStatus:none
  - ☐ cur-3725
    - ☐ Name:Fa0/0 Description:FastEthernet0/0 VlanId:none VlanType:none PortStatus:none
    - ☐ Name:Fa0/1 Description:FastEthernet0/1 VlanId:none VlanType:none PortStatus:none
    - ☐ Name:Lo0 Description:Loopback0 VlanId:none VlanType:none PortStatus:none
    - ☐ Name:Nu0 Description:Null0 VlanId:none VlanType:none PortStatus:none
    - ☐ Name:Se0/0 Description:Service-Engine0/0 VlanId:none VlanType:none PortStatus:none

So to finish this part of the example: let’s assume that in the template’s runtime wizard the user selects the interfaces FastEthernet0/0 on node bgp-2651 and FastEthernet0/1 on node cur-3725. When the user executes the template NCM replaces @portItem.InterfaceDescription with "FastEthernet0/0" and “FastEthernet0/6” in the two iterations of the foreach ( ) loop. Two iterations in this case since the user selected only two interfaces on which to perform the template’s config change. The result is that the CLI { } command parses to both:

```
 CLI

{

   interface FastEthernet0/0

}

 CLI

{

   interface FastEthernet0/1

}
```

Each interface command statement goes with its appropriate node selection. So far, for the two NCM nodes targeted for the config change, NCM will be passing these commands after logging on the Cisco device:

NCM Node bgp-2651-03

```
configure terminal

interface FastEthernet0/0

...
```

NCM Node cur-3725

```
Configure terminal

interface FastEthernet0/1

...
```

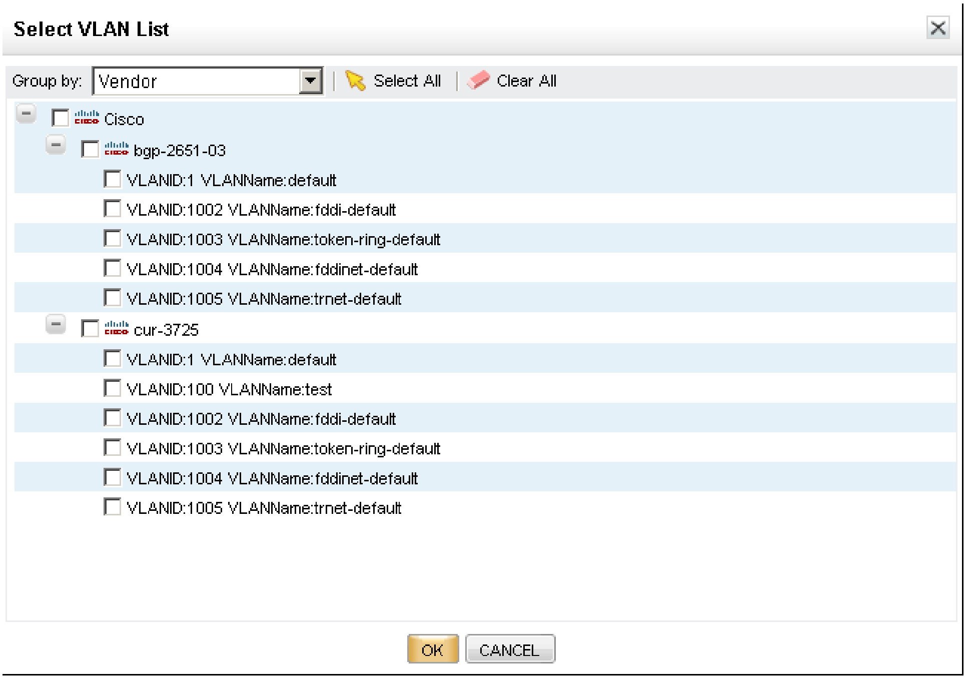
Example for `foreach{ }`: Select Interface(s) for VLAN Membership Changes

The next part of the script in our reference template is another CLI{ } comand with foreach ( ) loop. The loop in this case instructs NCM to remove VLAN access on the targeted NCM node interfaces for specific VLANs.

```
    foreach (@vlanRemove in @VlansToRemove)

    {

       CLI

       {

          no switchport access vlan @vlanRemove.VLANID

       }

    }
```

Recall that the variables @VlansToRemove and @VlantoAssign are each assigned the NCM.VLANs SWIS entity as a data type. The important diference is that @VlansToRemove is assigned the data type as an array (the user is able to select multiple VLANs in the template wizard) and @VlanToAdd is assigned the data type as a single object (allowing the user to select one VLAN fore each interface).

We have previously supposed that the user has selected interfaces FastEthernet0/0 on node bgp-2651-03 and FastEthernet0/1 on node cur-3725 as targets for the VLAN membershipt changes. And now the user must choose the VLANs to remove from those interfaces.



Select VLAN List

Group by: Vendor | Select All | Clear All

- ☐ Cisco
  - ☐ bgp-2651-03
    - ☐ VLANID:1 VLANName:default
    - ☐ VLANID:1002 VLANName:fddi-default
    - ☐ VLANID:1003 VLANName:token-ring-default
    - ☐ VLANID:1004 VLANName:fddinet-default
    - ☐ VLANID:1005 VLANName:trnet-default
  - ☐ cur-3725
    - ☐ VLANID:1 VLANName:default
    - ☐ VLANID:100 VLANName:test
    - ☐ VLANID:1002 VLANName:fddi-default
    - ☐ VLANID:1003 VLANName:token-ring-default
    - ☐ VLANID:1004 VLANName:fddinet-default
    - ☐ VLANID:1005 VLANName:trnet-default

OK | CANCEL

Let’s assume the user chooses for both NCM nodes to disable VLAN 1004 access to the selected device interface(s) and to enable VLAN 1002 access on the same interfaces.

This means that when the user, having selected desired values in the template wizard, clicks Execute at the end of the wizard, the specific `foreach(@vlanRemove in @VlansToRemove)` loop that is part of the CLI { } command that removes VLAN access to selected interfaces will pass in VLANID 1004 as the selected value of the @vlanRemove.VLANID variable. The variable @vlanRemove.VLANID represents the source of value from which the user selects; specifically, @vlanRemove was declared as data type SWIS entity NCM.VLANs[ ], and VLANID is one of the properties of that entity.Though the data type is an array, allowing the user to select multiple objects if desired, we are selecting only the single object VLANID 1004.

Now, for the two NCM node interfaces targeted for the config change, NCM will be passing these commands after logging on the Cisco device:

NCM Node bgp-2651-03

```
configure terminal

interface FastEthernet0/0

no switchport access vlan 1004
```

```
...
```

NCM Node cur-3725

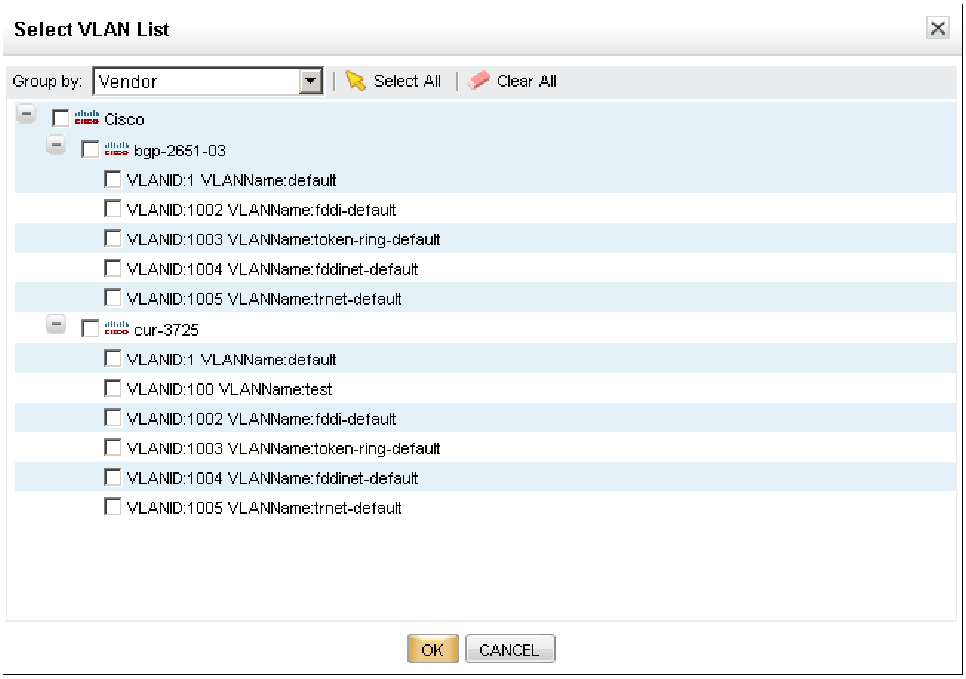
```
Configure terminal

interface FastEthernet0/1

no switchport access vlan 1004

...
```

The final part of the script in our reference template defines the VLAN that will be assigned to interfaces FastEthernet0/0 on node bgp-2651-03 and FastEthernet0/1 on node cur-3725.

Notice that the CLI { } command in this case does not include a foreach { } loop:

```
    CLI

    {

       switchport access vlan @VlanToAssign.VLANID

    }
```

As a result the user can only assign one VLAN access to the selected device interfaces in the template wizard.



Group by: Vendor

- □ Cisco
  - □ bgp-2651-03
    - □ VLANID:1 VLANName:default
    - □ VLANID:1002 VLANName:fddi-default
    - □ VLANID:1003 VLANName:token-ring-default
    - □ VLANID:1004 VLANName:fddinet-default
    - □ VLANID:1005 VLANName:trnet-default
  - □ cur-3725
    - □ VLANID:1 VLANName:default
    - □ VLANID:100 VLANName:test
    - □ VLANID:1002 VLANName:fddi-default
    - □ VLANID:1003 VLANName:token-ring-default
    - □ VLANID:1004 VLANName:fddinet-default
    - □ VLANID:1005 VLANName:trnet-default

Let’s assume the user chooses for both NCM nodes to enable VLAN 1002 access to the selected device interface(s).

As with VLANs to remove, NCM uses the selection of the VLAN to assign as the value for the variable @VlansToAssign.VLANID. And the next config-changing output commands executed through this config change template are:

NCM Node bgp-2651-03

```
configure terminal

interface FastEthernet0/0

no switchport access vlan 1004

switchport access vlan 1002

...
```

NCM Node cur-3725

```
Configure terminal

interface FastEthernet0/1

no switchport access vlan 1004

switchport access vlan 1002
```

```
...
```

Conditional Statements

We have already completed a walk-through of the “Change VLAN membership on ports Cisco IOS” config change template as it is included with SolarWinds NCM during installation.

However, we can imagine a scenario in which you would modify the existing “Change VLAN membership on ports Cisco IOS” template to make use of additional scripting resources.This section explains how to create conditional logic.

Conditional logic in a config change template script involves using 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:

```
If (condition is true)

CLI

{

execute commands

}

Else

CLI

{

execute other commands

}
```

Note: The `else` section is optional; if you omit it, and the ‘if’ condition is false, NCM excludes the relevant CLI{ } commands from the template output. For example, `if (@ITF.Name=='FastEthernet0/1')`; if the variable `@ITF.Name`

Use any of these operators to specify a parenthetical condition:

```
== Is Equal To

> Is Greater Than

>= Is Greater Or Equal To

< Is Less Than

<= Is Less Or Equal To

!= Is Not Equal To

Contains

containsExact (case sensitive)

startsWith

startsWithExact (case sensitive)

endsWith

endsWithExact (case sensitive)
```

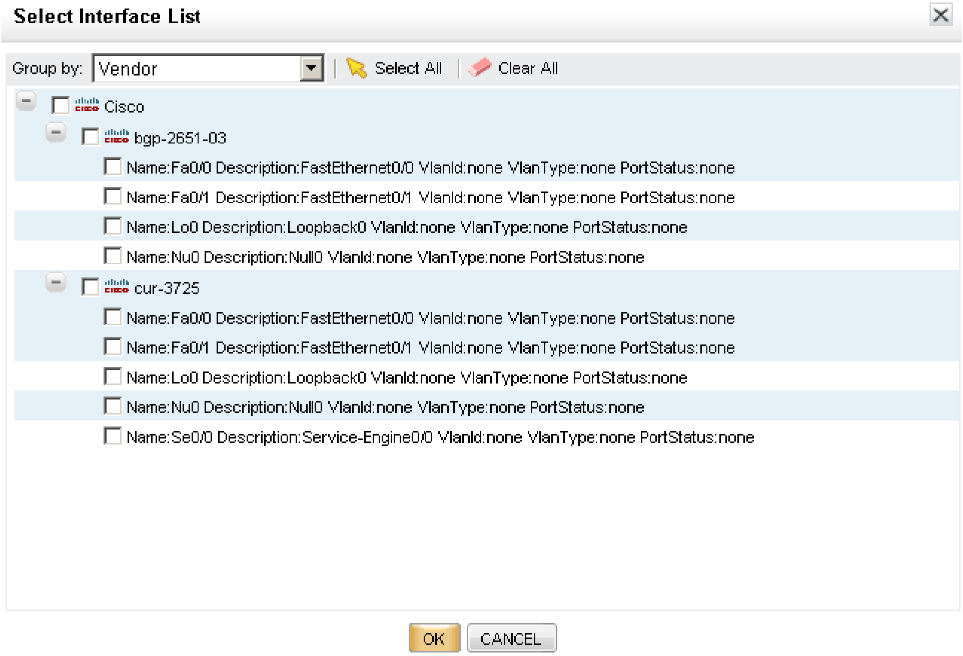
Note: use single quotes around all string values. For example: `if (@ITF.Name=='FastEthernet0/1')`

Example for `if/else` Condition: Select Interface(s) for VLAN Membership Changes

Let’s review the part of the the “Change VLAN membership on ports Cisco IOS” template script that presents interfaces for the template user to select in the template’s wizard. We saw that the script uses a `foreach ( )` loop to present the interface selection:

```
foreach (@portItem in @TargetPorts)

{

  CLI

  {

     interface @portItem.InterfaceDescription

  }
```

Recall that the @TargetPorts variable takes the array NCM.Interfaces[ ] (a SWIS entity) as its data type. And the result is that the template wizard in which the template user selects interfaces for the VLAN membership config change presents a comprehensive tree of NCM nodes and their interfaces.



Select Interface List

Group by: Vendor | Select All | Clear All

□ Cisco

□ bgp-2651-03

□ Name:Fa0/0 Description:FastEthernet0/0 VlanId:none VlanType:none PortStatus:none

□ Name:Fa0/1 Description:FastEthernet0/1 VlanId:none VlanType:none PortStatus:none

□ Name:Lo0 Description:Loopback0 VlanId:none VlanType:none PortStatus:none

□ Name:Nu0 Description:Null0 VlanId:none VlanType:none PortStatus:none

□ cur-3725

□ Name:Fa0/0 Description:FastEthernet0/0 VlanId:none VlanType:none PortStatus:none

□ Name:Fa0/1 Description:FastEthernet0/1 VlanId:none VlanType:none PortStatus:none

□ Name:Lo0 Description:Loopback0 VlanId:none VlanType:none PortStatus:none

□ Name:Nu0 Description:Null0 VlanId:none VlanType:none PortStatus:none

□ Name:Se0/0 Description:Service-Engine0/0 VlanId:none VlanType:none PortStatus:none

OK CANCEL

When the user finishes filling in values in the wizard, as part of executing the config changes, NCM will iterate through all selected interfaces, adjusting VLAN assignments as specified in another part of the script.

Now for purposes of this example, supose that you want to prevent the errors that might occur if the user accidentally selects an inappropriate interface (say the loopback address).

To do this we include conditional logic within the foreach ( ) loop related to interfaces.

```
foreach @portItem in @TargetPorts)

{

  if (@PortItem.InterfaceDescription contains 'Loop0')

  {

     // Do nothing if it’s the loopback

  }
```

```
else

  foreach (@portItem in @TargetPorts)

if (@PortItem.InterfaceDescription != ‘Loop0’)

  {

    CLI

    {

       interface @portItem.InterfaceDescription

    }
```

And yes this whole scripting passage can be written more simply as:

```
foreach @portItem in @TargetPorts)

if (@PortItem.InterfaceDescription != ‘Loop0’)

  {

    CLI

    {

       interface @portItem.InterfaceDescription

    }
```

The result of adding this conditional logic is that if in executing the “Change VLAN membership on ports Cisco IOS” template NCM encounters the loopback interface as an object for the config change then it does nothing and passes on to the next interface in the iteration. The purpose of this code would be to prevent damage due to a template user error.

Example for `if` Conditions: Tying a Command to Model Number

Let’s assume you want to run specific commands on a device only if the device has an exact model number. We can also assume that the input parameters of the script require the user to selected multiple nodes as targets for the configuration change action; and the user chose three nodes with the models Cisco 2628, Cisco 2621 XM, and Catalyst 3700 Stack.

Here is the section of a script that delimits the commands to run on different models of device.

```
script CiscoModels(NCM.Nodes[] @ContextNode)
```

```
...

{
 if (@ContextNode.MachineType Contains  'Cisco 2621 XM')
  {
  CLI
      {
      //do something
      }
  }

 if (@ContextNode.MachineType Contains  'Catalyst 37xx Stack')
  {
  CLI
      {
      //do something
      }
  }
}
...
```

In this case the `if` logic uses the .`MachineType` property of the SWIS entity NCM.Nodes[] and the "Contains" operator to instruct NCM to evaluate each selected node in terms of the machine type listed with inventory values in the database. For any device of machine type "Cisco 2621 XM," NCM will run a specific config change command on the device; for any device of machine type "Catalyst 37xx Stack," NCM will run an entirely different config command on the device.

Manipulating Strings and Integers

Five functions for manipulating strings, and two for converting strings and integers into each other, 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.

Substring

Allows you to specify a starting point within a string and the length from the starting point that you want to capture for manipulation.

Declaration:

```
string Substring (string str, int startIndex, int length)

where:

"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

Allows you to return the length of the string you specify.

Declaration:

```
In StrLength(string str)
```

where:

“str”is the user-input string whose length is used as the integer value.

Indexof

Allows you to find the number of characters associated with a string.

Declaration:

```
int IndexOf(string str, string search)
```

where:

“str”is a string upon which search will focus;

‘search’ is a user-input string NCM uses to find the numerical value of the string being searched.

.

Setoctet

Allows you to replace an octet within an IP address.

Declaration:

```
string SetOctet(string ipAddr, int octetPosition, string octet)
```

where:

“ipAddr”is the IP address;

“octetPostion” marks the position where the target octet begins;

“octet” is the new value of the target octet.

getoctet.

Allows you to retrieve an octet from a user-specified IP address and octet position.

Declaration:

```
string GetOctet(string ipAddress, int octetPosition)
```

where:

“ipAddress”is an user-input IP address;

“octetPosition” is the use-imput value for the place where the function finds the beginning of the octet to get.

ConvertStringToInt

Allows you to convert a string into an integer.

Declaration:

```
string ConvertStringToInt(string str)
```

where:

“str”is the string to convert;

ConvertIntToString

Allows you to convert and integer into a string.

Declaration:

```
string ConvertIntToString(int number)
```

where:

“number”is an integer to convert;

Example 1: Converting a String to an Integer

This example shows a simple conversion of a string to an integer value.

```
script ConvertStringToInt(string @str, int @number,
int @number2, int @result)
{
  string @str = '10'
  int @number = ConvertStringToInt(@str)
  int @number2 = 10
  int @result = @number + @number2

  CLI
  {
    @result
  }
}
```

Let’s assume user enters ’10’ for the `@str` variable, 10 for ‘@number2’ in the input fields of the template’s wizard.

Based on values the user inputs for `@str` and `@number2`, the script does these things: 1) uses ‘10’ in the `ConvertStringToInt` function to give a value of ‘10’ to a variable called `@number`; 2) adds the value of @number (in this case, ‘10’) to the value of @number2 (in this case, ‘10’) to set ‘20’ as the value for the variable called `@result`.

The script then issues a CLI command @result to any device targeted by the script, with the result being that ‘20’ is entered on the command line. The operations of this script would be most useful for transforming strings into integers within the context of a more complex script, in which you need string values in some functions (say, to represent an IP address) and the same characters treated as integers in other functions.

Example 2: Converting an Integer into a String

This example shows a simple conversion of a string to an integer value.

```
script ConvertIntToString (int @number)

{
Int @number = 100
string @str = ConvertIntoToString (@number)

  CLI
  {
       @str
  }
}
```

Let’s assume user enters ’100’ for the `@number` variable in the input field of the template’s wizard.

Based on values the user inputs for `@number`, the script uses ‘100’ in the `ConvertIntToString` function to give a value of ‘100’ to a variable called `@str`.

The script then issues a CLI command @str to any device targeted by the script, with the result being that the string ‘100’ is entered on the command line. The operations of this script would be most useful for transforming integers into strings within the context of a more complex script, in which you need integer values in some and the same characters treated as a string in other functions.

Example 3: Manipulating a String

This example shows simple manipulation of an IP address using the `Substring`, `indexof`, and `strlenth` functions.

```
script IPshuffle(string @str, string @search )
{
       int @length = strlength(@str)
      int @startIndex = indexof(@str,@search)
      int @substringLength = @length - @startIndex
       string @res = substring(@strA,@startIndex,
@substringLength)
       CLI
       {
       @res
       }
}

Output:
CDEF
```

Let's assume user enters 'ABCDEF' for the `@str` variable and 'CD' for the @search variable in the template's wizard.

Based on values the user inputs for `@str` and `@search`, the script does these things: 1) uses 'ABCDEF' in the `strlength` function to give a value of '6' to a vairable called `@length`; 2) uses 'CD' as the substring of 'ABCDEF' to set a value '2' for the variable called `@startIndex`; 3) subtracts 2 (@startIndex) from 6 (@length) to determine the value of `@substringLength` as 4; and finally takes the original string 'ABCDEF' and calculates a result `(@res)` using the value of @startIndex to count in 2 positions and the value of @substringlength to count four positions from the start index. This gives the result of 'CDEF' as the output of the string manipulation exercise.

Example 4: Changing an ACL

Let us assume, for example, that you want to create a block of ACL instructions that predictably vary the value of a specific octet within an IP address; conforming to the pattern 10.10.@id.10, where the value of **@id** will be determined by user input. We are assuming that in the config change template's runtime wizard the user enters 10.10.10.10 as the value of the `@ipaddress` variable; and 1, 22, 222 for the `@indexes` variable declared in the `script` command.

```
.PARAMETER_LABEL @ipadress

        IP address

.PARAMETER_DESCRIPTION @ipaddress

        Enter an IP address

.PARAMETER_LABEL @indexes

        Octets
```

```
.PARAMETER_DESCRIPTION @Indexes

        Enter a pattern of octet replacements. Separate numbers
with a comma.

*/

script ACLChanges(string @ipaddress, int[] @indexes)
       {
           string @ipnew
           foreach(@id in @indexes)
           {
               @ipnew = setoctet(@ipaddress,3,@id)
               CLI
               {
                   Allow @ipnew out
                   Allow @ipnew UDP 2055 OUT
               }
           }
       }
```

Note that 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 3rd octet with user-input vlaues.And for each new IP address the script produces command to create outgoing UDP transmission access through port 2055.

```
Allow 10.10.1.10 out
Allow 10.10.1.10 UDP 2055 OUT

Allow 10.10.22.10 out
Allow 10.10.22.10 UDP 2055 OUT

Allow 10.10.222.10 out
Allow 10.10.222.10 UDP 2055 OUT
```

Example 5: Managing an ACL 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 instruction for this device that varies based on a portion of the device's IP address.

If the store has 4 routers, 10.1.**1**.1, 10.1.**4**.1, 10.1.**6**.1, 10.1.**10**.1, the template script generates an ACL block that appears this way on the selected router (10.1.1.1):

```
Allow 10.1.2.0/24 out

Allow 10.1.2.4 UDP 2055 OUT

Allow 10.1.4.0/24 out
Allow 10.1.4.4 UDP 2055 OUT

Allow 10.1.6.0/24 out

Allow 10.1.6.4 UDP 2055 OUT

Allow 10.1.10.0/24 out

Allow 10.1.10.4 UDP 2055 OUT
```

Here is the script that produces the output:

```
       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 uses foreach( ) to loop through a user-input series of router IP addresses; uses the getoctet function to focus the 3rd octet of the current router IP address; uses the setoctet function to create a new IP address as a value for @ipnew; and then creates a CLI { } command that will execute allow operations for each of the selected routers.

The result is a set of `allow` command that will 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, through which the template user will select the router on which to make ACL changes, and input the target router IP address.

```
.PARAMETER_LABEL @ACLRouter

        Router for ACL Change

.PARAMETER_DESCRIPTION @ACLRouters

        Select a Router

.PARAMETER_LABEL @ipRouters

        Target Routers

.PARAMETER_DESCRIPTION @ipRouters
```

```
        Add Routers to Target with ACL Allowances
```

Additional Examples

These sections walk through the config chage template command output and the script logic for commonly used templates.

Enable NetFlow on Cisco ASAs

The Enable NetFlow on Cisco ASAs config change template automatically installs with the NCM software. It configures your Cisco ASA for NetFlow export.

Here are the commands that this template creates for NCM to execute on the command line of the targeted devices selects in the template’s runtime setup wizard. For the purposes of example, we are including values—as if a user selected or entered them in the wizard interface.

```
configure terminal

flow-export destination inside 10.10.18.157 2055

flow-export template timeout-rate 1

flow-export delay flow-create 60

logging flow-export syslogs disable

access-list netflow-export extended permit ip any

class-map netflow-export-class

match access-list netflow-export

policy-map netflow-policy

class netflow-export-class

flow-export event-type all destination 10.10.18.157

service-policy netflow-policy global

flow-export enable

exit

end
```

You could execute this set of CLI commands on your target device and the result would be config changes in the status of NetFlow data processing by the device.

The config change template that produces this output of CLI commands would be:

```
/*

.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 variable values.

.PARAMETER_LABEL @NetFlowCollectorIPAddress

    NetFlow Collector IP Address

.PARAMETER_DESCRIPTION @NetFlowCollectorIPAddress

    Enter the IP address of the server running the NetFlow traffic
analysis solution (e.g. SolarWinds NetFlow Traffic Analyzer)

.PARAMETER_LABEL @NetFlowExportPort

    NetFlow Export Port

.PARAMETER_DESCRIPTION @NetFlowExportPort

    Enter the NetFlow export port (default for SolarWinds NTA is
2055).

*/



script EnableNetflowOnCiscoASA (

    NCM.Nodes @ContextNode,

    string @NetFlowCollectorIPAddress,

    int @NetFlowExportPort )
```

```
{
    // Enter config terminal mode and generate NetFlow commands
    CLI
    {
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
        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
        end
    }
}
```

Parameters

The parameters defined at the beginning of this script create an interface in which the user types the IP address and port of the NetFlow receiver.

```
.PARAMETER_LABEL @NetFlowCollectorIPAddress
    NetFlow Collector IP Address
.PARAMETER_DESCRIPTION @NetFlowCollectorIPAddress
```

```
    Enter the IP address of the server running the NetFlow traffic
analysis solution (e.g. SolarWinds NetFlow Traffic Analyzer)

.PARAMETER_LABEL @NetFlowExportPort

    NetFlow Export Port

.PARAMETER_DESCRIPTION @NetFlowExportPort

    Enter the NetFlow export port (default for SolarWinds NTA is
2055).
```

The first line defines the parameter or variable name (in this case, @NetFlowCollectorIPAddress) for which the user enters a value in a wizard interface text box at runtime. 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. Together, by taking in specific user input, the parameter variables, labels, and descriptions guide the config change template's runtime execution.

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:

```
script EnableNetflowOnCiscoASA (

    NCM.Nodes @Node,

    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 will enter a string value for the NetFlow Collector IP Address and an integer value for the NetFlow Export Port on the device.

For a complete list of entities and properties, see SolarWinds Information Services Data Entities.

CLI{ } Commands

The majority of config change template code outputs original CLI commands with only a few parsed variables. Any time a variable is referenced, a value is used in its place. For example, in this case, since the user has typed 10.10.18.157 as the IP address, and 2055 as the collector port number, NetFlowCollectorIPAddress will be replaced with 10.10.18.157 and @NetFlowExportPort will be replaced with 2055 when the script runs.

```
flow-export destination inside @NetFlowCollectorIPAddress
@NetFlowExportPort
```

The previous line of code would generate the following output:

```
flow-export destination inside 10.10.18.157 2055
```

Executing a Config Change Template

Use the following steps to generate and execute a list of CLI commands that can appropriately change your network device configurations.

To execute a config change template:

1. Navigate to the Config Change Templates resource on the Orion Web Console (Configs > Config Change Templates).
2. Find the template in the alphanumerically sorted Config Change Template Name list.

   Alternately, if the list is long, click a relevant tag in the left pane and find the template in the filtered list.

   Templates are displayed by the tags applied to them at their time of creation or through editing.
3. Select the relevant template in the Config Change Template Name list.

   If you want to edit the template, click Advanced Modify and make your changes.

   As needed, consult “Understanding Config Change Template Details”.
4. Click Define Variables and Run.
5. Click all target devices in the Nodes list.

   Use the Group By controls to sort the list more efficiently.
6. Click Next.
7. Enter the appropriate values in the input fields.

Input fields for a change configuration template are defined and managed through the Edit Config Template resource. For example, in a template that turns on NetFlow data exporting for a set of Cisco devices, you might be asked to enter in one field the IP address of the a relevant NetFlow collector, and in another the port on which your target device exports flow data.

For more information, see Editing a Config Change Template.

8. Click Next.
9. [Optional] Click a relevant node in the tree and click Preview in a New Window to see the CLI commands for that device.

   If you choose to open a new window to view CLI commands, you will need to minimize or close it to return to the Execute <Template_Name> resource.
10. Copy the commands to a text file if desired.
11. Return to the Execute <Template_Name> resource and click Execute when you are ready to issue the CLI commands to all selected devices.

Creating a Config Change Template

Use the following steps to create a config change template that can guide network engineers in producing accurate sequences of CLI commands for enacting changes across multiple network devices.

To create a config change template:

1. Navigate to the Config Change Templates resource on the Orion web console (Configs > Config Change Templates).
2. Click Create New Config Change Template.
3. Enter an appropriate name for this template in Config Change Template Name.

   This is the name that appears in the Config Change Template Name list.
4. Provide a succinct sentence or phrase in Description that will help users quickly understand what your template helps them do.

   This description appears when a user selects a config change template in the resource list and clicks on its name.
5. Enter one or more Tags that will help users easily find your template by its tags.

   Templates can be displayed by the tags applied to them at their time of creation or through editing.

To be useful, your tagging scheme should be known to the user community and applied as consistently as possible.

6. Create your Config Change Template.

   As needed, consult “Creating a Config Change Template”.

7. Click Validate to check syntax in your new template.

8. Click Submit to save the template or Execute to save and run it.

   If you choose the execute the template, NCM validates the syntax of the template. If validation succeeds, NCM saves a copy of the template and loads the relevant interface for user input. If validation fails, NCM displays an error in red that serves as a guide make changes.

Importing a Config Change Template

Use the following steps to import a config change template into NCM from an accessible file system.

To import a config change template:

1. In the Config Change Template resource on the Orion web console, click Import.

2. Click Browse to find the file on your computer. Config change templates have the extension .ncm-template.

3. Click Submit.

4. Change the template name as needed.

   This is the name as it appears in the Config Change Template Name list.

5. Modify the description as needed to help users quickly understand what your template helps them do.

   This description appears when a user selects a config change template in the resource list and clicks on it.

6. Enter one or more Tags that will help users easily find your template by its tags.

   Templates can be displayed by the tags applied to them at their time of creation or through editing.

   To be useful, your tagging scheme should be known to the user community and applied as consistently as possible.

7. Modify the logic of your Config Change Template.

   As needed, consult “Config Change Template Basics”

8. Click Validate to check the new logic.

9. Click Submit.

Editing a Config Change Template

Use the following steps to modify how an existing config change template generates a list of CLI commands that can appropriately change your network device configurations.

To edit a config change template:

1. On the Config Change Templates resource in the Orion web console (Configs > Config Change Templates), find the template in the alphanumerically sorted Config Change Template Name list.

   Alternately, if the list is long, click a relevant tag in the left pane and find the template in the filtered list.

   Templates are displayed by the tags applied to them at their time of creation or through editing.

2. Select the relevant template in the Config Change Template Name list.

3. Click Advanced Modify.

   As needed, consult “Config Change Template Basics”

4. Change the template name as needed.

   This is the name as it appears in the Config Change Template Name list.

5. Modify the description as needed to help users quickly understand what your template helps them do.

   This description appears when a user selects a config change template in the resource list and clicks on it.

6. Enter one or more Tags that will help users easily find your template by its tags.

   Templates can be displayed by the tags applied to them at their time of creation or through editing.

   To be useful, your tagging scheme should be known to the user community and applied as consistently as possible.

7. Modify the logic of your Config Change Template.

   As needed, consult “Config Change Template Basics”

8. Click Validate to check the new logic.

9. Click Submit.

Tagging a Config Change Template

Use the following steps to manage tags for config change templates.

To add tags to a config change template:

1. On the Config Change Templates resource in the Orion web console (Configs > Config Change Templates), find and select the relevant template(s) in the alphanumerically sorted Config Change Template Name list.

   Alternately, if the list is long, click a relevant tag(s) in the left pane and find the template in the filtered list.

   Templates are displayed by the tags applied to them at their time of creation or through editing.

2. Click Tags.
3. In the Edit Tags for <Template_Name> resource, add tags.

   To add an existing tag, click a tag in the list.

   To add a new tag, click Add new tag(s) and type your tags in the highlighted text field, separating them from each other with commas.

   Templates can be displayed by the tags applied to them at their time of creation or through editing, as in this case. Either way, to be useful, your tagging scheme should be known to the user community and applied as consistently as possible.

4. Click Submit.

To delete tags from a config change template:

1. On the Config Change Templates resource in the Orion web console (Configs > Config Change Templates), find the template in the alphanumerically sorted Config Change Template Name list.

   Alternately, if the list is long, click a relevant tag in the left pane and find the template in the filtered list.

   Templates are displayed by the tags applied to them at their time of creation or through editing.

2. Click Tags.
3. In the Edit Tags for <Template_Name> resource, click a valid tag in the existing tag list and then click the Remove tag(s) option.
4. In the highlighted list select the tag(s) to remove.
5. Click Submit.

Exporting a Config Change Template (to thwack)

Use the following steps to share a config change template with your user community on thwack.com.

To export a config change template:

1. On the Config Change Templates resource in the Orion web console (Configs > Config Change Templates), find the template in the alphanumerically sorted Config Change Template Name list.

   Alternately, if the list is long, click a relevant tag in the left pane and find the template in the filtered list.

   Templates are displayed by the tags applied to them at their time of creation or through editing.
2. Select the template and click Export to thwack.
3. If prompted enter your user information and click Login.

Exporting a Config Change Template (as a file)

Use the following steps to save a config change template on a file system and to share it with your user community on thwack.com.

To export a config change template:

1. On the Config Change Templates resource in the Orion web console (Configs > Config Change Templates), find the template in the alphanumerically sorted Config Change Template Name list.

   Alternately, if the list is long, click a relevant tag in the left pane and find the template in the filtered list.

   Templates are displayed by the tags applied to them at their time of creation or through editing.
2. Select the template and click Export as File. Verify that a popup blocker is not preventing the file from being downloaded.
3. Download the file to a local directory.
4. Click Return to Config Change Templates if you are finished.
5. Click Share Now if you want to upload the template to thwack.com.
6. Click Upload a File in the content sharing area.
7. Click Specify File and browse to it on your local system.
8. Click Save.

9. Enter a name and description.
10. Select or enter tags.
11. Click Save.

Deleting a Config Change Template

Use the following steps to delete config change templates that are no longer needed.

To delete a config change template:

1. On the Config change templates resource in the Orion web console (Configs > Config Change Templates), find the template in the alphanumerically sorted Config Change Template Name list.

   Alternately, if the list is long, click a relevant tag in the left pane and find the template in the filtered list.

   Templates are displayed by the tags applied to them at their time of creation or through editing.
2. Select the template and click Delete.
3. Click Yes.

SolarWinds Information Services Data Entities

The following tables document all the SWIS entities and properties that you can use in developing config change templates.

NCM.ArpTables

Property Name	Datatype	Description
InterfaceIndex	System.Int32	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.
InterfaceID	System.String	A unique GUID ID from ncm.Interfaces table.
MAC	System.String	The media dependent `physical' address.
IPAddress	System.String	The IP address corresponding to the media dependent physical address.
IPSort	System.Double	A list of IP addresses sorted with octet markers (dots) omitted.
Source	System.String	The type of IP address associated with an ARP operation and media dependent address. Possible Values: Other (1) Invalid (2) Dynamic (3) Static (4) Setting this object to the value invalid (2) has the effect of invalidating the corresponding entry in the ipNetToMediaTable. That is, it effectively disassociates the interface identified with said entry from the mapping identified with said entry. It is an implementation specific matter as to whether the agent removes an Invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant ipNetToMediaType object.
RDNSLookup	System.String	Result of DNS lookup on IPAddress.
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 ARP 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.ARPTables Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsArpTables (System.Hosting)

NCM.BridgePorts

Property Name	Datatype	Description
InterfaceIndex	System.Int32	The value of the instance of the ifIndex object, defined in MIB-II, for the interface corresponding to this port.
Port	System.Int32	The port number of the port for which this entry contains bridge management information.
SpanningTreeEnabled	System.String	The enabled/disabled status of the port.

Property Name	Datatype	Description
		Possible Values: Enabled (1) Disabled (2)
SpanningTreeState	System.String	The port's current state as defined by application of the Spanning Tree Protocol. This state controls what action a port takes on reception of a frame. If the bridge has detected a port that is malfunctioning it will place that port into the broken(6) state. For ports which are disabled (see dot1dStpPortEnable), this object will have a value of disabled(1).

VlanType	System.String	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)

VLANID	System.Int32	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.

PortStatus	System.String	An indication of the current VLAN status of the port. A status of inactive(1) indicates that a dynamic port does not yet have a VLAN assigned, or a port is assigned to a VLAN that is currently not active. A status of active(2) indicates that the currently assigned VLAN is active. A status of shutdown(3) indicates that the port has been disabled as a result of VQP shutdown response.
		Possible Values:
		inactive(1)
		active(2)
		shutdown(3)

Property Name	Datatype	Description
NodeID	System.String	A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of interfaces for which bridge port data is reported.)
LastDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM last discovered the device during inventory.
FirstDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM first discovered the device during inventory.

NCM.BridgePorts Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsBridgePorts (System.Hosting)

NCM.CatalystCards

Property Name	Datatype	Description
CardIndex	System.Int32	A unique value for each module within the chassis.

CardType	System.Int32	The type of module. 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), lsa(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), atmadsl1(74), atmadsl2(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), atme3(94), atmt3(95), xdsl-fec(96), xdsl-adsl(97), xdsl-gshdsl(98), xdsl-bri(99), xdsl-scc(100), ge1(101), pos155m(102), cpos(103), fe1op(104), sae8(105), atm155m-mm(106), atm155m-sm(107), atm155m-sml(108), fe1op-sfx(109), fe1op-mfx(110), cpos-t1(111), ge1-op(112), ge2-op(113), ge2(114),fix-1wan(115), fix-1sae(116), cavium(117), sic-1Eth(118), atm1ADSLI(119), atm2ADSLI(120), fix-e11(121), fix-t11(122), e18-75(123), e18-120(124), t18(125), sic-1vifxs(126), sic-1vifxo(127), sic-2vifxs(128), sic-2vifxo(129), xdsl-fec-new(130), xdsl-sa(131), bs4(132), ima-8e175(133), ima-8e1120(134).ima-4e175(135),ima-4e1120(136), ima-8t1(137), ima-4t1(138), sic-1t1f(139), sic-1e1f(140). fe4(149), atm1shdsl4wire(151), atmIma4shdsl(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). wsx6302msm(206), wsf6kmsfc(207), wsx6024flmt(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), wsf6kmsfc2(234), wsx6324mmmt(235), wsx6348rj45(236), wsx6ksup22ge(237), wsx6324sm(238), wsx6516gbic(239), osm4geWanGbic(240), osm1oc48PosSS(241), osm1oc48PosSI(242), osm1oc48PosSL(243), wsx6381ids(244), wsc6500sfm(245), osm16oc3PosMM(246), osm16oc3PosSI(247),

Property Name	Datatype	Description
		osm16oc3PosSL(248), osm2oc12PosMM(249), osm2oc12PosSI(250), osm2oc12PosSL(251), wsx650210ge(252), osm8oc3PosMM(253), osm8oc3PosSI(254), osm8oc3PosSL(255), wsx6548rj45(258), wsx6524mmmt(259), wsx6066SlbApc(260), wsx6516getx(261), osm2oc48OneDptSS(265), osm2oc48OneDptSI(266), osm2oc48OneDptSL(267), osm2oc48OneDptSSDual(268), osm2oc48OneDptSIDual(269), osm2oc48OneDptSLDual(270), wsx6816gbic(271). osm4choc12T3MM(272), osm4choc12T3SI(273), osm8choc12T3MM(274), osm8choc12T3SI(275), osm1choc48T3SS(276), osm2choc48T3SS(277). wsx6500sfm2(278). osm1choc48T3SI(279), osm2choc48T3SI(280), wsx6348rj21(281), wsx6548rj21(282), wsSvcCmm(284), wsx650110gex4(285), osm4oc3PosSI(286). osm4oc3PosMM(289), wsSvcIdsm2(290), wsSvcNam2(291), wsSvcFwm1(292), wsSvcCe1(293). wsSvcSsl1(294). osm8choc3DS0SI(295), osm4choc3DS0SI(296), osm1choc12T1SI(297). wsx4012(300). wsx4148rj(301). wsx4232gbrj(302), wsx4306gb(303), wsx4418gb(304), wsx44162gbtx(305), wsx4912gb(306), wsx2948gbrj(307), wsx2948(309), wsx4912(310), wsx4424sxmt(311). wsx4232rjxx(312). wsx4148rj21(313), wsx4124fxmt(317), wsx4013(318). wsx4232l3(319), wsx4604gwy(320). wsx44122Gbtx(321). wsx2980(322), wsx2980rj(323), wsx2980gbrj(324). wsx4019(325). wsx4148rj45v(326), wsx4424gbrj45(330), wsx4148fxmt(331), wsx4448gblx(332), wsx4448gbrj45(334), wsx4148lxmt(337), wsx4548gbrj45(339). wsx4548gbrj45v(340). wsx4248rj21v(341), wsx4302gb(342), wsx4248rj45v(343), wsx2948ggetx(345), wsx2948ggetxgbrj(346), wsx6516aGbic(502), wsx6148getx(503), wsx6148x2rj45(506), wsx6196rj21(507), wssup32ge3b(509), wssup3210ge3b(510), mec6524gs8s(511), mec6524gt8s(512), me6524msfc2a(598), osm12ct3T1(600), osm12t3e3(601). osm24t3e3(602), osm4GeWanGbicPlus(603), osm1choc12T3SI(604). osm2choc12T3SI(605), osm2oc12AtmMMPlus(606), osm2oc12AtmSIPlus(607), osm2oc12PosMMPlus(608), osm2oc12PosSIPlus(609). osm16oc3PosSIPlus(610), osm1oc48PosSSPlus(611), osm1oc48PosSIPlus(612), osm1oc48PosSLPlus(613), osm4oc3PosSIPlus(614). osm8oc3PosSLPlus(615), osm8oc3PosSIPlus(616), osm4oc12PosSIPlus(617), wsSvcIpSec1(903), wsSvcCsg1(911), wsx6148rj45v(912), wsx6148rj21v(913), wsSvcNam1(914), wsx6548getx(915), wsx6066SlbSk9(920), wsx6148agetx(921), wsx6148arj45(923), wsSvcWlan1k9(924), wsSvcAon1k9(925), ace106500k9(926). wsSvcWebVpnk9(927). wsx6148FeSfp(928), wsSvcAdm1k9(929), wsSvcAgm1k9(930), ace046500k9(936), wssup720(1001), wssup720base(1002).

Property Name	Datatype	Description
		m7600Sip600(1004). wsx6748getx(1007). wsx670410ge(1008). wsx6748sfp(1009). wsx6724sfp(1010), wsx670810ge(1016). wsx65822pa(1101), m7600Sip200(1102). m7600Sip400(1103). c7600ssc400(1104). c7600ssc600(1105). esm2x10ge(1106), rsp720(1800). rsp720base(1801). c7600msfc4(1805)
CardName	System.String	A descriptive string used by the network administrator to name the module.
ModuleModel	System.String	The manufacturer's model number for the module.
CardSerial	System.String	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.
HWVersion	System.String	The hardware version of the module.
FWVersion	System.String	The firmware version of the module.
SWVersion	System.String	The software version of the module.
Slot	System.Int32	This value is determined by the chassis slot number where the module is located. Valid entries are 1 to the value of chassisNumSlots
Parent	System.Int32	The value of the instance of the entPhysicalIndex object, defined in ENTITY-MIB, for the entity physical index corresponding to this module

OperStatus	System.String	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)

SlotsOnCard	System.Int32	The number of ports supported by the module.
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.CatalystCards Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsCatalystCards (System.Hosting)

NCM.CiscoCards

Property Name	Datatype	Description
CardIndex	System.Int32	Index into cardTable (not physical chassis slot number).
CardType	System.Int32	Functional type of this card. (integer value)
CardName	System.String	Functional type of this card. (Parsed from type name value).

Property Name	Datatype	Description
CardDescr	System.String	Text description of this card.
CardSerial	System.String	The serial number of this card, or zero if unavailable.
HWVersion	System.String	Hardware revision level of this card, or an empty string if unavailable.
SWVersion	System.String	Version of the firmware or microcode installed on this card, or an empty string if unavailable.
Slot	System.Int32	Number of slots on this card, or 0 if no slots or not applicable, or -1 if not determinable.
Parent	System.Int32	cardIndex of the parent card which directly contains this card, or 0 if contained by the chassis, or -1 if not applicable nor determinable.
OperStatus	System.String	The operational status of the card. cardOperStatus is up when a card is recognized by the device and is enabled for operation. cardOperStatus is down if the card is not recognized by the device, or if it is not enabled for operation. cardOperStatus is standby if the card is enabled and acting as a standby slave. Possible Values: not-specified(1) up (2) down (3) standby (4) standbyMaster (5) activeMaster (6) outOfService (7) masterBooting(8) activeMasterBooting(9) standbyMasterBooting(10) slaveBooting(11)
SlotsOnCard	System.Int32	Number of slots on this card, or 0 if no slots or not applicable, or -1 if not determinable
NodeID	System.String	A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of interfaces for which card data is reported.)
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

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsCiscoCards (System.Hosting)

NCM.CiscoCdp

Property Name	Datatype	Description
ifIndex	System.Int32	An indication of the type of address contained in the corresponding instance of cdpCacheAddress (parse just ifIndex from value for example 1,2,3)

Property Name	Datatype	Description
CDPIndex	System.String	An indication of the type of address contained in the corresponding instance of cdpCacheAddress (full value. For example 1.6, 2.108, 2.3
RemoteDevice	System.String	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.
RemoteIPAddress	System.String	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.
RemoteVersion	System.String	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.
RemotePort	System.String	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
RemoteCapability	System.String	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.
RemotePlatform	System.String	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.

RemoteDuplex	System.String	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)

RemoteNativeVLAN	System.Int32	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
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 remote devices for which remote device data is reported.)
LastDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM last discovered the device during inventory.

Property Name	Datatype	Description
FirstDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM first discovered the device during inventory.

NCM.CiscoCdp Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsCiscoCdp (System.Hosting)

NCM.CiscoChassis

Property Name	Datatype	Description

chassisType	System.Int32	Chassis type (integer value).
		Possible Values:
		unknown(1)
		multibus(2)
		agsplus(3)

chassisName	System.String	Chassis type (parsed string value).
		Possible Values:
		unknown(1)
		multibus(2)
		agsplus(3)

chassisVersion	System.String	Chassis hardware revision level, or an empty string if unavailable.
chassisID	System.String	Unique ID string. Defaults to chassis serial number if available, otherwise empty. Can also be set with 'snmp-server chassis-id'.
chassisSerialNumberString	System.String	The serial number of the chassis. This MIB object will return the chassis serial number for any chassis that either a numeric or an alphanumeric serial number is being used.
romVersion	System.String	ROM monitor version.
romSysVersion	System.String	ROM system software version or an empty string if unavailable.
processorRAM	System.Int32	Bytes of RAM available to CPU.
nvRAMSize	System.Int32	Bytes of nonvolatile configuration memory.
nvRAMUsed	System.Int32	Bytes of non-volatile configuration memory in use.
chassisSlots	System.Int32	Number of slots in this chassis, or -1 of neither applicable nor determinable.
romID	System.String	This variable contains a printable octet string which contains the System Bootstrap description and version identification.
whyReload	System.String	This variable contains a printable octet string which contains the reason why the system was last restarted.
freeMem	System.Int32	Return the amount of free memory in bytes. Note: This MIB object is obsolete as of IOS release 11.1. IOS release 11.1 introduced the CISCO-MEMORY-POOL-MIB which better instruments all of the memory pools.
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 nodes for which data is reported.)
LastDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM last discovered the device during inventory.
FirstDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM first discovered the device during inventory.

NCM.CiscoChassis Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsCiscoChassis (System.Hosting)

NCM.CiscoFlash

Property Name	Datatype	Description
FlashSize	System.Int32	Total size of the Flash device. For a removable device, the size will be zero if the device has been removed.
Name	System.String	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.
FlashDescription	System.String	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.
PartitionCount	System.Int32	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).

Property Name	Datatype	Description
MinPartitionSize	System.Int32	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)
Controller	System.String	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.

Property Name	Datatype	Description

WriteProtectJumper	System.String	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)

MaxPartitions	System.Int32	Max number of partitions supported by the system for this Flash device. Default will be 1, which actually means that partitioning is not supported. Note that this value will be defined by system limitations, not by the flash device itself (for eg., the system may impose a limit of 2 partitions even though the device may be large enough to be partitioned into 4 based on the smallest partition unit supported). On systems that execute code out of Flash, partitioning is a way of creating multiple file systems in the Flash device so that writing into or erasing of one file system can be done while executing code residing in another file system. For systems executing code out of DRAM, partitioning gives a way of sub-dividing a large Flash device for easier management of files.

Property Name	Datatype	Description
Initialized	System.DateTime	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.
Removable	System.String	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.
NodeID	System.String	A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)
LastDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM last discovered the device during inventory.
FirstDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM first discovered the device during inventory.

NCM.CiscoFlash Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsCiscoFlash (System.Hosting)

NCM.CiscoFlashFiles

Property Name	Datatype	Description
FlashFileName	System.String	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.
FlashFileSize	System.Int32	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.
FlashCheckSum	System.String	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.

Property Name	Datatype	Description
		The checksum will be available for all valid and invalid-checksum files.

FlashFileStatus	System.String	Status of a file. A file could be explicitly deleted if the file system supports such a user command facility. Alternately, an existing good file would be automatically deleted if another good file with the same name were copied in. Note that deleted files continue to occupy prime Flash real estate.
		A file is marked as having an invalid checksum if any checksum mismatch was detected while writing or reading the file. Incomplete files (files truncated either because of lack of free space or a network download failure) are also written with a bad checksum and marked as invalid.
		Possible Values:
		deleted(1)
		invalidChecksum(2)
		valid(3)

NodeID	System.String	A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)
LastDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM last discovered the device during inventory.
FirstDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM first discovered the device during inventory.

NCM.CiscoFlashFiles Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsCiscoFlashFiles (System.Hosting)

NCM.CiscoImageMIB

Property Name	Datatype	Description
Name	System.String	The string of this entry.
Value	System.String	The string of this entry.
NodeID	System.String	A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)
LastDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM last discovered the device during inventory.
FirstDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM first discovered the device during inventory.

NCM.CiscoImageMIB Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsCiscoImageMIB (System.Hosting)

NCM.CiscoMemoryPools

Property Name	Datatype	Description
PoolName	System.String	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.
PoolUsed	System.Int32	Indicates the number of bytes from the memory pool that are currently in use by applications on the managed device.
PoolFree	System.Int32	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
PoolLargestFree	System.Int32	Indicates the largest number of contiguous bytes from the memory pool that are currently unused on the managed device.
NodeID	System.String	A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)
LastDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM last discovered the device during inventory.
FirstDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM first discovered the device during inventory.

NCM.CiscoMemoryPools Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsCiscoMemoryPools (System.Hosting)

NCM.EntityLogical

Property Name	Datatype	Description
Name	System.String	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.
TDomain	System.String	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]).

Type	System.String	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 > mib-2 a logical entity of a 802.1d bridge -> dot1dBridge a logical entity of a 802.3 repeater -> snmpDot3RptrMgmt If an appropriate node in the SMI's naming hierarchy cannot be identified , the value 'mib-2' should be used.
Community	System.String	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.
TAddress	System.String	The transport service address by which the logical entity receives network management traffic, formatted according to the corresponding value of entLogicalTDomain. For snmpUDPDomain, a TAddress is 6 octets long, the initial 4 octets containing the IP-address in network-byte order and the last 2 containing the UDP port in network-byte order. Consult 'Transport Mappings for Version 2 of the Simple Network Management Protocol' (RFC 1906 [RFC1906]) for further information on snmpUDPDomain.
NodeID	System.String	A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)
LastDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM last discovered the device during inventory.
FirstDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM first discovered the device during inventory.

NCM.EntityLogical Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsEntityLogical (System.Hosting)

NCM.EntityPhysical

Property Name	Datatype	Description
EntityName	System.String	The textual name of the physical entity. The value of this object should be the name of the component as assigned by the local device and should be suitable for use in commands entered at the device's `console'. This might be a text name, such as `console' or a simple component number (e.g. port or module number) , such as `1' , depending on the physical component naming syntax of the device. If there is no local name, or this object is otherwise not applicable, then this object contains a zero-length string. Note: The value of entPhysicalName for two physical entities will be the same in the event that the console interface does not distinguish between them, e.g., slot-1 and the card in slot-1.
EntityDescription	System.String	A textual description of physical entity. This object should contain a string which identifies the manufacturer's name for the physical entity, and should be set to a distinct value for each version or model of the physical entity.
EntityType	System.String	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. 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. 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.
ContainedIn	System.String	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. 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.
EntityClass	System.String	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.

Property Name	Datatype	Description
Position	System.Int32	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.
HardwareRevision	System.String	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). 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.
FirmwareRevision	System.String	The vendor-specific firmware revision string for the physical entity. 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.
SoftwareRevision	System.String	The vendor-specific software revision string for the physical entity. 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.
Serial	System.String	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).
Manufacturer	System.String	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).
Model	System.String	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.

Property Name	Datatype	Description
Alias	System.String	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.
AssetID	System.String	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.
FieldReplaceable	System.String	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.
NodeID	System.String	A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)
LastDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM last discovered the device during inventory.
FirstDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM first discovered the device during inventory.

NCM.EntityPhysical Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsEntityPhysical (System.Hosting)

NCM. Interfaces

Property Name	Datatype	Description
InterfaceID	System.String	[Swis]
InterfaceIndex	System.Int32	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.
InterfaceDescription	System.String	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.
VLANID	System.Int32	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

Property Name	Datatype	Description
		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).

PortStatus	System.String	An indication of the current VLAN status of the port. A status of inactive(1) indicates that a dynamic port does not yet have a VLAN assigned, or a port is assigned to a VLAN that is currently not active. A status of active(2) indicates that the currently assigned VLAN is active. A status of shutdown(3) indicates that the port has been disabled as a result of VQP shutdown response.
		
		Possible Values:
		inactive(1)
		active(2)
		shutdown(3)

VLANType	System.Int32	The type of this VLAN
InterfaceName	System.String	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 `console'. This might be a text name, such as `le0' or a simple port number, such as `1' , 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.
InterfaceAlias	System.String	This object is an 'alias' name for the interface as specified by a network manager, and provides a non-volatile 'handle' for the interface.
InterfaceType	System.Int32	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.
InterfaceTypeName	System.String	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.
InterfaceTypeDescription	System.String	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.
InterfaceSpeed	System.Single	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.

Property Name	Datatype	Description
MACAddress	System.String	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.
AdminStatus	System.String	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).
OperStatus	System.String	The current operational state of the interface. The testing (3) state indicates that no operational packets can be passed. If ifAdminStatus is down (2) then ifOperStatus should be down (2). If ifAdminStatus is changed to up (1) then ifOperStatus should change to up (1) if the interface is ready to transmit and receive network traffic; it should change to dormant(5) if the interface is waiting for external actions (such as a serial line waiting for an incoming connection) ; it should remain in the down (2) state if and only if there is a fault that prevents it from going to the up (1) state.
InterfaceMTU	System.Int32	The size of the largest packet which can be sent/received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.
LastChange	System.DateTime	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.
PhysicalInterface	System.Char	This object has the value 'true(1)' if the interface sublayer has a physical connector and the value 'false(2)' otherwise.
Promiscuous	System.Char	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.

Property Name	Datatype	Description
		The value of ifPromiscuousMode does not affect the reception of broadcast and multicast packets/frames by the interface.
NodeID	System.String	A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)
LastDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM last discovered the device during inventory.
FirstDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM first discovered the device during inventory.

NCM.Interfaces Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsInterfaces (System.Hosting)
IpAddresses	NCM.IpAddresses	NCM.InterfaceHostsIpAddresses (System.Hosting)

NCM.IpAddresses

Property Name	Datatype	Description
InterfaceIndex	System.Int32	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.
IPAddress	System.String	The IP address to which this entry's addressing information pertains.
IPAddrIPSort	System.Double	Store IP address in double representation
SubnetMask	System.String	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.
InterfaceID	System.String	InterfaceId from interfaces table
NodeID	System.String	A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)
LastDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM last discovered the device during inventory.
FirstDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM first discovered the device during inventory.

NCM.IpAddresses Entity Relationships

Type	Entity	Joined Data Entity
Interfaces	NCM.Interfaces	NCM.InterfaceHostsIpAddresses (System.Hosting)

NCM.MacForwarding

Property Name	Datatype	Description
Port	System.Int32	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).
MAC	System.String	A unicast MAC address for which the bridge has forwarding and/or filtering information.
Source	System.String	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.
NodeID	System.String	A SWIS-generated unique identifier of a network node in the current inventory. (Instances of this property recur in this table according to the number of Cisco devices for which data is reported.)
LastDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM last discovered the device during inventory.
FirstDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM first discovered the device during inventory.

NCM.MacForwarding Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsMacForwarding (System.Hosting)

NCM.Nodes

Property Name	Datatype	Description
AgentIP	System.String	Ip address of device entered by customer manually

Property Name	Datatype	Description

Status	System.Byte	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)

Community	System.String	SNMP community string entered by user
ReverseDNS	System.String	DNS name of device
SysName	System.String	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.
SysDescr	System.String	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.
SysContact	System.String	The textual identification of the contact person for this managed node , together with information on how to contact this person
SysLocation	System.String	The physical location of this node (e.g., `telephone closet, 3rd floor').
SystemOID	System.String	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 `what kind of box' is being managed. For example, if vendor `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'.
Vendor	System.String	Vendor of device- determined based on SystemOID.
VendorIcon	System.String	Vendor icon of device- determined based on SystemOID.
MachineType	System.String	Machine Type - determined based on SystemOID.
LastBoot	System.DateTime	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.
OSImage	System.String	Determined based on SysDescr
OSVersion	System.String	Determined based on SysDescr
SNMPLevel	System.Byte	SNMP version selected by user (1,2 or 3)
SNMPContext	System.String	SNMPv3 credentials entered by user
SNMPUsername	System.String	SNMPv3 credentials entered by user
SNMPAuthType	System.String	SNMPv3 credentials entered by user
SNMPAuthPass	System.String	SNMPv3 credentials entered by user
SNMPEncryptType	System.String	SNMPv3 credentials entered by user
SNMPEncryptPass	System.String	SNMPv3 credentials entered by user

Property Name	Datatype	Description
SNMPStatus	System.String	status of SNMP connection to device (OK,No SNMP support, SNMP error description if any)
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 devices for which data is reported.)
LastDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM last discovered the device during inventory.
FirstDiscovery	System.DateTime	A SWIS-generated date and time marker for when NCM first discovered the device during inventory.

NCM.Nodes Entity Relationships

Type	Entity	Joined Data Entity
Interfaces	NCM.Interfaces	NCM.NodeHostsInterfaces (System.Hosting)
MacForwarding	NCM.MacForwarding	NCM.NodeHostsMacForwarding (System.Hosting)
VLANs	NCM.VLANs	NCM.NodeHostsVLANs (System.Hosting)
BridgePorts	NCM.BridgePorts	NCM.NodeHostsBridgePorts (System.Hosting)
ArpTables	NCM.ArpTables	NCM.NodeHostsArpTables (System.Hosting)
CiscoCards	NCM.CiscoCards	NCM.NodeHostsCiscoCards (System.Hosting)
CiscoCdp	NCM.CiscoCdp	NCM.NodeHostsCiscoCdp (System.Hosting)
CiscoChassis	NCM.CiscoChassis	NCM.NodeHostsCiscoChassis (System.Hosting)
CiscoFlash	NCM.CiscoFlash	NCM.NodeHostsCiscoFlash (System.Hosting)
CiscoFlashFiles	NCM.CiscoFlashFiles	NCM.NodeHostsCiscoFlashFiles (System.Hosting)
CiscoImageMIB	NCM.CiscoImageMIB	NCM.NodeHostsCiscoImageMIB (System.Hosting)
CiscoMemoryPools	NCM.CiscoMemoryPools	NCM.NodeHostsCiscoMemoryPools (System.Hosting)
EntityLogical	NCM.EntityLogical	NCM.NodeHostsEntityLogical (System.Hosting)
EntityPhysical	NCM.EntityPhysical	NCM.NodeHostsEntityPhysical (System.Hosting)
PortsTcp	NCM.PortsTcp	NCM.NodeHostsPortsTcp (System.Hosting)
PortsUdp	NCM.PortsUdp	NCM.NodeHostsPortsUdp (System.Hosting)
RouteTable	NCM.RouteTable	NCM.NodeHostsRouteTable (System.Hosting)

NCM.PortsTcp

Property Name	Datatype	Description
NodeID	System.String	The unique identifier of a network node subject to configuration actions.

LastDiscovery	System.DateTime	Date and time NCM last discovered the device during inventory.
FirstDiscovery	System.DateTime	Date and time NCM first discovered the device during inventory.
TCPLocalAddress	System.String	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.
TCPLocalPort	System.Int32	The local port number for this TCP connection.
TCPLocalPortName	System.String	Port description based on TCPLocalPort value
TCPRemoteAddress	System.String	The remote IP address for this TCP connection.
TCPRemotePort	System.Int32	The remote port number for this TCP connection.
TCPState	System.String	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. 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).
TCPRemotePortName	System.String	Port description based on TCPRemotePort value

NCM.PortsTcp Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsPortsTcp (System.Hosting)

NCM.PortsUdp

Property Name	Datatype	Description
NodeID	System.String	The unique identifier of a network node subject to configuration actions.
LastDiscovery	System.DateTime	Date and time NCM last discovered the device during inventory.
FirstDiscovery	System.DateTime	Date and time NCM first discovered the device during inventory.
UDPAddress	System.String	The local IP address for this UDP listener. In the case of a UDP listener which is

Property Name	Datatype	Description
		willing to accept datagrams for any IP interface associated with the node, the value 0.0.0.0 is used.
UDPPort	System.Int32	The local port number for this UDP listener.
UDPPortName	System.String	Port description based on UDPPort value (like 161- SNMP)

NCM.PortsUdp Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsPortsUdp (System.Hosting)

NCM.RouteTable

Property Name	Datatype	Description
NodeID	System.String	The unique identifier of a network node subject to configuration actions.
LastDiscovery	System.DateTime	Date and time NCM last discovered the device during inventory.
FirstDiscovery	System.DateTime	Date and time NCM first discovered the device during inventory.
InterfaceIndex	System.Int32	The index value which uniquely identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.
InterfaceID	System.String	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.

Property Name	Datatype	Description

Destination	System.String	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)

Mask	System.String	The routing mechanism via which this route was learned. Inclusion of values for gateway routing protocols is not intended to imply that hosts should support those protocols.
		Possible Values:
		other(1)
		local(2)
		netmgmt(3)
		icmp(4)
		egp(5)
		ggp(6)
		hello(7)
		rip(8)
		is-is(9)
		es-is(10)
		ciscoIgrp(11)
		bbnSpfIgp(12)
		ospf(13)
		bgp(14)

NextHop	System.String	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.
RouteType	System.String	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

Property Name	Datatype	Description
		media, the value of this field is the agent's IP address on that interface.)
RouteProtocol	System.String	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.
RouteAge	System.Int32	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.
NextHopAS	System.Int32	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.
Metric1	System.Int32	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.
Metric2	System.Int32	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.
Metric3	System.Int32	The index value which uniquely identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.

Property Name	Datatype	Description
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.

Metric5	System.Int32	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)

NCM.RouteTable Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsRouteTable (System.Hosting)

NCM.VLANs

Property Name	Datatype	Description
NodeID	System.String	The unique identifier of a network node subject to configuration actions.
LastDiscovery	System.DateTime	Date and time NCM last discovered the device during inventory.
FirstDiscovery	System.DateTime	Date and time NCM first discovered the device during inventory.
VLANID	System.Int32	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).
VLANName	System.String	The name of this VLAN. This name is used as the ELAN-name for an ATM LAN-Emulation segment of this VLAN.
VLANMTU	System.Int32	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.
VLANType	System.Int32	The type of this VLAN

VLANState	System.Int32	The state of this VLAN.
		Possible Values:
		operational(1)
		suspended(2)
		mtuTooBigForDevice(3)
		mtuTooBigForTrunk(4)

NCM.VLANs Entity Relationships

Type	Entity	Joined Data Entity
Node	NCM.Nodes	NCM.NodeHostsVLANs (System.Hosting)

Chapter 9

Managing Inventory

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

Running a Complete Inventory Scan

To perform an inventory of all nodes managed by SolarWinds Network Configuration Manager, click **Inventory > Start Full Inventory** in the NCM application. Alternatively, you can use the steps in "Scheduling an Inventory Scan" and choose to update all NCM managed nodes in Step 7.

Note: 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 which statistics are collected, see "Adjusting Inventory Settings".

Running Inventory Scans

Complete the following procedure to run an individual inventory scan on a single node.

To do an individual inventory scan:

1. Open the SolarWinds NCM application.
2. Select the NCM managed node(s) in the Node List.
3. Right click and select Inventory Selected Nodes.

Scheduling an Inventory Scan

A full inventory scan can be set to run on a schedule. Scheduled inventory scans are referred to as inventory jobs.

1. If you want to create a new job, click Create New Job, select the Update Inventory as the job type, give the job a title (and add comments as needed), and then click Next.
2. If you want to edit the existing Update Inventory job, click Edit.
3. Select the schedule type.

Basic gives you Once, Daily, Weekly, and Monthly schedule settings (start, end, recurrence). .

Advanced gives you more granular control over the schedule, supporting more complex patterns defined with cron expressions.

4. If you are creating a Basic schedule, select the frequency of the job.

   Once: enter a day and time (at least 15 minutes from current NCM server time).

   Daily: Select Every Day or Every Week Day, enter a Start time, and then select start and end dates

   Weekly: Select the days, enter a Start time, and then select start and end dates.

   Monthly: Select the months, days of the month, enter a Start time, and then select start and end dates

5. If you are creating an Advanced schedule, use the five fields to create the appropriate cron expression.

   For example, if you want the job to run once a week over every month at midnight on Sunday morning, the values for the fields would be 0 0 * * 0.

   This transliterates as telling NCM to run the job at 0 minutes and 0 hours, on all valid days of month, in all valid months, on Sunday”.

6. Add a comment as needed and then click Next.

7. Select the NCM nodes to target with this job.

   Select Nodes: Click Select Nodes and select the NCM nodes you want the job to target.

   All Nodes: Selects all NCM nodes as targets for the the job.

   Dynamic Selection: Define the criteria that NCM will use to determine the selection of NCM nodes as targets for the job.

   Nodes defined in legacy job scheduling system: Select the option and then click Yes, change selection.

   Note: Use this option to target the node group of all wireless access points in the database.

8. Select an email notification option.

a. If you select Email Results, then enter the email from/to information.

b. Enter the email server address and port number.

c. If the email server expects credentials, then select Password.

d. Enter the username and password.

9. Click Next.

   The Add Job Specific Details page displays.

10. Select the information types you want to include in your Inventory job. (By default, all inventory information is included.)
11. Click Next.
12. Review the settings for the job.
13. When you are done reviewing the settings, click Finish.

Adjusting Inventory Settings

Complete the following procedure to change your inventory settings.

To change the statistics to collect during an inventory scan:

1. Open inventory settings the Orion Web Console (Settings > NCM Settings > Node Inventory).
2. Select the statistics (under Standard, Route Tables, Windows, Cisco) you want to collect, and then click Submit.(By default, all inventory information except ‘IP Route Table’ is included.)
3. Click Inventory Engine Settings in the left pane.
4. Adjust the slider to set the number of NCM devices (the default is 5) you want SolarWinds Network Configuration Manager to scan concurrently.

   Note: Increasing the number of devices NCM can scan concurrently increases the amount of system resources need during a scan.

5. If you have VLANs extended across network trunks, and you want to inventory the relevant devices, you can select Extend VLANs inventory.

   However, this is not recommend due to the slow performance of the inventory process under in this situation.

6. If the inventory process causes the NCM server to hang or if the process takes too long, You can select Disable inventory lookup.

   You would then need to analyze the cause of the problem (for example, server capacity) before re-selecting this option.

7. Click Submit.

Viewing Inventory Status

Complete the following procedure to view current inventory statistics.

To view your inventory statistics:

1. Open the Orion Web Console.
2. Click CONFIGS > Reports.
3. Click Inventory Status.
4. Find and click a node Under Node Name to see inventory details.
5. Click Back to return to Inventory Status.

Chapter 10

Managing Inventory Reports

SolarWinds Network Configuration Manager includes several standard reports. These reports display configuration information for each node and statistics collected by the inventory engine.

Auditing NCM Events

A few inventory reports provide information on events involving NCM’s interaction with managed devices.

The User Activity Tracking Report provides information on these NCM-related events:

- Real-Time Config Change Detection
- Download Config (Job, User)
- Edit Config
- Delete Config
- Upload Config (Job, User)
- Upload Scripts (Job, User)

Among the security reports are the Login Failure and Login Status. And the polling reports include report on Down Nodes and Device that don not respond to SNMP.

Viewing Reports

Complete the following task to view a report.

To view a report:

1. Open the Orion Web Console and navigate to the NCM Reports view (CONFIGS > Reports)

   Note: If you do not have the relevant role privileges you may not be able to see some nodes or settings.

2. Use Group by and the Search window as needed to organize and find reports.
3. Select the report you want to view, and then click View Report.
4. The available reports include the following:

- Node Details

  All Nodes

  Current IOS Image and Version

  Last Boot Time for each Device

  Last Inventory of each Device

  Backup Status of Running Config

  Backup Status of Startup Config

  System Information of each Device

- Cisco Inventory

  Cisco Card Data

  Cisco Discovery Protocol

  Cisco 3750 Stack – Physical Entity

  Old Cisco Cards

  Cisco Catalyst Cards

  Cisco Chassis IDs

  Cisco Flash File System

  Cisco Flash Memory

  Cisco IOS Image Details

  Memory in Cisco Devices

  Cisco Memory Pools

  Cisco VLANs

  ROM bootstrap for Cisco devices

- Juniper Inventory

  Juniper Physical Entities

- Inventory

  ARP Tables

  IP Addresses on each Interface

  Last status change for each Interface

  Juniper Physical Entities

  Interfaces

  Logical Entities

Physical Entities

Physical Entities (Serial Number) v2

Switch Ports

TCP Services

UDP Services

- Audit

  User Activity Tracking Report

  Syslog Tracking Report

- Security

  Community Strings for each Node

  Login Failure Report

  Login information for each Device

  Login Status

- Polling Status

  Down Nodes

  Devices that do not respond to SNMP

- Route Tables Inventory

  Route Tables

- Windows Servers Inventory

  Windows Accounts

  Installed Services

  Installed Software

Creating and Scheduling Reports

You can create a report that is not included with SolarWinds Network Configuration Manager. SolarWinds NCM allows you to schedule reports as well as send/receive them based on that schedule.

Complete the following procedure to create and schedule a new report.

To create and schedule a report:

1. Open the Orion Web Console and navigate to NCM
2. Click Create New Job, select the Run Report job type, give the job a title.

3. Select the schedule type.

   Basic gives you Once, Daily, Weekly, and Monthly schedule settings (start, end, recurrence). .

   Advanced gives you more granular control over the schedule, supporting more complex patterns defined with cron expressions.

4. If you are creating a Basic schedule, select the frequency of the job.

   Once: enter a day and time (at least 15 minutes from current NCM server time).

   Daily: Select Every Day or Every Week Day, enter a Start time, and then select start and end dates

   Weekly: Select the days, enter a Start time, and then select start and end dates.

   Monthly: Select the months, days of the month, enter a Start time, and then select start and end dates

5. If you are creating an Advanced schedule, use the five fields to create the appropriate cron expression.

   For example, if you want the job to run once a week over every month at midnight on Sunday morning, the values for the fields would be 0 0 * * 0.

   This transliterates as telling NCM to run the job at 0 minutes and 0 hours, on all valid days of month, in all valid months, on Sunday".

6. Add a comment as needed and then click Next.

7. Select an email notification option.

   a. If you select Email Results, then enter the email from/to information.

   b. Enter the email server address and port number.

   c. If the email server expects credentials, then select Password.

   d. Enter the username and password.

8. Click Next.

9. Select a report on the Job Details resource.

10. Set a limitation for the number of records that can be exported, as needed.

11. Click Next.

12. Review the settings for the job.

13. When you are done reviewing the settings, click Finish.

Exporting Reports to PDF and Printing

Complete the following procedure to export a report.

To export report results:

1. Open the Orion Web Console and navigate to NCM reports (CONFIGS > Reports).

   Use Group by and the Search window as needed to organize and find reports.

2. Select a report and then click View Report.

   Click Export to PDF and then click Save.

3. Define the directory target and then click Save.
4. Open the exported PDF on your computer in Adobe Acrobat and click the Print button.

Printing Reports

Complete the following procedure to print a report.

To print report results:

1. Launch the SolarWinds NCM client application on your SolarWinds NCM server.
2. Click Reports > View Report.
3. Select the report you want to print, and then click OK.
4. Click File > Print.
5. If you want to select specific columns to print, click File > Print Preview.
   a. Select or clear the appropriate fields, and then click OK.
   b. Review the Print Preview, and then click Print.

Deleting Reports

Complete the following procedure to delete a report.

To delete an existing report:

1. Open the SolarWinds Network Configuration Manager application.

   Note: If you do not have administrator privileges you may not be able to see some nodes or settings.

2. Click Reports > View Report.

3. Click the report you want to delete, and then click Delete Selected Report.

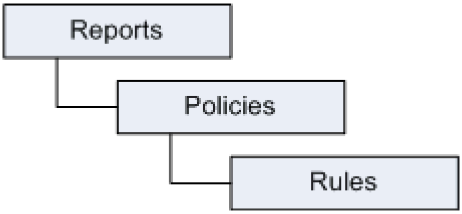
Chapter 11

Managing Policy Reports

Policy reports help ensure device configurations conform to both internal business practices and federal regulations, such as Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability (HIPAA), and Computer Inventory of Survey Plans (CISP). Policy reports scan configuration files and report any discovered rule violations. For example, a rule requires configurations do not include the read-only community string `public`. You can run a report on your configuration files, and then display any configurations that violate the rule. Your policy report lists violations, including the line number where the violation occurred if applicable. Several example reports, policies, and rules are included with SolarWinds Network Configuration Manager.

Creating a Policy Report

A policy report is a report that includes a collection of policies. A policy is a collection of rules. A report can contain several policies which, in turn, can contain several rules.



To create a policy report:

1. Login on the Orion Web Console with an administrator account.
2. Click Configs on the modules menu and select the Compliance view.
3. Click Manage Policy Reports and then Add New Report.
4. Type a name for your new report in Policy report name.
5. Type a description in Description.
6. If you want to assign this report to a folder, type a name in New folder name or select an existing folder from the Save in folder list.
7. If you want to display a summary with the report, .select Include report summary.
8. If you want to also display rules without violations, select Show rules without violation.

9. If you do not see your policy in the All Policies window (existing folders and subfolders), click Create a Policy.
10. Click relevant policies from folders in All Policies and click Add.

    The policies are placed in the Assigned Policies window.
11. Click Submit.

Creating a Policy

A policy is a collection of rules against which device configurations are reviewed for compliance. Policies are used in producing reports on device compliance.

To create a policy:

1. Login on the Orion Web Console with an administrator account.
2. Select Configs on the modules menu and select the Compliance view.
3. Click Manage Policy Reports.
4. Click Add New Policy on the Manage Policies tab.
5. Type a name for your new policy in Policy name.
6. Type a description in Description.
7. Select from the list the type of configuration you want to search with this policy.
8. If you do not see your rule in the All Policy Rules window (existing folders and subfolders), click Create a Rule.
9. Click relevant rules from folders in All Policy Rules and click Add.

   The rules are placed in the Assigned Policy Rules window.
10. Click Submit.
11. See these steps to include this policy in a report.

Creating a Policy Rule

A rule verifies policy compliance of a device by specifying a string that either must or must not be present in a configuration file. Rules are collected into policies and applied to specific network devices. Reports of policy violations are generated based on a schedule.

To create a rule:

1. Login on the Orion Web Console website with an administrator account.
2. Click Configs on the modules menu and select the Compliance view.

3. Click Manage Policy Reports .
4. Click Add New Rule on the Manage Rules tab.
5. Type a name for your new rule in Rule name.
6. Type a description in Description.
7. Click the alert level to associate with this rule.
8. If you want to assign this rule to a folder, type a name in New folder name or select an existing folder from the Save in folder list.
9. Click the type of alert trigger to associate with this alert.
10. If you want to search the device config for a simple string, click the appropriate String Type and enter the text in the box. Otherwise, go to step 10.
11. If you want to search the device config for a text block, or by a regular expression, click Advanced Config Search.

    a. Select the appropriate delimiter from the Must/Must Not Contain list.

    b. Select the appropriate type in the String Type list.

    c. Type your string or expression in the String box.

    See Regular Expression Pattern Matching Examples for help with regular expressions.

    Note: If there are some special non-printable characters at the end of the lines in a downloaded config, the $ operator might not match the line end. A test would be to copy lines from a config to a plain text file (in Notepad, for example); if you see extra, empty lines that are not in the pasted content then there are mostly likely non-printable characters in them.

    d. If you want to build conditions into your search, click Add Another String and create the string, as before.

    e. Repeat this step for as many strings as you need to define your search.

    For example, let’s assume that you need to search configs for occurrences of the string “access list” in conjunction with different names (Joe, Sam, Tom). To build the appropriate conditions into the search, you would create the following logic:

    Must Contain ^(?=.*?\bAccess-list\b)(?=.*?\joe\b).*$

    OR Must Contain ^(?=.*?\bAccess-list\b)(?=.*?\sam\b).*$

    OR Must Contain ^(?=.*?\bAccess-list\b)(?=.*?\tom\b).*$

A violation of this rule logic occurs if NCM finds in a line in a config that includes the string ‘Access-list’ and the string joe, sam’ or ‘tom’.

Note: In general, SolarWinds does not offer support in constructing regular expressions and instead expects NCM users to be proficient in creating their own. This example is to demonstrate how to use the resource NCM makes available to build a complex conditional statements using regular expression.

For more information on working with regular expressions see http://msdn.microsoft.com/en-us/library/az24scfc.aspx.

f. If needed, adjust the operators (And/Or) to determine relationships between strings in the execution of your search.

The default operator is ‘and’.

g. If needed, 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. And 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 doesn’t 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.

12. Select the search context under Search Config File/Block.
13. As needed, create a script in the Remediation box 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 (Telnet, SSH). Essentially, your script should put the device into configuration mode, make a series of config commands, and then logout.

14. Click Test to validate the rule against a device configuration.

    a. Select a node and config against which to test the rule.

    b. Click Test Rule Against Selected Config.

    Notes:

    The rule testing feature is available only in the Orion Web Console integration.

    Test your rule against at least two nodes and configurations, one known to comply the rule, the other known not to comply.

In testing a rule against a non-compliant configuration, you see a result that includes the rule and its violation. For example, if you were attempting to disable Reverse-Telnet with your rule, you would see something like this in case the config under test violates the rule:

Pattern 'line con 0.*\n(.*\n)*.*transport input none' was not found

This tells you that the NCM policy software used the regular expression specified under String Matching to search the specified config file and no matches were found. Since it expected to find the specified string, the software generates an alert.

c. Click Select Different Config to continue your rule test on another node/config. Repeat this step for as many spot checks you need to do among your network devices and configs.

d. Click Close when your are finished testing with the rule.

15. When you are ready to save the rule, click Submit.
16. See these steps to include this rule in a policy.

Executing a Policy Report

A policy report shows rule violations contained within the policies of the report.

To execute a policy report:

1. Select the policy report you want to execute in the Policy Reports list.
2. Click Reports > Execute Selected Reports.

   Note: When viewing a report, mouse over any rule or violation icon to display a description of the item.
3. To display and make changes to a configuration file that has violated a rule, right-click the violation icon, and then click View / Edit Config.
4. If you find a violation and want to execute a script on the device to make a change, right-click the device name, and then click Remediate Rule Violation. For more information, see "Executing Command Scripts" on page 147.

Rules

Rules describe what is to be found (or not found) in device configuration files. Rules contain the following properties:

Property	**Description**
Name	How the rule will be shown in display lists and Reports
Description	Description of the rule
Alert Level	Severity of the alert (informational, warning, critical)
Grouping	Folder to which the rule belongs
Pattern Must Exist	Whether the pattern should be found or not
String	Regular expression or string that defines the search object
String Type	Type of search expression (regular expression or find string)

If the Advanced Config Search feature is activated, string matching includes these additional properties:

Property	**Description**
And/Or	Operator that defines the relationship between two strings
Parentheses	Operator that logically groups strings
Must/Must Not Contain	Determines if the alert triggers based on the presence or absence of a string
String	Regular expression or string that defines the search object
String Type	Type of search expression (regular expression or find string)

Editing a Policy Rule

If you need to modify a rule to update a change in your policies, you will need to edit the rule. Complete the following procedure to modify your rule.

To edit a rule:

1. Login on the Orion Web Console website with an administrator account.
2. Click Configs on the modules menu and select the Compliance view.
3. Click Manage Policy Reports.
4. Click the Manage Rules tab.

5. Select the rule you want to edit, then click Edit.
6. Edit the appropriate values.

   See Creating a Rule for information on working with the rule template.
7. Review the rule details, and then click Submit.

Deleting a Policy Rule

Complete the following procedure to delete a rule.

To delete an existing rule:

1. Login on the Orion Web Console website with an administrator account.
2. Click Configs on the modules menu and select the Compliance view.
3. Click Manage Policy Reports.
4. Click the rule you want to delete, then click Delete.
5. Click Yes.

Policies

A policy is a collection of one or more rules. These rules define the type of configuration file to search and the nodes that are included in the search.

Editing a Policy

If you need to modify a policy, complete the following procedure.

To edit a policy:

1. Login on the Orion Web Console website with an administrator account.
2. Click Configs on the modules menu and select the Compliance view.
3. Click Manage Policy Reports.
4. Click the policy you want to edit, then click Edit.
5. Edit the appropriate values.

   See Creating a Policy for information on working with the policy template.
6. Review the policy details, and then click Submit.

Deleting a Policy

Complete the following procedure to delete a policy.

To delete a policy:

1. Login on the Orion Web Console website with an administrator account.
2. Click Configs on the modules menu and select the Compliance view.
3. Click Manage Policy Reports.
4. Click the policy you want to delete, then click Delete.
5. Click Yes.

Policy Reports

Reports provide a way to group policies, either by the devices that they will be executed against or by the type of report in which they are used. Report properties include Name, Comment, Grouping, and the policies included in the Report.

Editing a Policy Report

If you need to modify a report to update a change in your policies, complete the following procedure.

To edit a report:

1. Login on the Orion Web Console website with an administrator account.
2. Click Configs on the modules menu and select the Compliance view.
3. Click Manage Reports, select the report you want to edit, then click Edit.
4. Edit the appropriate values.

   See Creating a Report for information on working with the policy template.
5. Review the report details, and then click Submit when you are satisfied with the new values.

   Note: When viewing a report, mouse over any rule or violation icon to display a description of the item.
6. To display and make changes to a configuration file that has violated a rule, right-click the violation icon, and then click View / Edit Config.

Generating a Policy Report

Whenever you want to review a report for current compliance status, complete the following procedure.

To generate a policy report:

1. Login on the Orion Web Console website with an administrator account.
2. Click Configs on the modules menu and select the Compliance view.
3. Click Manage Reports, then click the report in the list to generate a current version.

   When viewing a report, mouse over any rule or violation icon to display a description of the item.
4. Click View Config if you need or want to see the entire configuration file on which the report for this node is based.
5. If you want to execute a remediation script for the specific node, click Execute Remediation Script on this Node.
   a. In the Execute Traffic Remediation Script resource, enter or modify the script so that it includes commands that will be accepted by your device.
   b. Click Execute Script when you are ready to run the remediation script on the selected node.
6. If you want to execute a remediation script for all nodes in violation of the specific rule, click Execute Remediation Script on All Nodes.
   a. In the Execute Traffic Remediation Script resource, enter or modify the script so that it includes commands that will be accepted by your devices.
   b. Click Select Nodes to confirm or modify the nodes against which your script will run.
   c. Click Execute Script when you are ready to run the remediation script on the selected nodes.

Exporting a Policy Report (to thwack)

Use the following steps to share a policy report with your user community on thwack.com.

To export a policy report:

1. Login on the Orion Web Console website with an administrator account.
2. Click Configs on the modules menu and select the Compliance view.
3. Select the relevant report in the folders under Manage Reports.
4. Click Export to thwack.

5. Enter your thwack credentials if prompted.
6. Click Close.

Exporting a Policy Report (as a file)

Use the following steps to a policy report on a file system.

To export a policy report:

1. Login on the Orion Web Console website with an administrator account.
2. Click Configs on the modules menu and select the Compliance view.
3. Select the relevant report in the folders under Manage Reports.
4. Click Export as File.
5. Pick a file type, find an appropriate location for the file on your computer and then click Save.

   Note: You must have Microsoft Excel installed to use the Excel Spreadsheet option. SolarWinds NCM does not currently support the Microsoft Office 2010 software package.

Deleting a Report

Complete the following procedure to delete a report.

To delete an existing report:

1. Login on the Orion Web Console website with an administrator account.
2. Click Configs on the modules menu and select the Compliance view.
3. Click Manage Reports, click the report you want to edit, then click Delete.
4. Click Yes.

Scheduling a Policy Report

A policy report can be scheduled to run at any time.

To schedule a policy report:

1. Open SolarWinds Network Configuration Manager in the SolarWinds program group.
2. Click Reports > Schedule Report.
3. Type a name for the job, and then click Next.
4. Select the frequency of the job from the Schedule Job list.

5. Type or select a time in the Start Time field.
6. Type or select a date in the Starting On field.
7. Type or select a date in the Ending On field. To assign a job to run with no end date, leave this field blank.
8. If you want to run the job daily, type a number in the Every days field to set the daily frequency.
9. If you want to run the job weekly, complete the following procedure:
    a. Type a number in the Every weeks on field to set the frequency.
    b. Select the days of the week you want to run your job.
10. If you are running your job monthly, complete the following procedure:
    a. Type a number in the Every months on field to set the frequency.
    b. Select each month you want to run your job.
11. Click Next.
12. Type the Windows user account name for the job.
13. Type the password for the user account in the appropriate password fields.
14. Click Finish.
15. Type any comments in the Comments field.
16. Click Report.
17. Select the policy report that is to be executed when the job is run.
18. Click Report Destinations.
19. If you want to print the results, complete the following procedure:
    a. Select Print Results.
    b. Select a printer from the Printer list on the Printer Settings tab.
20. If you want to write the results to a file, complete the following procedure:
    a. Select Save Results To File.
    b. Click the File Settings tab.
    c. Type or browse to the file in which you want to write the results in the Path and Filename field.
    d. If you want to ignore results that do not contain errors, select Only save results if this job encounters an error during execution.
21. If you want to email the results, complete the following procedure:

a. Select E-Mail Results.

b. Click the Email Settings tab.

c. Type the email addresses to which you want to send the results in the To, CC and BCC fields. Use a semicolon to separate multiple email addresses.

d. Type the subject of the email in the Subject field.

22. If you want to log the job steps to a log file, select Log job steps to JOB-#####.log.
23. If you want to ensure that all Notification settings are configured properly, click Test Notifications.
24. If you need to change the Windows account information, complete the following procedure:

    a. Click the Security tab.

    b. Type the Windows account name that will be used to run the job.

    c. Click Set Password.

    d. Type the password for the Windows account in the appropriate password fields.

25. Click OK.

Modifying Policy Reporter Settings (Application)

Complete the following procedure to modify the SolarWinds Network Configuration Manager Policy Reporting settings.

To adjust policy reporting settings:

1. Open the SolarWinds Network Configuration Manager Policy Reporter in the SolarWinds program group.
2. Click File > Settings.
3. Select the tabs you want to display on startup in the Startup Options group.
4. If you want to group reports by the report group, select Use Grouping on Report List.
5. Select the report display options you want to enable in the Report Options group.

Enabling the Policy Cache

By default, if you enable policy caching, the policy cache is automatically updated at 11:55 pm every evening. You can modify the update time by using the NCM Cache Settings (Settings > NCM Settings > Advanced Settings).

The policy cache data is used to display policy and compliance information in the Web Console.

Enabling the policy and config caches occurs with the same control.

To enable the policy cache:

1. Open the Orion Web Console.
2. Click Settings.
3. Click NCM Settings.
4. Click Advanced Settings.
5. Select Enable Config and Policy Caches under Cache Settings.
6. Set the time when the policy cache will be generated each day.
7. Click Submit.

   You can immediately refresh the policy cache and display the most up-to-date information on the Orion Web Console.

To manually refresh the policy cache:

1. Click the Configs modules bar on the Orion Web Console, and then click the Compliance view.
2. Click Update All to refresh the policy cache.

   When you run a policy report or a scheduled job from the SolarWinds NCM application, the data returned is a snapshot of current policy compliance and does not rely on the policy cache.

Using the Policy Creation Wizard (Application Only)

The SolarWinds Network Configuration Manager Policy Reporting application is launched by clicking **Reports > SolarWinds Network Configuration Manager Policy Reporter** from the SolarWinds Network Configuration Manager application.

The Policy Creation wizard allows you to create a complete policy report, including the creation of rules and policies. Complete the following procedure to create a policy report using the Policy Creation wizard.

To create a policy report:

1. Click File > Policy Creation Wizard.
2. Review the welcome text, and then click Next.
3. Review the introduction to rules, and then click Next.
4. Click Walk me through creating a new Rule, and then click Next.
5. Type a name for your new rule, and then click Next.
6. Type any comments in the Comment field.
7. If you want to assign this rule to a group, type a new group name in the Grouping field or select an existing group from the list.
8. Click Next.
9. If you want to use a regular expression for your search pattern, complete the following procedure:
   a. Set the Search Pattern Type to RegEx Expression.
   b. Type the expression in the Search Pattern field. For more information see “Regular Expression Pattern Matching” on page 371.

Note: To view examples, click Example Search Patterns.

10. If you want to use a simple expression for your search pattern, complete the following procedure:
    a. Select Simple Find for the search pattern type. The simple find expressions allow you to use the asterisk and question mark (?) characters as wildcard characters.
    b. Type the expression in the Search Pattern field.
11. Click Found or Not Found to determine how violation is defined, and then click Next.
12. Click Informational, Warning, or Critical to set the severity of your rule, and then click Next.
13. Review the Rule Details, select Save This Rule, and then click Next.
14. Review the introduction to policies, and then click Next.
15. Click Yes, Let’s Create a New Policy, and then click Next.
16. Type a name for your new policy.
17. Type any comments in the Comment field.

18. If you want to assign this policy to a group, type a new group name in the Grouping field or select an existing group from the list.

19. Click Next.

20. If you want to select which devices the policy applies to, complete the following procedure:

    a. Click Add Devices.

    b. Select the devices you want to add to the list.

    c. Click OK.

21. If you want your policy to apply to all devices, click Select Nodes Directly, and then click All Nodes in the Database.

22. If you want your policy to apply to a specific group of nodes, complete the following procedure:

a. Click Select Nodes Directly

b. Click Specify Selection Criteria.

c. Click Browse, and then click Add a Simple Condition.

d. Click the first asterisk, and then click the appropriate field.

e. If you want to change the comparison operator, click is equal to, and then click the comparison operator you want to use.

f. Click the second asterisk, and then type the value or select it from the list.

   Note: All values currently in the database for the field are displayed when you browse the list.

5. Click Next, and then select the configuration file types you want to search when executing this policy. Any searches the last downloaded configuration file, regardless of type.

6. Click Next, and then select the rules in the All Rules list you want to add to your policy, and then click the Right Arrow to add the rules to the Assigned Rules list.

7. Click Next, and then click Yes to save the new policy.

8. Click Next, and then click Yes, Let’s Create a New Report, and then click Next.

9. Type a name for your new report.

10. Type any comments in the Comment field.

11. If you want to assign this report to a group, type a new group name in the Grouping field or select an existing group from the list.

12. Click Next, and then select the policies in the All Policies list you want to add to your report, and then click the Right Arrow to add your selection to the Assigned Policies list.
13. Click Next, and then click Yes to save the new report.
14. Click Exit.

Chapter 12

Managing Jobs

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

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

Notes:

- Orion Platform Administrator, NCM Administrator and NCM Engineer roles have full access to all jobs in the job list. Other assigned NCM roles can access and manage only the jobs they create but not others.
- If you are an Orion platform administrator with account limitations that are designed to limit your area of operation to a specific set of nodes, but you use NCM job editing controls to limit the nodes upon which a specific job acts, NCM will not honor those node limitations. Keep in mind that any job you create or edit will affect all nodes to which your Orion platform Administrator account gives you access.

Enabling and Disabling a Job

Enabling or disabling operations apply to jobs that run according to a schedule. You can delete any job you no longer use.

Enabling a Job

You must enable a job before you can start it.Trying to start a job that is not enabled will fail.

To enable a job:

1. Open the Orion Web Console and navigate to the NCM Jobs view (CONFIGS > Jobs).
2. Select the job in the list.
3. If the job is currently disabled, click Enable.

Disabling a job

If you need to suspend a job but not delete it use the disable feature.

To disable a job:

1. Open the Orion Web Console and navigate to the NCM Jobs view (CONFIGS > View).
2. Select the job in the list.
3. Click Disable.

Starting and Stopping a Job

Though using a schedule is the most efficient way to manage jobs, you can manually start and stop jobs. as needed.

Starting a Job

You can start any job that is enabled. Trying to start a job that is not enabled will fail.

To start a job:

1. Open the Orion Web Console and navigate to the NCM Jobs view (CONFIGS > View).
2. Select the job in the list.
3. If the job is currently disabled, click Enable.
4. Click Start.

Stopping a job

A job currently running shows the status ‘running’.

To stop a job:

1. Open the Orion Web Console and navigate to the NCM Jobs view (CONFIGS > View).
2. Select the job in the list.
3. Click Stop.

Creating or Editing a Job

You must be an Orion platform administrator to create and manage jobs. However, if you are an Orion platform administrator with account limitations that are designed to limit your area of operation to a specific set of nodes, but you use NCM job editing controls to limit the nodes upon which a specific job acts, NCM will not honor those node limitations. Any job you create or edit will affect all nodes to which your Orion platform Administrator account gives you access.

Note: When running an active job, NCM uses the credential settings of the user who last edited the job. So, for example, if the user has user level login credentials set, NCM uses those credentials in running the job. Otherwise, NCM runs the job by using device credentials (defined manually or through a connection profile) on each relevant node's Node Details page.

Use these procedures to create a new job or edit an existing one.

To create or edit a job:

1. Open the Orion Web Console and navigate to the NCM Jobs view (CONFIGS > Jobs).
2. If you are creating a new job, click Create New Job, select the appropriate job type, give the job a title.
3. If you want to edit an existing job, click Edit.
4. Select the schedule type.

    Basic gives you Once, Daily, Weekly, and Monthly schedule settings (start, end, recurrence). .

    Advanced gives you more granular control over the schedule, supporting more complex patterns defined with cron expressions.

5. If you are creating a Basic schedule, select the frequency of the job.

    Once: enter a day and time (at least 15 minutes from current NCM server time).

    Daily: Select Every Day or Every Week Day, enter a Start time, and then select start and end dates

    Weekly: Select the days, enter a Start time, and then select start and end dates.

    Monthly: Select the months, days of the month, enter a Start time, and then select start and end dates

6. If you are creating an Advanced schedule, use the five fields to create the appropriate cron expression.

    For example, if you want the job to run once a week over every month at midnight on Sunday morning, the values for the fields would be 0 0 * * 0.

    This transliterates as telling NCM to run the job at 0 minutes and 0 hours, on all valid days of month, in all valid months, on Sunday".

7. Add a comment as needed and then click Next.

8. Select the NCM nodes to target with this job.

  Select Nodes: Click Select Nodes and select the NCM nodes you want the job to target.

  All Nodes: Selects all NCM nodes as targets for the the job.

  Dynamic Selection: Define the criteria that NCM will use to determine the selection of NCM nodes as targets for the job.

  Nodes defined in legacy job scheduling system: Select the option and then click Yes, change selection.

  Note: Use this option to target the node group of all wireless access points in the database.

9. Select an email notification option.

  a. If you select Email Results, then enter the email from/to information.

  b. Enter the email server address and port number.

  c. If the email server expects credentials, then select Password.

  d. Enter the username and password.

10. Click Next.

The Add Job Specific Details page displays.

11. Add details based on the resource the specific job provides.

Executing a Script

12. If you are executing a script, do these things:

  a. If you want to enter or edit a script, use the text box.

  What you enter in the text box is what NCM executes against the selected NCM nodes.

  b. If you want to save a script, click Save Script, specify a location, and then click Save.

  c. If you want to load an existing command script, click Load Script, browse to your command script file, and then click Open.

  d. Select Filter results that match a pattern if you want to see in the script output only those lines that match a specific regex pattern

  e. Select Show commands in output to view what NCM sent to the targeted devices.

  f. Click Next.

Uploading a Config to a Device

13. If you are uploading a config to a device, do these things:

- **a.** If you want to select config changes from a config in the database, click Load Script, browse to your command script file, and then click OK.
- **b.** If you want to select a config snippet, click Select Config Changes from Snippet, and copy the relevant snippet from the Select Config Snippet box.

  For more information on config snippets see “Uploading a Config Snippet”.
- **c.** If you want to select config changes from a config in the database, click Select Config Changes from Database, locate the config in the node tree, and the click OK.
- **d.** Verify the config information in the Upload Changes to Devices Job box is what you want NCM to upload.
- **e.** Select Write config to NVRAM after upload if you want the upload to reside in RAM.
- **f.** Click Next.

Running a Report (Job Details)

14. If you are running a report, do these things:

- **a.** Select a report on the Job Details resource.

  Note: Only one report can be executed at a time. To execute more than one report, a new job will have to be created for each additional report.
- **b.** Click Next.

Exporting Configs (Job Details)

15. If you are exporting a config, do these things:

- **a.** Set the template for the filename structure.
- **b.** Select the types of configuration file to export.
- **c.** Choose whether to export all configurations, or only the last downloaded for each node.
- **d.** Click Next.

Perform Routine Database and Archive Maintenance (Job Details)

Note: the NCM Maintenance job does not rebuild the database index.

16. If you are performing database maintence, do these things:

a. Select one or more purge operations and, for each, select a cutoff.

Purge configs from the config archive folder older than: Selecting this operation purges archived config files from the NCM server that are older than the selected age.

Purge config cache data older than: Selecting this operation purges config cache data from the database that are older than the selected age.

Purge completed Approval Requests older than: Selecting this operation purges completed config change approval requests from the database that are older than the selected age.

b. Click Next.

Update Inventory (Job Details)

17. If you are updating inventory, do these things:

a. Select the information types you want to include in your Inventory job. (By default, all inventory information is included.)

b. Click Next.

18. If you are generating a config change report, do these things:

a. If the job you are editing does not have a Config Change Report Job page, skip to step 54.

b. Select the type of config change report to generate on the Config Change Report Job page and then click Next.

The choices are as follows:

Compare most recent Download to the Runing Startup, or Baseline Config:

This will display all the differences between the last downloaded configuration file and most recent version of the selected configuraton type.

Compare the most recent Download to the Configuration on a specified date:

This will show you all differences between the most recent downloaded configuration file and a configuration file from the specified date.

Note: If no configuration file was downloaded on the specified date, the next configuration file downloaded after that date will be used.

Show changes made over the past ## days:

This will show you all changes that were made over the specified amount of days.

Show changes made between one date and another:

This will show you all changes that were made over the specified date range.

c. Click Next.

Generate a Policy Report (Job Details)

19. If you are generating a policy report, select the policy report that is to be executed when the job is run.

    a. If you want to suppress notifications when no violations are found, select Send Notification only when Policy Violations are present.

    b. Click Next.

Purge Old Configs from Database (Job Details)

20. If you are purging old configs from the database, do these things:

    a. Select a config purge option..

       If you want to purge configs before a specific date, select Purge all configs that were downloaded before this date, use the calendar tool to adjust the date. Click Include time and select a time if you want the purge to include those configs on the selected date that are timestamped before your selected time.

       If you want to delete all except a specific number of most recently downloaded configs, select Delete all configs except for the last XX current configs and insert an appropriate number.

       If you purge all configs except those falling within a recent time span, select Purge all configs except fort he last XX and select a interval.

       If you want to protect base configs as NCM takes action on your purge setting, select Do not purge any baseline configs.

    b. Click Next.

Download Configs from Devices

21. If you are downloading configs from devices, do these things:

- **a.** Select the configuration types you want to download on the Download Config Job page.
- **b.** If you want to be notified when the downloaded configuration file is different from the last configuration, select Last downloaded config file.
- **c.** If you want to be notified when the downloaded configuration file is different from the baseline configuration, select Baseline config file.
- **d.** If you want to be notified when the downloaded configuration file is different from the startup configuration, select Startup config file.
- **e.** Select Send config change notification details in a separate text email and Send config change notification details in a separate HTML email as appropriate. These options allow you to separate change details from change notification.
- **f.** If you only want to save the configuration file when changes are found, select Only save Configs that have changed.
- **g.** Click Next.

Baseline Entire Network (Job Details)

22. If you are baselining the network, do these things:

- **a.** If you want to use the last config downloaded from each device as your baseline, select Set the Network Baseline to the last Config downloaded from each Node.
- **b.** If you want to set the Network Baseline to a spefic date, select Set the Network Baseline to a specific date and select a date.
- **c.** If instead of setting the baseline you want to remove existing baselines, select Clear all Baselines.
- **d.** Click Next.

23. Review the settings for the job.

24. When you are done reviewing the settings, click Finish.

Viewing Job Logs

If you ever need to verify that a job was run as scheduled, or to view the history of the job, view the job log.

To view a job log:

1. Open the Orion Web Console and navigate to the NCM Jobs view (CONFIGS > Jobs).
2. Select the job in the list and view its Last Date Run and History information.

Deleting a Job

You can permanently remove rather than temporarily disable a job, as needed.

To delete a job:

1. Open the Orion Web Console and navigate to the NCM Jobs view (CONFIGS > Jobs).
2. Select the job in the list.
3. If the job is currently disabled, click Delete.

Viewing and Modifying Scheduled Jobs

Any job created with SolarWinds Network Configuration Manager can be viewed and modified with the Windows Task Scheduler. You can launch the Windows Task Scheduler from the Control panel. For more information, see your Windows documentation.

Chapter 13

Approving Device Configuration Changes

SolarWinds Network Configuration Manager enables you to define a semi-automated approval process for making configuration changes on network devices.

SolarWinds NCM uses roles to determine which Orion accounts are able to perform the tasks of changing device configurations (WebUploader), approving those changes (Administrator), and changing the roles of Orion accounts (Engineer, Administrator).

SolarWinds NCM uses email to relay config change approval requests. As part of setting up the config change approval system, you must provide SMTP information.

The following sections cover topics related to using the device configuration change approval system.

Enabling and Disabling Config Change Approval

SolarWinds NCM uses the Windows Job Scheduler to perform scheduled work. When you enable the change approval system, SolarWinds NCM prevents the system from executing device uploads—keeping them in a disabled state—until an NCM Administrator has manually approved the scheduled job.

When you disable the system, SolarWinds NCM processes device configuration changes normally, either as scheduled or immediately, depending on the actions of the relevant team member with the WebLoader account privileges.

You must setup the system before the change request approval queue can be processed. To setup the system, refer to “Setting-up the Config Change Approval System”.

To enable the change approval system:

1. Login on the Orion Web Console with an administrator account.
2. Click Configs on the modules menu and then click NCM Settings.
3. Click Enable Approval System in the Config Management Change Approval group.

To disable the change approval system:

1. Login on the Orion Web Console with an administrator account.
2. Click Configs on the modules menu and then click NCM Settings.
3. Click Disable Approval System in the Config Management Change Approval group.

Setting-up the Config Change Approval System

SolarWinds NCM uses email to relay config change approval requests. The Setup Wizards guides you through the process of setting up the email server the system will use, the addresses of Administrator who will receive change configuration approval requests, and the user accounts of team members who either manage device configurations or approve their changes.

To setup the change approval system:

1. Login on the Orion Web Console with an administrator account.
2. Click Configs on the modules menu and then click NCM Settings.
3. Click Setup Wizard in the Config Management Change Approval group of features.
4. Enter SMTP settings.
   a. Enter your E-mail Server Address and Port Number on the SMTP setup page.
   b. Select SSL if needed.
   c. Select an Authentication type and enter credentials if needed.
   d. Click Submit.
5. Enter Email settings.
   a. Enter an appropriate email address or list of email addresses in the To: box.

   The address(es) in this box will receive notifications of pending device config changes.

   b. Enter an address in the From: line.

   This address will be shown as the sending address for config change approval requests.

c. Enter a description (for example, “NCM Approval Needed”) in the Subject: line.

This description will appear in the subject line of config change approval requests.

d. Add an additional message regarding config change approval requests.

This note should inform approvers of the standard action to take. For example: “An approval request has been submitted in NCM. Please login to NCM and manage the request.”

e. Click Submit.

6. Click MANAGE USERS.
7. If the account you want to manage does not appear in the list under Individual Accounts, click Add New Account.

a. Click Orion individual account.

b. Enter a User Name and Password.

c. Assign appropriate settings for this Orion individual account.

Note: Specifically decide if this account should have Administrator Rights and Node Management Rights.

d. Assign appropriate account limitations.

For information on setting up account limitations, search the Help system for ‘account limitations’.

e. Accept the current defaults under Default Menu Bar and Views.

This account holder will be able to access these settings after account setup and customize them as preferred.

f. Assign a role appropriate role to the account under Network Configuration Manager Settings.

Note: The account must at least be a WebUploader for the account holder to make configuration changes to network devices.

g. Accept the defaults for other Network Configuration Manager Settings and Orion General Settings.

Besides the role setting, the account holder will be able to access all other settings after account setup.

h. Click Submit.

8. If the account you want to manage appears on the list under Individual Accounts, click Edit.

a. Assign appropriate settings for this account.

Note: Specifically decide if this account should have Administrator Rights and Node Management Rights.

b. Assign any appropriate account limitations.

For information on setting up account limitations, search the Help system for ‘account limitations’.

c. Accept the current defaults under Default Menu Bar and Views.

This account holder will be able to access these settings after account setup and customize them as preferred.

d. Assign a role appropriate role to the account under Network Configuration Manager Settings.

Note: The account must at least be a WebUploader for the account holder to make configuration changes to network devices.

e. Accept the defaults for other Network Configuration Manager Settings and Orion General Settings.

The account holder will be able to customize the appearance of the Orion Web Console.

f. Click Submit.

Managing NCM Approval Requests

This resource enables NCM users to view requests and NCM administrators to view, approve and decline them.

To approve or decline request:

1. Login on the Orion Web Console with an administrator account.
2. Click Configs on the modules menu and then click NCM Settings.
3. Click Pending Approval in the Config Mnagement Change Approval section.
4. If you are looking for a specific request, enter the requester’s NCM username in the Search window and click the icon.
5. Select the appropriate request(s) in the list and then click Approve or Decline, as needed.

Creating and Editing an NCM Account

Orion accounts are setup for NCM mainly in terms of the NCM role associated with them. The roles currently available in NCM are:

Administrator

This role has unlimited access to NCM functionality, including device configuration management, user account management, configuration change approvals.

Engineer

This role has Administrator privileges but cannot view the device configuration transfer status for all users.

WebUploader

This role has read/write access on network devices but cannot change device configurations without Administrator approval.

WebDowloader

This role can download can read and download network device configurations.

WebViewer

This role can only read network device configurations.

None

This role cannot access NCM features and functions.

An SolarWinds NCM user logs-in directly at the network device with unencrypted credentials; and can perform whatever level of action the account is permissioned for.

Should the network administrator want to use the same credentials for SolarWinds NCM login on all network devices, the NCM software provides a Global Login (Settings > NCM Settings > Global Device Defaults > Device Login Information) and an option to enable global login settings on all devices. See the section Setting Node Communication Defaults.

If a network administrator sets-up third-party authentication such as a Radius or TACACS server, part of the setup should involve defining valid accounts and permissions in the authentication server database for appropriate SolarWinds NCM users.

In any case, NCM only interacts with network devices, not the authentication server. Though the network device must handle interaction with Radius, TACACS, or any other authentication server, there is special logic in the relevant NCM component (SWTelnet9) to handle the RADIUS authentication prompt since devices connected to the RADIUS server may have a slightly different login flow.

Use the following procedures in the following sections to create or manage an Orion account for use with SolarWinds NCM.

Only a user with Administrator privileges can create a new account. Use the following procedures to create, edit, or remove an account.

To create a new account:

1. Login on the Orion Web Console with an administrator account.
2. Click Configs on the modules menu and then click NCM Settings.
3. Click MANAGE USERS.
4. Click Add New Account.
5. Click Orion individual account.
6. Enter credentials for the new account.
7. Click Next.
8. Assign appropriate settings for this Orion individual account.

   Note: Specifically decide if this account should have Administrator Rights and Node Management Rights.
9. Assign appropriate account limitations as needed.

   For information on setting up account limitations, refer to the SolarWinds Platform Administrator Guide.
10. Accept the current defaults under Default Menu Bar and Views.

    The account holder will be able to customize these settings.
11. Assign the role under the Network Configuration Manager Settings that allows the account holder to perform the tasks relevant to their job.

    Note: The account must at least be a WebUploader for the account holder to make configuration changes to network devices.
12. Accept the defaults for other Network Configuration Manager Settings and Orion General Settings.

    The account holder will be able to customize these settings.
13. Click Submit.

To edit an existing SolarWinds NCM account:

1. Login on the Orion Web Console with an administrator account.
2. Click Configs on the modules menu and then click NCM Settings.
3. Click MANAGE USERS.
4. Select an account by name and click Edit.

5. Click Orion individual account.
6. Enter a User Name and Password.
7. Assign appropriate settings for this Orion individual account.

   Note: Specifically decide if this account should have Administrator Rights and Node Management Rights.
8. Assign appropriate account limitations.

   For information on setting up account limitations, search the Help system for ‘account limitations’.
9. Accept the current defaults under Default Menu Bar and Views.

   This account holder will be able to access these settings after account setup and customize them as preferred.
10. Assign a role appropriate role to the account under Network Configuration Manager Settings.

    Note: The account must at least be a WebUploader for the account holder to make configuration changes to network devices.
11. Accept the defaults for other Network Configuration Manager Settings and Orion General Settings.

    Besides the role setting, the account holder will be able to access all other settings after account setup.
12. Click Submit.

To delete an account:

1. Login on the Orion Web Console with an administrator account.
2. Click Configs on the modules menu and then click NCM Settings.
3. Click MANAGE USERS.
4. Select an account and click Delete.

Chapter 14

Understanding the Web Console

The Web Console, provided with SolarWinds Network Configuration Manager, offers you access to your device configs without requiring physical access to your SolarWinds NCM server. Through the Web Console, you gain flexibility and power. You can perform any of 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

Launching and Logging On to the Web Console

To launch the Web Console, point any remote browser to the SolarWinds NCM server: `http://`*`hostnameOrIPAddress`*`:`*`port`*. Where, hostnameOrIPAddress is either the hostname or IP address of the SolarWinds NCM server and port is the Web Console port defined for the website.

To Login on the Web Console, you can use either Windows credentials or an SolarWinds NCM credential set. You must have previously defined the credentials using the user access control settings and associated the credentials with the Web Viewer role.

Understanding Web Console Resources

Each view within the Web Console provides a number of resources. The following sections are divided by the view on which the resources can be displayed. You can customize your views, adding and removing resources based on the account with which you Login on. For more information about customizing your views, see “Personalizing the Web Console” on page 273.

HOME

The Home view allows you to display the following resources. For more information about any of these resources, click **Help** on the resource in the Web Console.

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 Triggered Alerts

All Triggered Alerts Resource

If there are any alerts that have triggered involving the viewed node, or, if any device on the network triggers an alert if this resource is on the Network Summary Home view, they will display in the All Triggered Alerts resource. For each alert, this resource presents the date and time of the alert, the network device that triggered the alert, the current value of the alert, if available, and a description of the alert.

CONFIGS

Config Summary View

NCM Node List

Provides a list of the nodes currently managed in NCM. (All NCM nodes must also be managed as an Orion node.)

Search NCM

Allows you to 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

Provides a list of detected configuration changes, including the node, time of upload, and the type of configuration. Clicking a configuration takes you to a configuration change report showing additions, deletions, and modifications. The `BEFORE` and `AFTER` columns display the appropriate text and use the following colors to designate the detected actions:

Overall Configuration Changes Snapshot

Provides 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

Provides a pie chart designating the percentage of devices running different configurations than their startup configurations.

Overall Policy Report Violations

Provides a stacked bar chart of status of your devices in relation to a specific policy report.

Policy Violations

Provides a list of the policy reports available and a brief overview of the contents of each report.

Overall Baseline vs. Running Config Conflicts

Provides 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

Provides 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

Provides a pie chart designating the percentage of device that have been backed up using the SolarWinds NCM application in comparison to those that have not been backed up.

Overall Devices Inventoried vs. Not Inventoried

Provides a pie chart designating the percentage of devices inventoried in relation to those that have not.

NCM Events

Allows you to specify a time period and the configuration events you want to see displayed in an easily scanned chart.

To modify the time period you want included in the resource, click **Edit**.

Node Details Views

The Node Details view allows you to display the following resources. You navigate to the Node Details view by clicking the name of a node in the SolarWinds NCM Web Console. For more information about any of these resources, click **Help** on the resource in the Web Console.

Node Details

Provides an overview of the device you selected, including the IP Address, OS Version, Location, OS image, among other information.

Config List

Provides a list of the last X number of configurations downloaded from this device.

Download Config

Allows you to download the startup or running configuration from the current node.

Execute Script

Allows you to execute a script against the current node.

Upload Config

Allows you to upload a configuration file you have previously downloaded from the selected node.

Inventory Details

Provides a list of inventory reports that pertain to the selected device.

Policy Violations

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

Last 10 Config Changes

Provides a list of detected configuration changes, listing the user committing the change, the time of upload, and the type of configuration.

Compare Configurations

Allows you to select two configurations from different time periods to compare to one another.

Config Change Report

Allows you to specify a time period and a node, and then display a change report that covers the set time range.

NCM Events

Allows you to specify a time period and the configuration events you want to see displayed in an easily scanned chart.

To modify the time period you want included in the resource, click **Edit**.

Configuration Management

The Configuration Management view allows you to display the following resources. For more information about any of these resources, click **Help** on the resource in the Web Console.

View Changes

Allows you to specify a time period and a node, and then display a change report that covers the set time range.

Note: Consult this SolarWinds NCM Knowledge Base article for special setup needed to ensure the accuracy of Config Change Reports based on a date range.

Compare Selected Configs

Allows you to select any two configurations to compare to one another. You can select configurations from the same device archived at different times, a startup versus a running configuration, or you can select configuration from differing devices.

Compare to Baseline

Allows you to select a single configuration to compare to a set baseline. You must set a baseline to use this feature. For more information, see "Understanding Baselines" on page 95.

Download Config

Allows you to select nodes and download running, startup, or custom configurations for those nodes.

Execute Script

Allows you to enter or load a script from a text file to execute against the nodes you select.

Upload Config – Multi Node

Allows you to select a configuration you want to upload to multiple nodes.

Upload Config – Single Node

Allows you to select a configuration you want to upload to the source node.

Transfer Status

Provides the most recent actions taken on a node.

Config Change Templates

The Config Change Templates view allows you to display the following resources. For more information about these resources, click **Help** or see Working with Config Change Templates.

Config Change Templates

Allows you to create, edit, import, export, tag, and delete config change templates.

Shared Config Change Templates on thwack

Allows you to view and download config change templates from thwack.

Reports

The Reports view allows you to view both the supplied inventory reports and those you have created with the SolarWinds NCM. SolarWinds NCM provides over 40 unique inventory reports and allows you to create your own. For more information, see “Managing Inventory Reports”.

Compliance

The Compliance view allows you to view both the supplied policy reports and those you have created with the SolarWinds NCM application. SolarWinds NCM provides numerous policy compliance tests, while also allowing you to create your own. To ensure you are viewing the most up-to-date information, click **Update Now** on the Compliance view. For more information, see “Managing Policy Reports”.

Jobs

The Jobs view allows you to view both the supplied inventory reports and those you have created with the SolarWinds NCM application. SolarWinds NCM provides 40 unique inventory reports and allows you to create your own. For more information, see “Managing Jobs”.

End of Life

The End of Life view allows you to track the end of sales and end of life status of your NCM nodes. For more information, see “Managing End of Support and End of Sales (EOS):

Searching

The Advanced Search function allows you to search 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.

Personalizing the Web Console

You can select the resource you want to display on a particular view. To do so, click **Personalize** on the view you want to customize. You can then select the resources to include, drag-and-drop them from one column to another, or drag-and-drop them in a different order in the same column. Changes are saved as preferences associated with the logged on user account. For more information about user accounts and roles, see “Managing Web Accounts”.

Integrating with Engineer’s Toolset

When you navigate to a Node Details page, if you have the Toolset installed on the local computer, you can take advantage of a number of integration points, including the following:

- Web browser to the selected node
- Telnet to the selected node
- Ping the selected node
- Run a trace route to the selected node
- Remote desktop to the selected node

Chapter 15

Integrating NCM Actions into Orion Alerts

Orion alerting software can alert on polled, syslog, and trap data. Alerts are defined in terms of thresholds related to data in the Orion database. Scans in the form of SQL queries at set intervals detect recorded values that exceed thresholds, triggering an alert if relevant conditions pertain.

When an Orion alert is triggered, the software evaluates suppression criteria. If an alert is not qualified to be suppressed, the software executes a defined action. If no action is defined, the software merely displays the alert on the web console.

Throughout this workflow timers are used to allow the software to do its work at each step and to ensure that the alerting workflow had appropriate redundancy for timely reporting of alerts.

For an excellent overview of alerting in Orion advanced alerts, see Understanding Orion Advanced Alerts. For all specific information on advanced alerts, including detailed instructions for creating and managing them with the Orion Alert Manager, see “Using the Advanced Alert Manager”.

Types of NCM Alert Actions

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

Note: As a security enhancement related to executing NCM actions, NCM account passwords are not stored in the database. As part of configuring NCM 7.3.X, the installation software removes passwords from the database as part of the Configuration Wizard session.

In ordering NCM actions, keep in mind that NCM cannot execute an email action (to notify team members) before it takes specified NCM actions. For example, NCM must download the config from an NCM managed device before it can send the email notification about the alert. Sequence the actions accordingly.

You can use three types of NCM actions in processing an Orion advanced alert:

- Backup Running Config
- Execute Config Script
- Show Last Config Changes

Backup Running Config

With this action NCM simply downloads the latest configuration from the context node. It is the same as running Nodes > Download Configs for a selected node. 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

With this action NCM executes the command(s) that you have entered into the Command Script to Execute field. For example, if you enter `show version,` and include it as a Trigger Action on an alert, NCM will run the `show` command as part of alert processing and include the results with the alert notification.

Show Last Config Changes

With this action 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 setup your alert action.

When the alert triggers, the results of the NCM action are stored in the Orion database (in `${Notes}`) and used as part of runtime processing of an alert. You can also view this information as part of the Alert Details on any relevant alert reported through the Orion Web Console (Home > Alerts). For detailed information, see “Viewing Alerts in the Orion Web Console”.

If an alert is triggered for a node without relevant config history, NCM cannot contribute any data and the Orion alert is processed without it. So selecting this action only makes sense if you already have a history of device configurations.

Using the Default NCM Alert

When you install SolarWinds NCM 7.1.x, the software automatically creates in the Orion Alert Manager a predefined alert called “Alert me and trigger an NCM action”.

The primary purpose of this alert is to determine if the changes in device configuration are responsible for the alert triggering issue.

Accordingly, by default, this predefined alert does these three things in order:

- Backs up the running config on the alerting device
- Determines the last config changes made on the device
- Sends an email regarding the alert to a relevant administrator that includes the results of both NCM actions

The instructions in this section assume you are familiar with the Orion Alert Manager and already know how to setup an advanced alert.

For steps on creating an advanced alert see the sections on advanced alerts in “Using Orion Advanced Alerts”.

To use the default NCM alert:

1. Open the Orion Alert Manager in the Orion program group.
2. Navigate to the Manage Alerts resource (View > Configure Alerts).
3. Select “Alert me and trigger an NCM action” and click Edit.

a. On General, select Enable this Alert and select an appropriate Alert Evaluation Frequency.

b. On Trigger Condition, define the conditions in which the software launches the alert.

The default condition is a node that responds in 200 ms or more. You can adjust this condition or add conditions.

c. On Reset Condition, define the conditions in which the software resets the alert.

The default condition the node responds in 100 ms or less. You can adjust this condition or add conditions.

d. On Alert Suppression, define the conditions in which the software suppresses the alert.

The default condition is no suppression.

e. 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.

f. On Trigger Actions, create actions to execute when the software triggers the alert, and enter your NCM credentials.

As discussed, the 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.

g. On Reset Conditions, define actions to execute when the software resets the alert.

4. Click OK and then click Done.

Adding Scripted Commands to the Default NCM Alert

You can modify the default NCM advanced alert to execute specific command scripts at the time the alert is triggered.

The following example adds a simple `show version` command as a scripted action.

To add a scripted command to the default NCM alert:

1. Open the Orion Alert Manager in the Orion program group.
2. Navigate to the Manage Alerts resource (View > Configure Alerts).
3. Select “Alert me and trigger an NCM action” and click Edit.
4. On Trigger Actions, click Execute Config Script and enter the relevant command in Command Script to Execute.

   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.

5. Use the up/down arrows to move 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.

6. Click OK, then click Done.

Using Orion Advanced Alerts

Alerts are generated for network events, and they may be triggered by the simple occurrence of an event or by the crossing of a threshold value for a monitored Interface, Volume, or Node. Alerts can be set to notify different people on different days, different times of the day, different people for different events, or any combination of times, events, and people. Alerts may be configured to notify the people who need to know about the emergent event by several mediums, including:

- Sending an e-mail or page
- Playing a sound on the Orion Network Performance Monitor server
- Logging the alert details to a file
- Logging the alert details to the Windows Event Log
- Logging the alert details to the NetPerfMon Event Log
- Sending a Syslog message
- Executing an external program
- Executing a Visual Basic script
- E-mailing a web page
- Playing text-to-speech output
- Sending a Windows Net Message
- Dialing a paging or SMS service
- Sending an SNMP trap
- GETting or POSTing a URL to a web server

Creating and Configuring Advanced Alerts

SolarWinds UDT allows you to configure advanced alerts with the following features:

2. Sustained state trigger and reset conditions
3. Multiple condition matching
4. Automatic alert escalation
5. Separate actions for triggers and resets

Advanced alerts are configured using the Advanced Alert Manager, as shown in the following section.

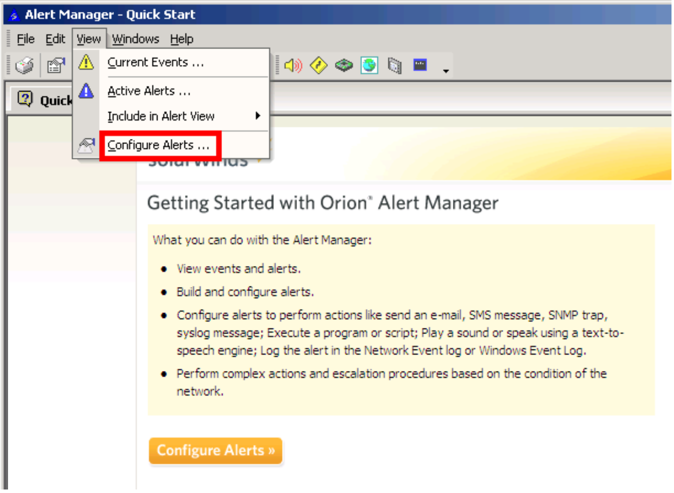
Note: If you want to configure advanced alert features, such as timed alert checking, delayed alert triggering, timed alert resets, or alert suppression, check **Show Advanced Features** at the lower left of any Advanced Alert windows. For the purposes of this document, **Show Advanced Features** is always enabled.

Creating a New Advanced Alert

The following procedure creates a new advanced alert.

To create a new advanced alert:

1. Click **Start > SolarWinds > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Configure Alerts**.

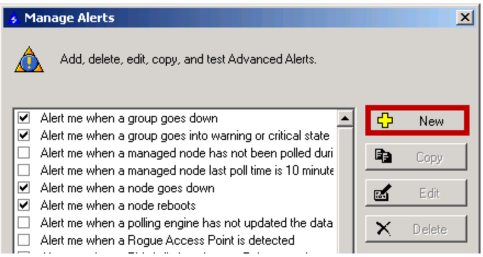


Getting Started with Orion® Alert Manager

What you can do with the Alert Manager:

- View events and alerts.
- Build and configure alerts.
- Configure alerts to perform actions like send an e-mail, SMS message, SNMP trap, syslog message; Execute a program or script; Play a sound or speak using a text-to-speech engine; Log the alert in the Network Event log or Windows Event Log.
- Perform complex actions and escalation procedures based on the condition of the network.

3. Click **New**.



Add, delete, edit, copy, and test Advanced Alerts.

☑ Alert me when a group goes down
☑ Alert me when a group goes into warning or critical state
☐ Alert me when a managed node has not been polled duri
☐ Alert me when a managed node last poll time is 10 minute
☑ Alert me when a node goes down
☑ Alert me when a node reboots
☐ Alert me when a polling engine has not updated the data
☐ Alert me when a Rogue Access Point is detected

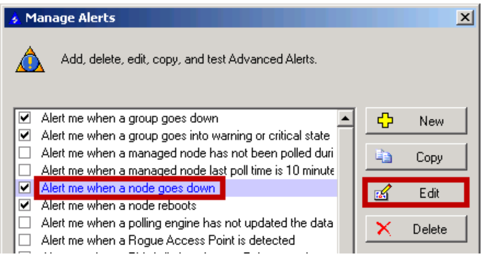
The Edit Alert window displays, providing an array of configurable alerting options, including trigger and reset conditions, suppressions, and date and time limitations. The following sections provide more information about configuring alert options.

Naming, Describing, and Enabling an Advanced Alert

Use the following steps, after clicking **New**, **Copy**, or **Edit** from the Manage Alerts Window, to name and describe an advanced alert.

To name and describe an advanced alert:

1. Click **Start > SolarWinds > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Configure Alerts**.
3. ***If you want to create a new alert,*** click **New.**
4. ***If you want to copy or edit an existing alert,*** select an alert from the list, and then click **Copy** or **Edit**, as appropriate.

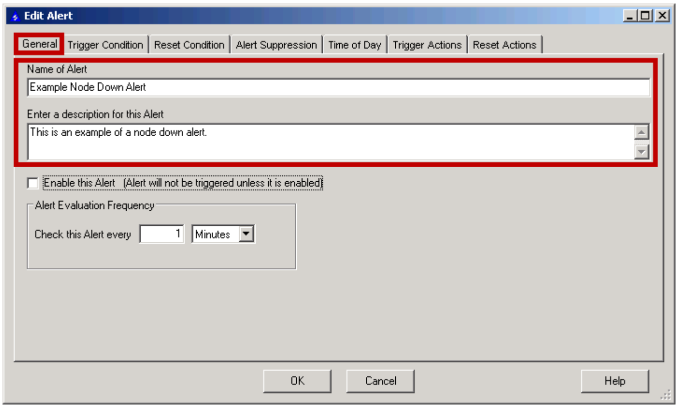


Manage Alerts

Add, delete, edit, copy, and test Advanced Alerts.

☑ Alert me when a group goes down
☑ Alert me when a group goes into warning or critical state
□ Alert me when a managed node has not been polled duri
□ Alert me when a managed node last poll time is 10 minute
☑ Alert me when a node goes down
☑ Alert me when a node reboots
□ Alert me when a polling engine has not updated the data
□ Alert me when a Rogue Access Point is detected

5. Click **General**, type the name of your alert in the **Name of Alert** field, and then type a description of your alert in the description field.



Edit Alert

Name of Alert: Example Node Down Alert

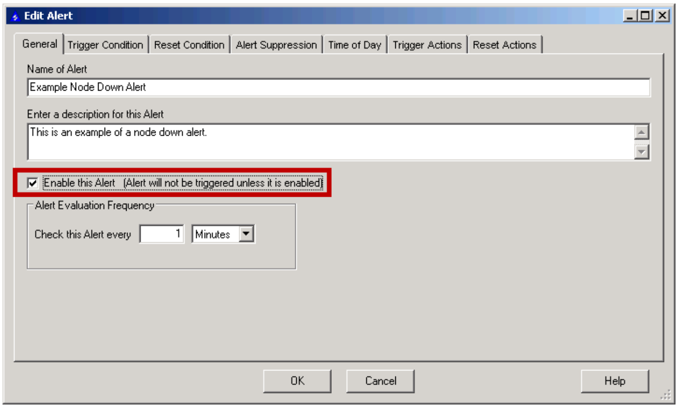
Enter a description for this Alert: This is an example of a node down alert.

□ Enable this Alert (Alert will not be triggered unless it is enabled)

Alert Evaluation Frequency

Check this Alert every 1 Minutes

6. Check **Enable this Alert**.



Name of Alert: Example Node Down Alert

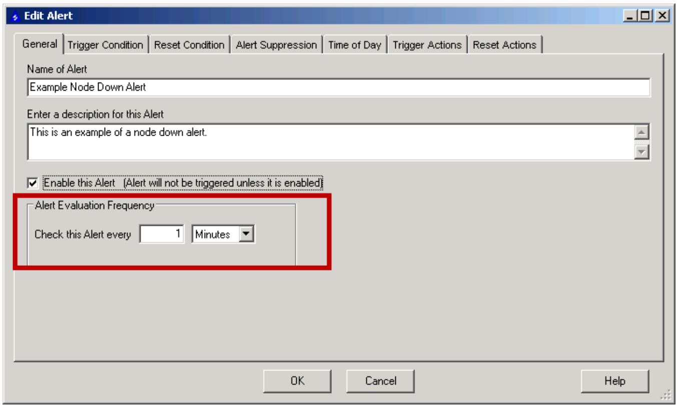
Enter a description for this Alert: This is an example of a node down alert.

☑ Enable this Alert (Alert will not be triggered unless it is enabled)

Alert Evaluation Frequency

Check this Alert every 1 Minutes

7. Type the Alert Evaluation Frequency and select Seconds, Minutes, or Hours from the list to set the checking interval for your alert.



Name of Alert: Example Node Down Alert

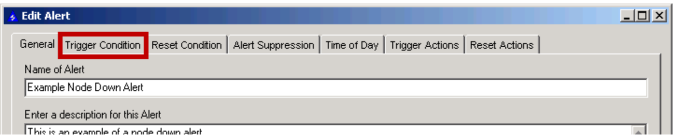
Enter a description for this Alert: This is an example of a node down alert.

☑ Enable this Alert (Alert will not be triggered unless it is enabled)

Alert Evaluation Frequency

Check this Alert every 1 Minutes

8. Click **Trigger Condition** to set the trigger condition for your alert. For more information, see “Setting a Trigger Condition for an Advanced Alert” on page 282.



Name of Alert: Example Node Down Alert

Enter a description for this Alert: This is an example of a node down alert.

Setting a Trigger Condition for an Advanced Alert

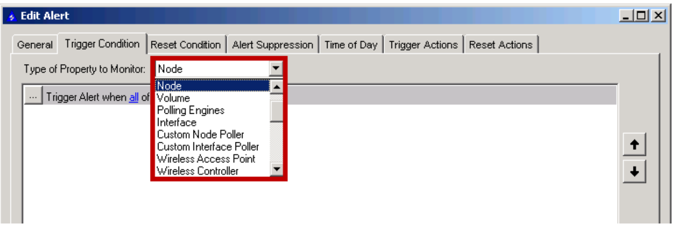
You can set the specific conditions for triggering an advanced alert with the following procedure.

Note: Properly defining alert trigger conditions to address specifc network conditions on selected network objects can eliminate the need for alert suppression conditions. SolarWinds recommends the use of appropriately specific trigger conditions to define alerts instead of suppression conditions, if possible. For more information about defining conditions, see “Understanding Condition Groups” on page 290.

To set the trigger conditions for an advanced alert:

1. Click **Start > SolarWinds > Alerting, Reporting, and Mapping > Advanced Alert Manager.**
2.
3. Click **View > Configure Alerts**.
4. ***If you want to create a new alert,*** click **New.**
5. ***If you want to copy or edit an existing alert,*** select an alert from the list, and then click **Copy** or **Edit**, as appropriate.
6. Click **Trigger Condition**.
7. Select the **Type of Property to Monitor** from the list.

Note: The following image is a screen capture from an Orion Network Performance Monitor installation. Other modules will look similar, but different objects may be present.



Type of Property to Monitor: Node

8. ***If you select* Custom SQL Alert,** complete the following steps:

a. Select the object on which you want to alert in the **Set up your Trigger Query** field.

b. Provide your custom SQL in the field below the object selection query.

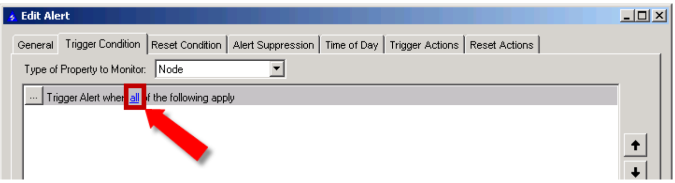
c. ***If you want to delay the trigger of this alert,*** provide the value and unit of your desired alert trigger delay.

d. ***If you want to confirm your provided SQL,*** click **Validate SQL**.

9. ***If you select a type of monitored object,*** complete the following steps:

a. Generate trigger conditions in the text field by selecting appropriate descriptors from the linked context menus and by clicking **Browse** (**…**) on the left of the text field.

b. Click the linked text to select the number of conditions that you want to apply (**all**, **any**, **none**, **not all**). For more information about linked text conditions, see “Understanding Condition Groups” on page 290.

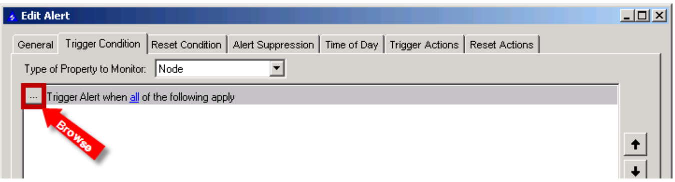


Type of Property to Monitor: Node

Trigger Alert when all of the following apply

c. Click **Browse** (**…**) to view the following condition options:

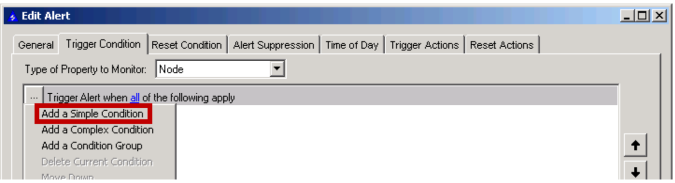
Note: The **has changed** condition is only valid for the **Last Boot**, **IOS Version**, and **IOS Image Family** device characteristics.



Type of Property to Monitor: Node

Trigger Alert when all of the following apply

- ○ To generate a condition based on a comparison of device states, click **Add a Simple Condition**.



Type of Property to Monitor: Node

Trigger Alert when all of the following apply

- ○ To generate a condition based on a comparison of device fields and values, click **Add a Complex Condition**.
- ○ To define more conditions, click **Add a Condition Group**.
- ○ To remove a selected condition, click **Delete Current Condition**.
- ○ To change the order of your conditions, click **Move Down** or **Move Up**, as appropriate.

d. ***If you need an additional condition,*** click **Browse** (**…**), and then click **Add** *ConditionType*, as appropriate for the condition you want to add.

e. ***If you need to delete a condition,*** click **Browse** (**…**), next to the condition you want to delete, and then click **Delete Current Condition.**

Notes:

- Conditions may be exported for use with other alerts by clicking **Export Conditions** and saving as appropriate.
- Click **Import Conditions** to import existing conditions from other alerts. Imported trigger conditions automatically overwrite any existing trigger conditions.

f. ***If you want to specify a time duration for the condition to be valid,*** type the interval and select Seconds, Minutes, or Hours from the list.

Note: You may need to delay alert trigger actions until a condition has been sustained for a certain amount of time. For example, an alert based on CPU load would not trigger unless the CPU Load of a node has been over 80% for more than 10 minutes. To set up a sustained-state trigger condition, at the bottom of the Trigger Condition tab, provide an appropriate amount of time the alert engine should wait before any actions are performed. By default, the alert triggers immediately, if the trigger condition exists. The maximum alert action delay is eight hours after the trigger condition is met.

g. ***If you are finished configuring your advanced alert,*** click **OK**.

Setting a Reset Condition for an Advanced Alert

Set specific conditions for resetting an advanced alert using the following steps.

To set the conditions for resetting an advanced alert:

1. Click **Start > SolarWinds > Alerting, Reporting, and Mapping > Advanced Alert Manager.**

2. Click **View > Configure Alerts**, and then click **New** or select an alert from the list and click **Copy** or **Edit**.

3. Click **Reset Condition**.

4. ***If you want a simple alert reset when trigger conditions no longer exist,*** select **Reset when trigger conditions are no longer true**.

5. ***If you want a conditional alert reset,*** select **Reset this alert when the following conditions are met**.

Notes: Generate reset conditions in the text field by selecting appropriate descriptors from the linked context menus and by clicking **Browse** (**…**).

6. ***If you want to copy the condition used on the Trigger Condition tab,*** click **Copy From Trigger**.
7. Click the linked text to select the number of conditions to apply. For more information, see “Understanding Condition Groups” on page 290.
8. Click **Browse** (**…**) to view the following condition options:
    - To generate a condition based on a comparison of device states, click **Add a Simple Condition**.
    - To generate a condition based on a comparison of device fields and values, click **Add a Complex Condition**.
    - To further define condition application, click **Add a Condition Group**.
    - To remove a selected condition, click **Delete Current Condition.**
    - To change the order of your conditions, click **Move Down** or **Move Up**.
9. ***If you need an additional condition,*** click **Add**, and then select the type of condition you want to add.
10. ***If you need to delete a condition,*** select the condition from the condition list, and then click **Delete**.

Notes:

- Conditions may be exported for use with other alerts by clicking **Export Conditions** and saving as appropriate.
- Conditions from other alerts may be imported to the current alert by clicking **Import Conditions**.
- **Warning:** Imported trigger conditions automatically overwrite any existing trigger conditions.
- Because there are many situations where the reset conditions are the opposite of, or are very similar to, the trigger conditions, SolarWinds has provided a function that copies the trigger conditions to the reset conditions. Click **Copy From Trigger** to add the trigger condition.

11. ***If you want to specify a time duration for the condition to be valid,*** type the time interval and select Seconds, Minutes, or Hours from the list.

Note: It is often appropriate to delay alert reset actions until a condition has been sustained for a certain amount of time. For example, an alert based on node status would not reset until the node has been up for more than five minutes. To establish a sustained-state reset condition, provide an appropriate interval at the bottom of the Reset Condition tab for the amount of time that the alert engine should wait before any actions are performed. The default setting is to reset the alert immediately, once the reset condition exists. The maximum interval between when the trigger condition first exists and when the corresponding alert action is performed is eight hours.

12. ***If you are finished configuring your advanced alert,*** click **OK**.

Setting a Suppression for an Advanced Alert

You can set the specific conditions for suppressing an advanced alert using the following procedure.

Notes:

6. Alert Suppression is only available if you have checked **Show Advanced Features** in the lower left of the Edit Advanced Alert window.
7. In many cases, because suppression conditions are checked against all monitored objects on your network, properly defining alert trigger conditions may eliminate the need for alert suppression. For more information about defining alert trigger conditions, see “Setting a Trigger Condition for an Advanced Alert” on page 282 and “Understanding Condition Groups” on page 290.

To set conditions for advanced alert suppression:

1. Click **Start > All Programs > SolarWinds > Alerting, Reporting, and Mapping > Advanced Alert Manager.**
2. Click **View > Configure Alerts**.
3. Click **New** or select an alert from the list.
4. Click **Copy** or **Edit**, as appropriate.
5. Click **Alert Suppression**.

Note: Generate suppression conditions in the text field by selecting appropriate descriptors from the linked context menus and by clicking **Browse** (**…**) on the left of the text field.

6. ***If you want to copy the condition used on the Trigger Condition tab,*** click **Copy From Trigger**.

7. Click the linked text to select the number of conditions that you want to apply (**all**, **any**, **none**, **not all**). For more information about linked text conditions, see “Understanding Condition Groups” on page 290.
8. Click **Browse** (**…**) to view the following condition options:
    - To generate a condition based on a comparison of device states, click **Add a Simple Condition**.
    - To generate a condition based on a comparison of device fields and values, click **Add a Complex Condition**.
    - To further define the application of your conditions, click **Add a Condition Group**.
    - To remove a selected condition, click **Delete Current Condition**.
    - To change the order of your conditions, click **Move Down** or **Move Up**.
9. ***If you need an additional condition,*** click **Add** and then select the type of condition you want to add.
10. ***If you need to delete a condition,*** select the condition from the condition list, and then click **Delete**.

Note: Conditions may be exported for use with other alerts by clicking **Export Conditions** and saving as appropriate. Conditions from other alerts may be imported to the current alert by clicking **Import Conditions**.

Warning: Imported conditions automatically overwrite existing conditions.

11. ***If you are finished configuring your advanced alert,*** click **OK**.

Setting the Monitoring Period for an Advanced Alert

You can select the specific time periods and days that your advanced alert will monitor your network objects with the following procedure.

To set the monitoring time period and days for an advanced alert:

1. Click **Start > All Programs > SolarWinds > Alerting, Reporting, and Mapping > Advanced Alert Manager.**
2. Click **View > Configure Alerts**.
3. Click **New** or select an alert from the list.
4. Click **Copy** or **Edit**.
5. Click **Time of Day**.
6. Enter the time period over which you want to monitor your network.

Note: Alerts only trigger if the trigger condition is met within this time period.

7. Select the days on which you want to monitor your network.

Note: Alerts will only trigger if your trigger condition is met on the days selected.

8. ***If you are finished configuring your advanced alert,*** click **OK**.

Setting a Trigger Action for an Advanced Alert

Select actions that will occur when your advanced alert is triggered as follows.

To set a trigger action for an advanced alert:

1. Click **Start > SolarWinds > Alerting, Reporting, and Mapping > Advanced Alert Manager.**
2. Click **View > Configure Alerts**.
3. Click **New** or select an alert from the list, and then click **Copy** or **Edit**, as appropriate.
4. Click **Trigger Actions**.
5. ***If you are adding a new advanced alert action,*** click **Add New Action**, and then select the actions you want to occur when the alert triggers.
6. ***If you are editing an existing advanced alert action,*** select the existing alert action, and then click **Edit Selected Action**.
7. Follow the instructions to configure each action.

Note: Depending on the type of action selected, different options will be displayed to configure the alert action. For more information about individual alert actions, see “Available Advanced Alert Actions” on page 391.

8. ***If you need to delete an action,*** select the action and then click **Delete Selected Action**.
9. ***If you are finished configuring your advanced alert,*** click **OK**.

Setting a Reset Action for an Advanced Alert

Select actions that will occur when your advanced alert is reset with the following procedure.

To set a reset action for an advanced alert:

1. Click **Start > SolarWinds > Alerting, Reporting, and Mapping > Advanced Alert Manager.**
2. Click **View > Configure Alerts**.
3. Click **New Alert**, **Copy Alert**, or **Edit Alert**, as appropriate.
4. Click **Reset Actions**.

5. ***If you are adding a new advanced alert action,*** click **Add New Action**, and then select the actions you want to occur when the alert triggers.
6. ***If you are editing an existing advanced alert action,*** select the existing alert action, and then click **Edit Selected Action**.
7. Follow the instructions to configure each action.

Note: Depending on the type of action selected, different options display configuring the alert action. For more information about individual alert actions, see “Available Advanced Alert Actions” on page 391.

8. ***If you need to delete a selected action,*** click **Delete Selected Action**.
9. ***If you are finished configuring your advanced alert,*** click **OK**.

Alert Escalation

When editing any trigger or reset action, use the Alert Escalation tab, if it is available, to define additional alert action options. Depending on the alert action being configured, any or all fo the following options may be available on the Alert Escalation tab:

8. To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
9. To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
10. To delay the execution of the alert action, check **Delay the execution of this Action** and then provide an appropriate interval that the alert engine should wait after the alert condition is met before the alert action is executed.

For more information, see “Escalated Advanced Alerts” on page 312.

Understanding Condition Groups

A condition group is a set of user-defined rules governing alert triggers and resets. By default, the condition group `Trigger Alert when all of the following apply` is added when new alert triggers or reset conditions are created. Four different logical descriptors are used to create conditions: `all`, `any`, `none`, and `not all`, and clicking the word `all` and enables you to select different values. The following sections describe these logical descriptors.

All Condition Group

`Trigger Alert when` *`all`* `of the following apply` means that every condition in the group must be true before the alert is triggered.

In the following example, there are three conditions within the condition group:

11. Node Status is equal to Up
12. Percent Loss is greater than or equal to 75
13. CPU Load is greater than or equal to 85

This alert will not trigger unless the Node is Up, packet loss is greater than or equal to 75%, and CPU load is greater than or equal to 85%.

When setting the condition group to *`all`*, picture every condition as being separated by an *`and`* statement. So, in this example, the alert trigger would read:

```
Alert when: (Node Status = Up) and (Percent Loss >= 75) and (CPU
Load >= 85)
```

Any Condition Group

Changing the condition group to `Trigger Alert when` *`any`* `of the following apply` changes the logic to *`or`* statements. In this example, changing the condition group to *`any`* would change the alert trigger to:

```
Alert when: (Node Status = Up) or (Percent Loss >= 75) or (CPU
Load >= 85)
```

In this situation, if **any** of the three conditions become true, the alert will trigger.

None Condition Group

Changing the condition group to `Trigger Alert when` *`none`* `of the following apply` means that all conditions in the group must be false before the alert is triggered.

In this example the alert trigger would read:

```
Alert when: (Node Status = Down) and (Percent Loss <= 75) and
(CPU Load <= 85)
```

Each condition is separated by an *`and`* statement just like the *`all`* condition group; however, the conditions have been inverted (`Node Status = Down` instead of `Node Status = Up`).

Not All Condition Group

Changing the condition group to `Trigger Alert when` *`not all`* `of the following apply` means that any condition in the group must be false before the alert is triggered. So, in this example the alert trigger would read:

```
Alert when: (Node Status = Down) or (Percent Loss <= 75) or (CPU
Load <= 85)
```

Each condition is separated by an *`or`* statement just like the *`any`* condition group; however, the conditions have been inverted (`Node Status = Down` instead of `Node Status = Up`).

Using the Advanced Alert Manager

The Advanced Alert Manager is an interface used to view network events and alerts. You can also use Advanced Alert Manager to create and manage advanced alerts. The following procedures introduce the main features of the Advanced Alert Manager showing how to configure and view advanced alerts.

Current Events Window

The Current Events window of the Advanced Alert Manager shows the most recent network events with their descriptions and other information from the events log.

To use the Current Events window to view network events:

1. Click **Start > All Programs > SolarWinds > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Current Events**.
3. Select one of the following **Group By** criteria for grouping events: **Event Type**, **Object Type**, **Network Node**, **Acknowledged**, or **No Grouping**.
4. ***If you want to change the viewable category columns in the Current Events window,*** click **Include**, and then complete the following procedure:

   a. Click the Event View Columns tab, and then select column IDs from the **All Columns** field.

   b. Click the right arrow to move your column IDs into the **Selected Columns** field.

   c. ***If there are any column IDs in the* Selected Columns *field that you do not want to view,*** select them, and then click the left arrow to move your selected column IDs to the **All Columns** field.

   d. Click the up or down arrows to change the order of your selected columns accordingly.

   e. Position the slider to set the Event View refresh rate.

   f. Type the number of events that you want to be able to review in the **Display a maximum of** xx **events in the Event View** field.

   g. ***If you are finished configuring your Current Events View,*** click **OK**.
5. Click **Refresh** to update the Current Events window with the latest events and column IDs.
6. ***If you want to acknowledge a network event,*** click **X** next to the event.

Active Alerts Window

The Active Alerts window of the Advanced Alert Manager shows network alerts with their descriptions and other information from the alerts log.

To use the Active Alerts window to view active network alerts:

1. Click **Start > All Programs > SolarWinds > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Active Alerts**.
3. Select one of the **Group By** criteria for grouping alerts: **Alert Name**, **Object Type**, **Object Name**, **Alert State**, **Acknowledged**, **Acknowledged By**, or **No Grouping**.
4. Click **Include**, and then check the types of alerts that you want to view: **Acknowledged**, **Trigger Pending**, **Triggered**, or **Reset Pending**.
5. ***If you want to change the viewable category columns in the Current Events window,*** click **Include > Select Alert Columns**, and then complete the following procedure:

   a. Select column IDs from the **All Columns** field.

   b. Click the right arrow to move your column IDs into the **Selected Columns** field.

   c. ***If there are any column IDs in the* Selected Columns *field that you do not want to view,*** select them, and then click the left arrow to move your selected column IDs to the **All Columns** field.

   d. Click the up or down arrows to change the order of your selected columns accordingly.

   e. Position the slider to set the Alert View refresh rate.

   f. ***If you are finished configuring your Active Alerts View,*** click **OK**.
6. Click **Refresh** to update the Active Alerts window with the latest alerts and column IDs.
7. Click **Configure Alerts** to change the settings for individual alerts.
8. ***If you want to acknowledge an active alert,*** check the alert in the **Acknowledged** column.

Note: As soon as the alert is acknowledged, the user information and date/time is recorded in the database.

Alert Viewer Settings

Alert views in the Orion Advanced Alert Manager are configured in the Alert Viewer Settings window, as presented in the following procedure.

To configure alert views in the Advanced Alert Manager:

1. Click **Start > All Programs > SolarWinds > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **File > Settings**.

Note: The Configure Alerts tab of the Alert Viewer Settings window displays all available network alerts, and from this window you can create, copy, edit, and delete alerts. For more information, see “Creating and Configuring Advanced Alerts” on page 279.

3. Click **Alert View Columns**.
4. Select the information titles that you want to see about your alerts from the **All Columns** list.
5. Click the right arrow to transfer them to the **Selected Columns** list.

Note: The Selected Columns list provides a list of all the information that the Alert Viewer will show for each active alert.

6. ***If you want to remove titles from the Selected Columns list,*** select titles that you want to remove from the active view in the **Selected Columns** list, and then click the left arrow.
7. ***If you want to rearrange the order in which the different pieces of alert information are presented in the Alert Viewer,*** select titles from the **Selected Columns** list and use the up and down arrows to arrange the titles accordingly.
8. Position the slider at the bottom of the tab to set the Alert View refresh rate.
9. Click **Event View Columns**.
10. Select the information titles that you want to see about events from the **All Columns** list.
11. Click the right arrow to transfer them to the **Selected Columns** list.

Note: The Selected Columns list provides a list of all the information that the Alert Viewer will show for each recorded event.

12. ***If you want to remove titles from the Selected Columns list,*** select titles that you want to remove from the active view in the **Selected Columns** list, and then click the left arrow.
13. ***If you want to rearrange the order in which the different pieces of event information are presented in the Alert Viewer,*** select titles from the **Selected Columns** list and use the up and down arrows to arrange the titles accordingly.
14. Position the slider at the bottom of the tab to set the Event View refresh rate.
15. Enter the number of events that you want to see in the Event View.

Adding Alert Actions

Orion Network Performance Monitor provides a variety of actions to signal an alert condition on your network. These alert actions are available for both basic and advanced alerts, and the following procedure assigns actions to the alert conditions that you have defined for your network.

To add an alert action:

1. Click **Start > All Programs > SolarWinds > Network Performance monitor > System Manager**.
2. Click **Alerts > Active Alerts**, and then click either **Configure Basic Alerts** or **Configure Advanced Alerts**, as appropriate.
3. Check the alert to which you want to add the action, and then click **Edit Alert**.
4. Click **Actions**, and then select the action you want to edit.
5. Click **Add Alert Action**, and then click the action to add to your chosen alert.

For more information about individual alert actions, see "Available Advanced Alert Actions" on page 391.

Available Advanced Alert Actions

The following sections detail the configuration of available alert actions:

14. Sending an E-mail / Page
15. Playing a Sound
16. Logging an Advanced Alert to a File
17. Logging an Advanced Alert to the Windows Event Log
18. Logging an Advanced Alert to the NetPerfMon Event Log
19. Sending a Syslog Message
20. Executing an External Program
21. Executing a Visual Basic Script
22. Emailing a Web Page
23. Using Text to Speech Output
24. Sending a Windows Net Message
25. Sending an SNMP Trap
26. Using GET or POST URL Functions

Dial Pag

27. ing or SMS Service

Sending an E-mail / Page

The following procedure configures an e-mail/page action for an advanced alert.

Note: Emails and pages are sent in plain text.

To configure an email/page action for an advanced alert:

1. Click **E-mail/Pager Addresses**, and then
2. Complete the **To**, **CC**, **BCC**, **Name**, and **Reply Address** fields.

   Note: You must provide at least one email address in the **To** field, and multiple addresses must be separated with commas. Some pager systems require a valid reply address to complete the page.

3. Click **Message**.
4. Select the format (**Plain text** or **HTML**) for your alert email.
5. Type the **Subject** and **Message** of your alert trigger email/page.

   Note: Messaging is disabled if both **Subject** and **Message** fields are empty.

6. ***If you want to insert a variable into the Subject or Message field,*** click the location of the new variable, and then complete the following procedure:

   a. Click **Insert Variable**.

   b. Select a **Variable Category**, and then select the variable to add.

   c. ***If you want to change the parser,*** check **Change Parser**, and then select the parser you want to use.

   d. ***If you want to define the SQL variable to copy to the clipboard,*** check **Define SQL Variable**, and then click **Insert Variable From Above List**.

   e. Click **Build Selected Variable**.

7. Click **SMTP Server**.
8. Type the **Hostname or IP Address of your SMTP Server** and the designated **SMTP Port Number**.

   Note: The SMTP server hostname or IP address field is required. You cannot send an email/page alert without identifying the SMTP server.

9. ***If you want to use SSL/TLS encryption for your alert email,*** check **Enable SSL**.

10. ***If your SMTP server requires authentication,*** check **This SMTP Server requires Authentication**.
11. Click **Time of Day**.
12. Enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
13. ***If you want to enable alert escalation,*** click the Alert Escalation tab, and then check any of the following options, as appropriate for your alert:
14. To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
15. To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
16. To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.
17. ***If you are finished configuring your email/page alert action,*** click **OK**.

Playing a Sound

Orion can be configured to play a sound upon alert trigger or reset. The following procedure configures a sound to play for an advanced alert.

Note: Due to restrictions on Windows service applications, the Play a Sound action is not available to SolarWinds installations on either Windows 7 or Windows Server 2008 and higher.

To configure a play sound action for an advanced alert:

1. Click **Play Sound**.
2. Specify a sound file for the alert trigger by doing either of the following in the **Sound file to play** field:
   - Type the complete directory path and file name.
   - Click **Browse** (**…**) to navigate your file system and select the target file.
3. Click the musical note button to the right of either text field to test the sound file you have specified.
4. Click **Time of Day**.
5. Enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

6. ***If you want to enable alert escalation,*** click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:
    - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
    - To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
    - To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.
7. ***If you are finished configuring your play a sound alert action,*** click **OK**.

Logging an Advanced Alert to a File

Orion can be configured to log alerts to a designated file. The following procedure logs an advanced alert to a designated file

To configure an alert log file for an advanced alert:

1. Click **Event Log**, and then specify an alert log file by doing either of the following in the **Alert Log Filename** field:

Note: If the file specified does not exist, it will be created with the first alert occurrence.

Type the complete path and name of the target file.

Click **Browse** (**…**) to navigate your file system and select the target file.

2. Type the message you want to log to your alert log file in the **Message** field.
3. ***If you want to insert a variable into the Message field,*** complete the following procedure:

a. Click **Insert Variable**, and then select a **Variable Category**.

b. Select the variable you want to add.

c. ***If you want to change the parser,*** check **Change Parser**, and then select the parser you want to use.

d. ***If you want to define the SQL variable to copy to the clipboard,*** check **Define SQL Variable**, and then click **Insert Variable From Above List**.

e. Click **Build Selected Variable**.

4. Click **Time of Day**.
5. Enter the time period over which you want to activate your alert action.
6. Select the days on which you want to activate your alert action.

- ***If you want to enable alert escalation,*** click the Alert Escalation tab, and then check any of the following options, as appropriate for your alert:
  - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
  - To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
  - To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.

7. ***If you are finished configuring your alert log file,*** click **OK**.

Logging an Advanced Alert to the Windows Event Log

You may specify that an alert be logged to the Windows Event Log either on the Server or on a remote server. The following procedure logs an advanced alert to the Windows Event Log on a designated server.

To configure advanced alert logging to the Windows Event Log:

1. Click **Windows Event Log**.
2. ***If you want your alert to write to the Windows Event Log on your Server,*** select **Use Event Log Message on Network Performance Monitor Server**.
3. ***If you want your alert to write to the Windows Event Log on a remote server,*** select **Use Event Log Message on a Remote Server**, and then provide the **Remote Server Name or IP Address**.
4. Type the message you want to log to the Windows Event Log in the **Message to send to Windows Event Log** field.

5. ***If you want to insert a variable into the Message field,*** complete the following procedure:

   a. Click **Insert Variable**.

   b. Select a **Variable Category**.

   c. Select the variable you want to add.

   d. ***If you want to change the parser,*** check **Change Parser**, and then select the parser you want to use.

   e. ***If you want to define the SQL variable to copy to the clipboard,*** check **Define SQL Variable**, and then click **Insert Variable From Above List**.

   f. Click **Build Selected Variable**.

6. Click **Time of Day**.
7. Enter the time period and select the days over which you want to activate your alert action.
8. ***If you want to enable alert escalation,*** click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:

- To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
- To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
- To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.

9. ***If you are finished configuring your alert log file,*** click **OK**.

Logging an Advanced Alert to the NetPerfMon Event Log

You may specify that an alert be logged to the NetPerfMon Event Log either on the Server or on a remote server. The following procedure logs an advanced alert to the NetPerfMon Event Log on a designated server.

To configure advanced alert logging to the NetPerfMon Event Log:

1. Click **NPM Event Log**.
2. Type the message you want to log to the NetPerfMon Event Log in the **Message to send to Network Performance Monitor Event Log** field.

3. ***If you want to insert a variable into the Message field,*** complete the following procedure:

   a. Click **Insert Variable**.

   b. Select a **Variable Category**.

   c. Select the variable you want to add.

   d. ***If you want to change the parser,*** check **Change Parser**, and then select the parser you want to use.

   e. ***If you want to define the SQL variable to copy to the clipboard,*** check **Define SQL Variable**, and then click **Insert Variable From Above List**.

   f. Click **Build Selected Variable**.

4. Click **Time of Day**.

5. Enter the time period and select the days over which you want to activate your alert action.

6. ***If you want to enable alert escalation,*** click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:

   - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.

   - To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.

   - To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.

7. ***If you are finished configuring your alert log file,*** click **OK**.

Sending a Syslog Message

Orion can log received alerts to the Syslog of a designated machine. The following procedure configures an advanced alert to send a message to a designated Syslog server.

To configure an advanced alert to send a Syslog message:

1. Click **Syslog Message**.

2. Type the **Hostname or IP Address of the Syslog Server** to which you want to send Syslog messages.

3. Select the **Severity** of your alert Syslog message.

Note: For more information, see “Syslog Severities”.

4. Select **Facility** of your alert Syslog message.

Note: For more information, see “Syslog Facilities”.

5. Type the **Syslog Message** you want to send.
6. ***If you want to insert a variable into the Message field,*** complete the following procedure:
   - **a.** Click **Insert Variable**.
   - **b.** Select a **Variable Category**.
   - **c.** Select the variable you want to add.
   - **d.** ***If you want to change the parser,*** check **Change Parser**, and then select the parser you want to use.
   - **e.** ***If you want to define the SQL variable to copy to the clipboard,*** check **Define SQL Variable**, and then click **Insert Variable From Above List**.
   - **f.** Click **Build Selected Variable**.
7. Click **Time of Day**.
8. Enter the time period over which you want to activate your alert action.
9. Select the days on which you want to activate your alert action.
10. ***If you want to enable alert escalation,*** click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:
    - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
    - To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
    - To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.
11. ***If you are finished with the configuration of your send Syslog message action,*** click **OK**.

Executing an External Program

There are several circumstances where you may want to execute a program when a specific network event occurs. Use the Edit Execute Program Action window to specify the executable that should be started when the specified alert is triggered or reset, as shown in the following procedure.

Note: External programs selected for this action must be executable using a batch file called from the command line.

To configure an advanced alert to execute an external program:

1. Click **Execute Program**.
2. Specify the batch file to execute, either by typing the complete path and name of the target file into the **Program to execute** field or by clicking **Browse** (**…**), to browse your folder structure and select the target executable.
3. Click **Time of Day**, and then enter the time period when you want to execute the external program.
4. Select the days on which you want to execute the external program.
5. Click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:
    - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
    - To execute the action repeatedly, while the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered**, and then provide an action execution interval.
    - To delay alert action execution, check **Delay the execution of this Action**, and then provide the interval the alert engine should wait.
6. ***If you are finished configuring your external program execution action,*** click **OK**.

Executing a Visual Basic Script

In some situations you may want to execute a Visual Basic (VB) script when a network event occurs. The Edit Execute VB Script Action window is used to specify the name and complete path of the file that shall be executed when the specified alert is triggered or reset.

To configure alerts to execute a Visual Basic (VB) script:

1. Click **VB Script**.

2. Select an available **VB Script Interpreter**.
3. Specify a VB script to execute either by typing the complete path and name of the VB script into the **VB Script to execute** field or by clicking **Browse (…)** to browse your folder structure and select the script.
4. Click **Time of Day**, and then enter the time period and select the days on which you want to execute the selected VB script.
5. Click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:
   - To disable the script when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
   - To execute the script repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
   - To delay script execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the script executes.
6. ***If you are finished configuring your VB script execution action,*** click **OK**.

Emailing a Web Page

The Edit E-mail Web Page Action window includes several tabs for configuration. The following procedure configures an e-mail URL action for an advanced alert.

Note: Emails are sent in plain text.

To configure an email web page action for an advanced alert:

1. Click **E-mail a Web Page**, and then then click **OK**.
2. Complete the **To**, **CC**, **BCC**, **Name**, and **Reply Address** fields.

   Note: You must provide at least one address in the **To** field. When entering multiple addresses, you may only separate addresses with a comma. Some pager systems require a valid reply address to complete the page.
3. Click **SMTP Server**.
4. Type the **Hostname or IP Address of your SMTP Server** and the designated **SMTP Port Number**.

   Note: The SMTP server hostname or IP address field is required. You cannot email a web page without identifying the SMTP server.

5. Click **URL**, and then type the **Subject** of your alert email.

Note: Messaging is disabled if both **Subject** and **URL** fields are empty.

6. ***If you want to insert a variable into the Subject field,*** click the location of the new variable, and then complete the following procedure:

   a. Click **Insert Variable**, select a **Variable Category**, and then select the variable to add.

   b. ***If you want to change the parser,*** check **Change Parser**, and then select the parser you want to use.

   c. ***If you want to define the SQL variable to copy to the clipboard,*** check **Define SQL Variable**, and then click **Insert Variable From Above List**.

   d. Click **Build Selected Variable**.

7. Provide the **URL** of your alert email.

Note: Messaging is disabled if both **Subject** and **URL** fields are empty.

8. ***If the web server of the URL you want to email requires user access authentication,*** provide both the **Web Server UserID** and the **Web Server Password** in the Optional Web Server Authentication area.

9. Click **Time of Day**, and then enter the time period and select the days when you want to activate your alert action.

10. ***If you want to enable alert escalation,*** click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:

   - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
   - To execute the action repeatedly, as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
   - To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval for the alert engine to wait after the alert condition is met before executing the alert action.

11. ***If you are finished configuring your URL email alert action,*** click **OK**.

Using Text to Speech Output

You may specify a phrase that will be spoken upon alert trigger and a separate phrase for the alert reset. Orion Platform Microsoft Speech Synthesis Engine version 5.0, as included with Windows 2003 and XP Professional. If you have Orion 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 advanced alert trigger or reset.

Note: Due to restrictions on Windows service applications, the Text to Speech action is not available to SolarWinds installations on either Windows 7 or Windows Server 2008 and higher.

To configure a text-to-speech output action for an advanced alert:

1. Click **Text to Speech output**, and then then click **OK**.
2. On the General tab, Select a Speech Engine, and then use the sliders to set the required **Speed**, **Pitch** and **Volume**.
3. On the Phrase tab, type the text you want to output as speech in the **Phrase to speak** field.

Note: Click **Speak** to hear the text, as provided, with the options configured as set on the General tab.

4. On the Time of Day tab enter the time period and select the days on which you want to activate your alert action.
5. ***If you want to enable alert escalation,*** open the Alert Escalation tab, and then check any of the following options, as appropriate for your alert:
   - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
   - To execute the action repeatedly, as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
   - To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval for the alert engine to wait after the alert condition is met before executing the alert action.
6. ***If you are finished configuring your text-to-speech alert action,*** click **OK**.

Sending a Windows Net Message

Alerts can be configured to display a pop-up Windows Net Message either on a specific computer or on all computers in a selected domain or workgroup. The following steps configure Windows Net messaging for triggered or reset alerts.

Note: The only operating systems supporting Windows Net Messaging on which SolarWinds supports SolarWinds installations are Windows Server 2003 and Windows XP. SolarWinds only supports evaluation installations of Orion on Windows XP.

To configure Orion to send a Windows Net message upon alert:

1. Click **Send a Windows Net Message**, and then then click **OK**.
2. On the Net Message tab, enter the **Computer Name or IP Address** of the machine where you want to send a Windows Net message upon an alert trigger or reset.
3. ***If you want to send the message to all computers in the domain or workgroup of your target computer,*** check **Send to all Computers in the Domain or Workgroup**.
4. Enter the Windows Net message you want to send in the **Message to send** field.
5. On the Time of Day tab enter the time period and select the days on which you want to activate your alert action.
6. ***If you want to enable alert escalation,*** open the Alert Escalation tab, and then check any of the following options, as appropriate for your alert:
    - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
    - To execute the action repeatedly, as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
    - To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval for the alert engine to wait after the alert condition is met before executing the alert action.
7. ***If you are finished configuring your text-to-speech alert action,*** click **OK**.

Sending an SNMP Trap

The following steps configure an alert to send an SNMP trap on trigger or reset.

To configure Orion to send an SNMP trap upon alert:

1. Click **Send an SNMP Trap**, and then then click **OK**.
2. On the SNMP Trap tab, in the **SNMP Trap Destinations** field, enter the IP addresses of the servers to which you want to send your generated SNMP traps.

Note: Use commas to separate multiple destination IP addresses.

3. Select the type of trap to send on alert trigger from the **Trap Template** list.

Note: Some trap templates may use an alert message. You may change any provided text, if you want, but it is important that you understand the use of variables beforehand.

4. Enter the **SNMP Community String** for your network in the designated field.
5. On the Time of Day tab enter the time period and select the days on which you want to activate your alert action.
6. ***If you want to enable alert escalation,*** open the Alert Escalation tab, and then check any of the following options, as appropriate for your alert:
   - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
   - To execute the action repeatedly, as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
   - To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval for the alert engine to wait after the alert condition is met before executing the alert action.
7. ***If you are finished configuring your SNMP trap alert action,*** click **OK**.

Using GET or POST URL Functions

Orion can be configured to communicate alerts using HTTP GET or POST functions. As an example, a URL may be used as an interface into a trouble ticket system, and, by correctly formatting the GET function, new trouble tickets may be created automatically. The following procedure configures Orion to use GET or POST HTTP functions to communicate alert information.

To configure Orion to use GET or POST URL functions with alerts:

1. Click **Get or Post a URL to a Web Server**, and then then click **OK**.
2. Select either **Use HTTP GET** or **Use HTTP POST** to set the function that you want to use to communicate alert information.
3. ***If you selected Use HTTP GET,*** enter the **URL** you want to GET.
4. ***If you selected Use HTTP POST,*** enter the **URL** you want to POST, and then enter the **Body to POST**.
5. On the Time of Day tab enter the time period and select the days on which you want to activate your alert action.
6. ***If you want to enable alert escalation,*** open the Alert Escalation tab, and then check any of the following options, as appropriate for your alert:
    - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
    - To execute the action repeatedly, as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
    - To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval for the alert engine to wait after the alert condition is met before executing the alert action.
7. ***If you are finished with the configuration of Orion to use HTTP GET or POST URL functions,*** click **OK**.

Dial Pag

ing or SMS Service

If NotePager Pro is installed Orion can be configured to communicate alerts using paging and SMS services. For more information about installation and configuration, see “SolarWinds Network Performance Monitor Integration” at www.notepage.net.

Testing Alert Actions

The Advanced Alert Manager provides an alert action test feature so you can confirm the desired function for actions you have configured to fire when Orion detects an alert condition on your network. Complete he following procedure to test an alert action.

To test an alert action:

1. Click **Start > All Programs > SolarWinds > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **Configure Alerts**.
3. Click the alert for which the action you want to test is configured.
4. Click **Test**.
5. ***If the alert is configured to fire on a node condition,*** select **Alert on Network Node**, and then select the node against which you want to test the action.
6. ***If the alert is configured to fire on an interface condition,*** complete the following steps:

Note: Testing alert actions against interfaces is only available if Orion Network Performance Monitor is installed and monitoring interfaces on your network. For more information, see the *SolarWinds Network Performance Monitor Administrator Guide*.

   a. Select **Alert on Network Node**, and then select the parent node of the interface against which you want to test the action.

   b. Select **Select Interface on** *ParentNode*, and then select the interface against which you want to test the action.

7. ***If the alert is configured to fire on a volume condition,*** complete the following steps:

   a. Select **Alert on Network Node**, and then select the parent node of the volume against which you want to test the action.

   b. Select **Select Volume on** *ParentNode*, and then select the volume against which you want to test the action.

8. ***If you are testing an alert trigger action,*** click **Test Alert Trigger**.
9. ***If you are testing an alert reset action,*** click **Test Alert Reset**.
10. When the test completes, as indicated by the test log, click **Done**.

    Confirm that the expected action occurred as a result of the selected alert trigger or reset.

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 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.

Acknowledging Advanced Alerts in the Web Console

SolarWinds UDT allows you to acknowledge advanced alerts in the Orion Web Console, allowing you to eliminate time lost either when multiple users attempt to resolve the same issue or when a user tries to address an issue that has already been resolved.

To acknowledge advanced alerts using the Orion Web Console:

1. Log in to the Orion Web Console using an account that has been granted alert acknowledgement privileges.

Note: For more information about access privileges for Orion Web Console users, see “User Account Access Settings” on page 71.

2. Click **Alerts** on the Views toolbar.
3. ***If you want to limit the list of alerts to only those dealing with a single device,*** select the specific device from the **Network Object** list.

Note: This option is only available if alerts fire on multiple network devices.

4. ***If you want to limit the list of alerts to only those dealing with a single type of device,*** select the device type from the **Type of Device** list.

Note: This option is only available if Orion is monitoring multiple types of network devices.

5. ***If you want to limit the list of alerts to only those of a single type,*** select the specific alert type from the **Alert Name** list.

Note: This option is only available when multiple types of SolarWinds UDT alerts have been triggered.

6. Confirm the number of alerts displayed in the **Show Alerts** field.

7. ***If you want acknowledged alerts to remain in the Alerts view, even after they have been acknowledged,*** check **Show Acknowledged Alerts**.
8. Click **Refresh** to update the alerts list with your new settings.
9. Check **Acknowledged** next to the alerts you want to acknowledge.
10. Click **Acknowledge Alerts**.

Escalated Advanced Alerts

By creating an escalated alert, SolarWinds UDT enables you to customize a series of alerts to trigger successive actions as an alert condition persists. The following sections provide both a scenario where an escalated alert may be useful and the steps required to create one using the Orion Advanced Alert Manager.

Escalated Alert Example

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 SolarWinds UDT recognizes an alert condition, SolarWinds UDT generates both an email and a page that are sent to one of the two technicians. An entry is also recorded in the Orion events log.
2. If the alert is not acknowledged in the Orion Web Console within 20 minutes, a second alert is fired, generating another email and another page, both sent to both technicians. An entry is also recorded in the Orion events log.
3. If the second alert is not acknowledged within 20 minutes, SolarWinds UDT 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.

Creating a Series of Escalated Alerts

The following procedure creates a series of escalated alerts similar to the scheme described in the preceding example.

Note: Repeat these steps to create a separate alert for each notification level. The example provided in the previous section uses a three-level escalated alert, The following procedure should be completed three times, once for each alert, to replicate the escalated alert of the previous section.

To create an escalated alert:

1. Click **Start > All Programs > SolarWinds > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **Configure Alerts**.
3. Click **New**, and then click **General.**
4. Type `Level` *`X`* , where *`X`* is the level corresponding to the currently configured alert, as the name of your escalated alert in the **Name of Alert** field.

Note: The example provided in the previous section uses a three-level escalated alert.

5. Type a description of your first level escalated alert in the description field, and then check **Enable this Alert**.
6. Type the Alert Evaluation Frequency and select Seconds, Minutes, or Hours from the list to set the checking interval for your alert.
7. Click **Trigger Condition.**

Note: For more information about configuring trigger conditions, see “Setting a Trigger Condition for an Advanced Alert” on page 282.

8. Select **Node** as the Type of Property to Monitor.
9. Confirm that the linked text in the alert definition field displays **all**.

Note: Click the linked text to select the number of conditions that you want to apply (**all**, **any**, **none**, **not all**). For more information about linked text conditions, see “Understanding Condition Groups” on page 290.

10. Click **Browse** (**…**), and then click **Add a Simple Condition**.
11. Click the first asterisk (*****), and then select **Network Nodes > Node Details > Node Name**.
12. Confirm that **is equal to** is the linked condition text in the trigger definition.

Note: Click the linked text to select the condition you want to apply (**equal**, **greater**, **less**, **…**). For more information about linked text conditions, see “Understanding Condition Groups” on page 290.

13. Click the second asterisk (*****), and then select your production web server from the list of monitored nodes.
14. Click **Add**, and then click **Simple Condition**.
15. Click the first asterisk (*****) in the second condition, and then select **Network Nodes > Node Status > Node Status**.
16. Confirm that **is equal to** is the linked condition text in the second trigger definition.

Note: Click the linked text condition to select the condition you want to apply (**equal**, **greater**, **less**, **…**). For more information about linked text conditions, see “Understanding Condition Groups” on page 290.

17. Click the second asterisk (*****) in the second condition, and then select **Down**.
18. ***If you want to apply any reset conditions to your escalated alert,*** click **Reset Condition**, and then provide appropriate conditions. For more information, see “Setting a Reset Condition for an Advanced Alert” on page 285.
19. ***If you want to apply any alert suppressions to your escalated alert,*** click **Alert Suppression**, and then provide appropriate suppression conditions. For more information, see “Setting a Suppression for an Advanced Alert” on page 287.
20. ***If you want to restrict when your escalated alert is valid,*** click **Time of Day**, designate the Valid Time of Day for your escalated alert, and then select the Days of the Week on which your escalated alert is valid. For more information, see “Setting the Monitoring Period for an Advanced Alert” on page 288.

Note: By default, your escalated alert is always valid.

21. Click **Trigger Actions**, and then click **Add New Action**.
22. Select **Send an E-mail / Page**, and then click **OK**.
23. Click **E-mail/Pager Addresses**, and then complete the **To**, **CC**, **BCC**, **Name**, and **Reply Address** fields for your Level 1 contact.

Note: You must provide at least one email address in the **To** field. When entering multiple addresses in a field, y separate addresses with a comma.

24. Click **Message**, and then type the **Subject** and **Message** of your escalated alert email.

Notes:

- Messaging is disabled if both **Subject** and **Message** fields are empty.
- For more information about variables in email subjects and messages, see “Sending an E-mail / Page” on page 296.

25. Click **SMTP Server**, and then provide the **Hostname or IP Address of your SMTP Server** and the designated **SMTP Port Number**.

Note: The SMTP server hostname or IP address field is required. You cannot send an email/page alert without identifying the SMTP server.

26. ***If your SMTP server requires authentication,*** check **This SMTP Server requires Authentication**.
27. ***If you want to restrict when your escalated alert is valid,*** check **Execute this Action only between specific hours**, and then configure the appropriate settings.

Note: By default, your escalated alert is always valid. For more information, see “Setting the Monitoring Period for an Advanced Alert” on page 288.

28. Click **Alert Escalation**.
29. Check **Do not execute this Action if the Alert has been Acknowledged**.
30. ***If you want to execute the action repeatedly as long as the trigger condition exists,*** check **Execute this Action repeatedly while the Alert is Triggered**, and then provide an appropriate action execution interval.
31. ***If you want to delay alert action execution,*** check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.

Note: Typically, if you are configuring the first level alert, you should leave this option unchecked. If you are configuring the second level alert, check this option and provide the desired delay between the first and second notifications. If you are configuring the third level alert, check this option and provide the desired delay between the first and third notifications.

32. Click **OK**.
33. ***If you want your escalated alert to perform any actions upon reset,*** click the Reset Action tab, and then configure appropriate actions. For more information, see “Setting a Reset Action for an Advanced Alert” on page 289.
34. ***If you are finished configuring your escalated alert,*** click **OK**.

Viewing Alerts from Mobile Devices

SolarWinds UDT 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.

.

Chapter 16

Creating and Managing Reports

The Orion Platform database accumulates a great deal of information that can be presented in a variety of formats using the SolarWinds Report Writer feature. SolarWinds has developed Orion Report Writer to help you quickly and easily extract viewable data from your Orion database.

Because SolarWinds NCM version 7.1.x is integrated with Orion common components, you gain the ability to generate any of the predefined reports packaged with Orion Platform products. For more information, see “Predefined Orion Reports”.

When you have finished editing your reports, you can print them with the click of a button. You can also view most reports in the Orion Web Console by default. For more information, see “Customizing Views”. To schedule automatic email reports for individual users or groups of users, open the Orion Report Scheduler by clicking **Start > All Programs > SolarWinds > Alerting, reporting, and Mapping > Orion Report Scheduler**.

Report Writer capabilities are enhanced when they are used in conjunction with the Custom Property Editor. Once added, properties are available for report sorting and filtering. For more information, see Creating Custom Properties.

NCM-NPM Predefined Reports

Two NCM-generated reports are available when you install NCM and NPM in an integrated implementation. You can modify them or create new reports as necessary.

The following reports are immediately available only if you have NCM integrated with NPM; view them on Network Performance Monitor Reports page, accessible by clicking **Reports** in the Views toolbar. These reports may be modified with Report Writer, as necessary, to suit your network performance reporting requirements. The following reports are predefined for your network devices.

Topology Reports

Discovered Links

Displays switch port mapping details across all switches in the system including wireless access points where this information is available.

Wireless Reports

Wireless Host Mapping

Displays switch port mapping details from wireless access points.

Predefined Orion Reports

The following sections describe the reports that are immediately available with your Orion installation. These reports may be modified, as necessary, to suit your network performance reporting requirements.

Note: If the report you require is not listed in any of the following sections, you can use Orion Report Writer to create your own custom report. For more information about creating your own custom reports, see “Using Report Writer” on page 324.

Availability

The following network availability reports are provided by default with Orion.

Availability – Last Month

Displays the IP address and average availability of all monitored nodes over the last month.

Availability – This Year

Displays the IP address and average availability of all monitored nodes over the last year.

Availability – Yesterday

Displays the IP address and average availability of all monitored nodes over the previous day.

Availability of Entire Network – Last Month

Displays the availability of all monitored nodes on the entire network over the last month.

Top 25 Percent Down – Last Month

Displays the top 25 nodes, by percent downtime, over the last month.

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.

Events

The following network events reports are provided by default with Orion.

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

SolarWinds NCM 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.

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.

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.

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

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.

Inventory

The following network inventory reports are provided by default with Orion.

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.

Viewing Reports

All reports, custom or predefined, are available for viewing in both the Orion Web Console and in Report Writer, as shown in the following procedures:

- Viewing Reports in the Orion Web Console
- Viewing Reports in the Orion Report Writer

Note: By default, no report folder is configured for newly created users. If a new user is not seeing reports, you may need to select a **Report Folder** for the new user. For more information, see “Configuring an Account Report Folder” in the SolarWinds Network Performance Administrator Guide.

Viewing Reports in the Orion Web Console

The following procedure opens reports for viewing in the Orion Web Console.

To view reports in the Orion Web Console:

1. Click Start > All Programs > SolarWinds > Orion Web Console.
2. Log in to the Orion Web Console, and then click Home > Reports.
3. Select a report group name to expand the report group.
4. Click the title of the report you want to view, and it displays directly in the web console browser.

It is also possible to include a report within a web console view as a Report from Orion Report Writer resource. For more information about adding the Report from Orion Report Writer resource, see “Editing Views”.

Viewing Reports in the Report Writer

The following procedure opens reports for viewing in the Report Writer.

To view reports with Report Writer:

1. Click Start > All Programs > SolarWinds > Alerting, Reporting, and Mapping > Report Writer.
2. If report groups are not already expanded in the left pane, click + next to a report group name to expand the group, and then click the title of the report you want to view.
3. Click Preview.

Using Report Writer

Before using Report Writer, you must have collected at least a few minutes worth of data in a database populated with devices you want to monitor. A variety of reports are included with Report Writer, and icons that precede report names distinguish available report types. The following procedure starts Report Writer.

To start Report Writer:

1. Click Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Report Writer.
2. Click File > Settings.
3. In the General tab of the Report Writer Settings window, select either of the following as a default viewing mode:

   Preview displays the report as it will appear in printed form. For more information, see “Preview Mode” on page 325.

   Report Designer is the report creation and editing interface. For more information, see “Design Mode” on page 325.

   Note: You can toggle between Preview and Report Designer modes at any time by clicking Preview or Design, respectively, on the toolbar.
4. If you want to separate the data for individual network objects with horizontal lines, click Report Style, and then select Display horizontal lines between each row.
5. Click OK to exit Report Writer Settings.

Preview Mode

Preview mode shows a report as it will print. When you open a report in Preview mode, or switch to Preview mode from Design mode, Orion runs the query to generate the report, and then Report Writer displays the results.

The Preview window toolbar provides the following actions and information:

- Current page number and total number of pages in the report.
- Page navigation buttons: First Page, Page Up, Page Down, and Last Page
- Zoom views

Note: Double-click a preview to zoom in and double-right-click to zoom out.

- Print report

Design Mode

Use Design mode to create new reports and modify or rename existing reports. The options available for both creating and modifying reports are the same. Design mode options are also dynamic, based upon the type of report, included report data, and report presentation. Available options differ according to the type of report that you are designing, but all reports require that you select the data to include and decide how that data will be sorted, ordered, filtered, and presented.

Creating and Modifying Reports

Use the following procedure to modify or create reports in Report Writer.

To open a report with Report Writer:

1. If you want to modify an existing report, click an existing report from the inventory in the left pane of the main Report Writer window.
2. If you want to create a new report, click File > New Report, select the type of report that you would like to create, and then click OK.

   Each report offers different configuration options, so, depending on the report, some formatting tabs described in the following sections may not be available.

   Notes:

   The SQL query used to generate a report may be viewed in an additional tab. Click Report > Show SQL to add a read-only SQL tab to the Design window.

   A preview of your report is also available at any time. Click Preview to enter Preview Mode, and then click Design to return to Design Mode.

General Options Tab

The General tab opens by default and shows titling and display options.

To configure General options:

1. Specify the Report Group, Report Title, Subtitle, and Description.

   Note: If you use an existing report group name, the new report is added to that existing group in the left pane of the main window.
2. Select the display Orientation of your report.
3. If you are configuring an historical report and you do not want to group data by days, clear Group historical data by days.

   Note: By default, data in some availability and historical reports is grouped by days when displayed in the Orion Web Console. Data grouping by days is not viewable in Report Viewer.
4. If you do not want to make this report available on your Orion Web Console, clear Make this Report available from the Orion website.

   Note: By default, most reports are made available for display in the Orion Web Console.

Select Fields Options Tab

The Select Fields tab allows you to select the data fields in a report.

To select and configure fields:

1. Click Select Fields.
2. If you are creating a new report or adding fields to an existing report, click the ellipsis, select Add a new field, and then dynamically define each new report field as follows:
   a. Click the asterisk after Field:, and then select the type of information to include in the current report field.

   b. If you want to sort the data in the current field, click the sort asterisk and select a sort order.

   c. If you want to perform an operation on the data in the current field, click the function asterisk and select an operation.
3. If you are modifying an existing report, click the Field, sort, or function that you want to change and select a new value as follows.
   a. Click the asterisk after Field:.

   b. Select the type of information to include in the current report field.

   c. If you want to sort the data in the current field, click the sort asterisk and select a sort order.

   d. If you want to perform an operation on the data in the current field, click the function asterisk and select an operation.
4. If you want to test your selections as you assemble your report, click Execute SQL Query to view the current query results.
5. If you want to delete a field or rearrange the order of the fields that are listed in your report, select a field, click Browse (…), and then select the appropriate action.

   Note: Unselected fields are not displayed in your report, but their sort and function configurations are retained.
6. If you want to preview your report, click Preview.

Filter Results Options Tab

The Filter Results tab allows you to generate filter conditions for field data by selecting appropriate descriptors from the linked context menus. Results filters are configured as follows.

To configure results filters:

1. Click Browse (…), and then select from the following options:

   Select Add a new elementary condition to generate a condition that is based on a direct comparison of network object data fields.

   Select Add a new advanced elementary condition to generate a condition based on a comparison of device data fields and values.

   Select Add a new complex condition to define a condition that filters other defined conditions.

   Select Delete current condition to remove a selected condition.

   Select Move current condition forward or Move current condition backward to change the order of your conditions accordingly.

   Note: The lists of available linked descriptors are dynamically generated in consideration of all other variables within the same condition. For more information about condition groups and their application, see "Understanding Condition Groups" on page 290.

2. Select or clear individual filter conditions to enable or disable their application, respectively, to your report.

Top XX Records Options Tab

The Top XX tab allows you to limit the number of records that are shown in your report to either a top *number* or a top *percentage* of all results. Top XX options are configured as shown in the following procedure.

To configure Top XX records:

1. If you want to show all records in your report, select Show All Records.
2. If you want to specify a truncated list of eligible items for your report, complete the following steps:
   a. select either Show only the Top number Records or Show the Top percentage % of Records
   b. Provide appropriate number or percentage values.

Time Frame Options Tab

The Time Frame options tab allows you to limit the scope of your report to a specific period of time. To configure Time Frame options, select a **Named**, **Relative**, or **Specific Time Frame**, and then select or provide required values.

Notes:

- If you receive a SQL Timeout error message, you may edit the timeout setting in the SWNetPerfMon.db file. By default, this file is located in the `C:\Program Files\SolarWinds\Orion` directory
- Since the **Relative Time Frame** is continuously variable, reports run with it may show different results, even if they are run close together in time.

Summarization Options Tab

The Summarization tab allows you to generate summaries of your results over specific periods of time. Summarization options are configured as follows.

To configure results summarization:

1. If you do not want to summarize your results, confirm that Do not Summarize the Results is selected.
2. If you want to summarize your results, complete the following steps:
    a. Select Summarize the Results by Hour, Date, Month, etc, and then select the summarization period.
    b. Specify the location of the summary field for your report.
    c. Select a location for the Summary Date/Time field.

Report Grouping Options Tab

The Report Grouping tab allows you to group results by field descriptor within your report. Add, edit and delete report groups to organize the data in your report. Establish and edit report groups as follows.

To add and edit report groups:

1. If you want to add a new report group, select a field from the list to define your group, and then click Add Report Group to add your selected field to the Report Groups list.

   Note: Use up and down arrows to change the grouping order accordingly.
2. If you want to edit an existing report group, select the field from the Report Groups list, and then click Edit Report Group.
3. The following options may be changed as needed:

   The Group Header is the text that designates groups on your report.

   The Web URL is the dynamic location of your published report with respect to your Orion Web Console.

   Font size, face, color, and background may all be modified by clicking associated ellipses.

Alignment may be left, center, or right.

Select Transparent Background for better results when publishing your report to the Web.

If you want to change the grouping order, use the up and down arrows to change the grouping order accordingly.

Field Formatting Options Tab

The Field Formatting tab allows you to customize the format of the various results fields in your report. To format results fields, select the field you want to format, and then edit labels and select options as appropriate.

Notes:

- The formatting options available for each field may be different according to the nature of the data contained in that field.
- Select **Hidden Field** to hide any field in your report.
- To view your changes at any time, click **Preview**.

Customizing the Report Header and Footer Image

The image that is displayed at the top and bottom of each report can be changed. To add your company logo as the report header and footer, save your logo as `Header.jpg` in the `SolarWinds\Common\WebResources` folder, typically located in `C:\Program Files\`, and then click **Refresh**.

Note: The image must be in JPEG format with a height of 150 pixels or less.

Exporting Reports

Orion Report Writer gives you the ability to present your created reports in any of the following industry-standard formats:

- Comma-delimited (*.csv, *.cdf)
- Text (*.txt)
- HTML (*.htm, *.html)
- MIME HTML, with embedded images (*.mhtml)
- Excel® spreadsheet (*.xls)

Note: You must have Microsoft Excel installed to use the Export to Excel Spreadsheet option. SolarWinds NCM does not currently support Microsoft Office 2010 software package.

- Adobe® PDF (*.pdf)
- Image (*.gif)

The following procedure presents the steps required to export an open report from Orion Report Writer into any of the previously listed formats.

To export a report from Report Writer:

1. Select a report to export by clicking any of the following:

   Select a report from the file tree in the left pane

   File > Open to open an existing report

   File > New Report to create a new report.
2. Select File > Export and then click the format in which you want to export your report:
3. Select the fields in your open report that you want to export into the selected format, and then click OK.
4. Select a location to save your file.
5. Provide a File name, and then click Save.

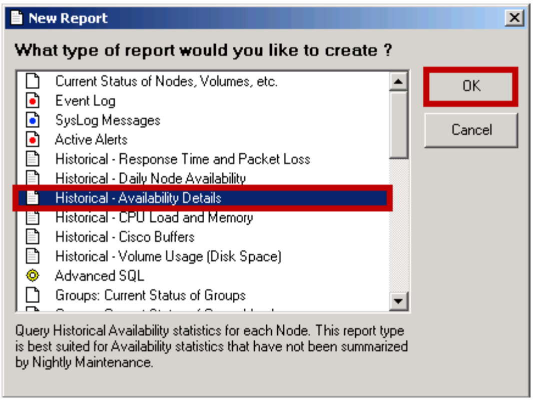
Example Device Availability Report

The following procedure generates an example report of network device availability information over the previous week. The final report is sorted so that the worst errors are viewed first. Down nodes that are still down are at the top with all devices listed in order of increasing availability.

Note: At any point during the creation of a report (or perhaps at many points), you may save what you have done by clicking **File > Save**. The first time you save you must give your report a filename or accept the default, which will be the report title that you assign in the following procedure.

To generates an example report of network device availability information:

1. Click Start > All Programs > SolarWinds > Alerting, Reporting, and Mapping > Report Writer.
2. Click File > New Report.
3. The example calls for a report on availability over the past week, so select Historical Availability Details, and then click OK.

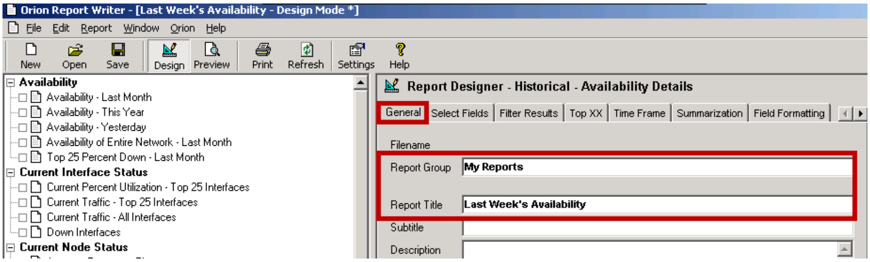


What type of report would you like to create ?

- Current Status of Nodes, Volumes, etc.
- Event Log
- SysLog Messages
- Active Alerts
- Historical - Response Time and Packet Loss
- Historical - Daily Node Availability
- Historical - Availability Details
- Historical - CPU Load and Memory
- Historical - Cisco Buffers
- Historical - Volume Usage (Disk Space)
- Advanced SQL
- Groups: Current Status of Groups

Query Historical Availability statistics for each Node. This report type is best suited for Availability statistics that have not been summarized by Nightly Maintenance.

4. Type My Reports in the Report Group field, and then enter Last Week's Availability as the Report Title.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File
Edit
Report
Window
Orion
Help
New
Open
Save
Design
Preview
Print
Refresh
Settings
Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Report Designer - Historical - Availability Details
General
Select Fields
Filter Results
Top XX
Time Frame
Summarization
Field Formatting

Filename

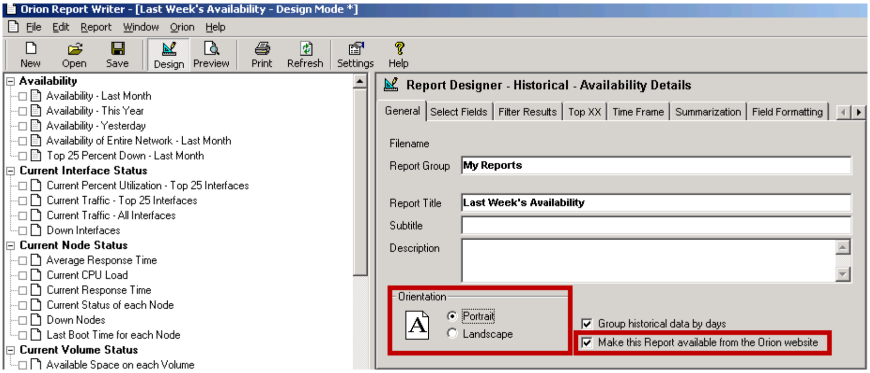
Report Group: My Reports

Report Title: Last Week's Availability

Subtitle

Description

5. Select Portrait for the paper orientation, and then confirm that Make this Report available from the Orion website is selected.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File
Edit
Report
Window
Orion
Help
New
Open
Save
Design
Preview
Print
Refresh
Settings
Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Average Response Time
Current CPU Load
Current Response Time
Current Status of each Node
Down Nodes
Last Boot Time for each Node
Current Volume Status
Available Space on each Volume
Report Designer - Historical - Availability Details
General
Select Fields
Filter Results
Top XX
Time Frame
Summarization
Field Formatting

Filename

Report Group: My Reports

Report Title: Last Week's Availability

Subtitle

Description

Orientation

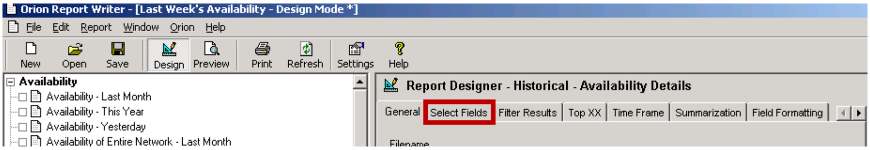
● Portrait

○ Landscape

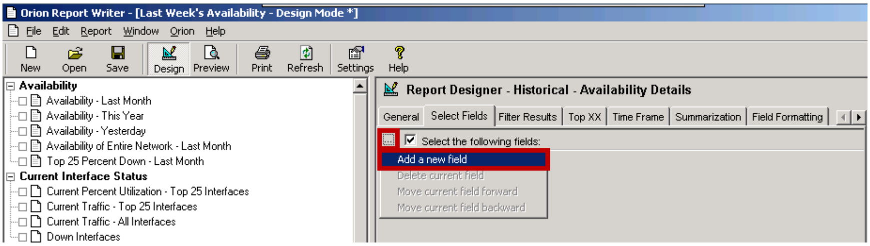
☑ Group historical data by days

☑ Make this Report available from the Orion website

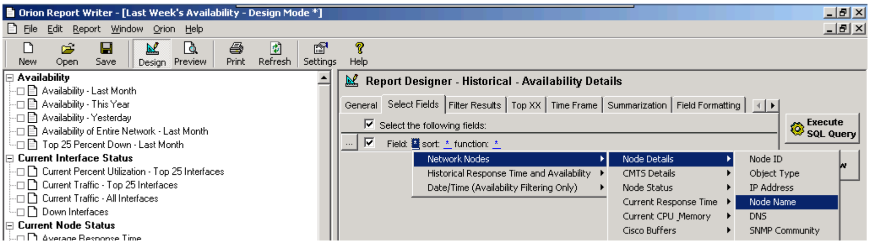
6. Click Select Fields.



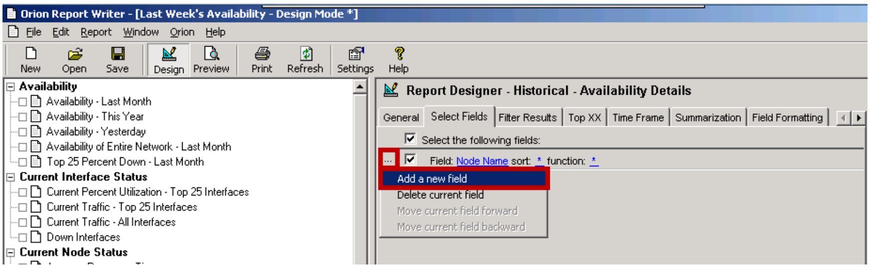
7. Click Browse (…), and then select Add a new field.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting
Select the following fields:
Add a new field
Delete current field
Move current field forward
Move current field backward

8. Click the Field asterisk, and then select Network Nodes > Node Details > Node Name.

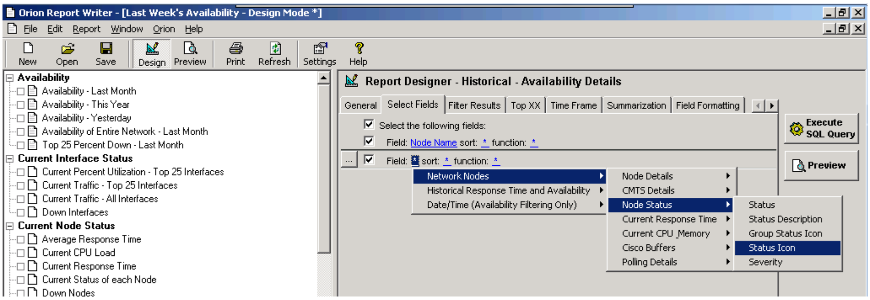

Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Average Response Time
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting
Execute SQL Query
Select the following fields:
Field: * sort: * function: *
Network Nodes
Historical Response Time and Availability
Date/Time (Availability Filtering Only)
Node Details
CMTS Details
Node Status
Current Response Time
Current CPU_Memory
Cisco Buffers
Node ID
Object Type
IP Address
Node Name
DNS
SNMP Community

9. Click Browse (…), and then select Add a new field.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting
Select the following fields:
Field: Node Name sort: * function: *
Add a new field
Delete current field
Move current field forward
Move current field backward

10. Click the Field asterisk, and then select Network Nodes > Node Status > Status Icon.

Note: While this field makes a distinct visual difference for a report viewed in color, it will make little or no difference if printed in black and white.

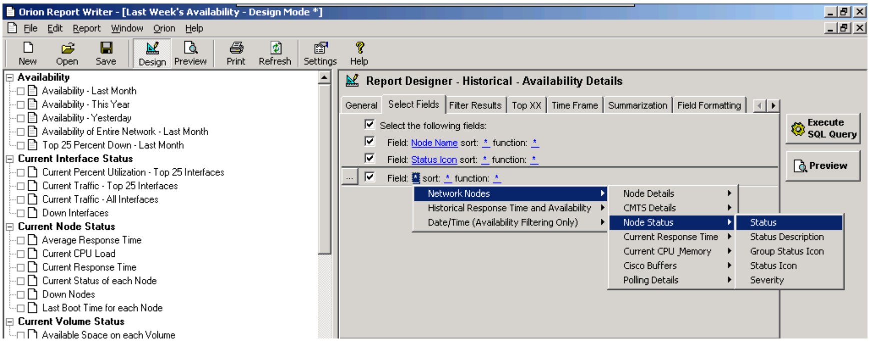

Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Average Response Time
Current CPU Load
Current Response Time
Current Status of each Node
Down Nodes
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting
Execute SQL Query
Preview
Network Nodes
Historical Response Time and Availability
Date/Time (Availability Filtering Only)
Node Details
CMTS Details
Node Status
Current Response Time
Current CPU Memory
Cisco Buffers
Polling Details
Status
Status Description
Group Status Icon
Status Icon
Severity

☑ Select the following fields:

☑ Field: Node Name sort: * function: *

☑ Field: ▪ sort: * function: *

11. Click Browse (…), and then select Add a new field.
12. Click the Field asterisk, and then select Network Nodes > Node Status > Status.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Average Response Time
Current CPU Load
Current Response Time
Current Status of each Node
Down Nodes
Last Boot Time for each Node
Current Volume Status
Available Space on each Volume
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting
Execute SQL Query
Preview
Network Nodes
Historical Response Time and Availability
Date/Time (Availability Filtering Only)
Node Details
CMTS Details
Node Status
Current Response Time
Current CPU Memory
Cisco Buffers
Polling Details
Status
Status Description
Group Status Icon
Status Icon
Severity

☑ Select the following fields:

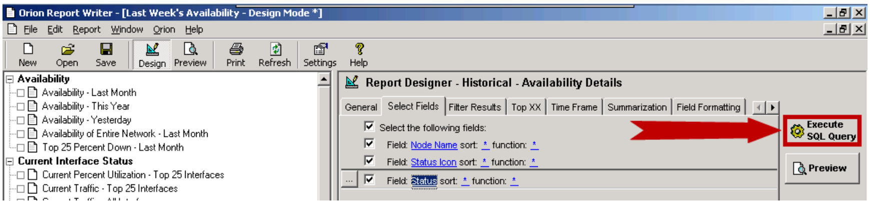
☑ Field: Node Name sort: * function: *

☑ Field: Status Icon sort: * function: *

☑ Field: ▪ sort: * function: *

13. Click Execute SQL Query to view the report data in the preview window.

    Note: The report preview should show information about both current and historical status. Current status entries must be relabeled to avoid confusion.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting
Execute SQL Query
Preview

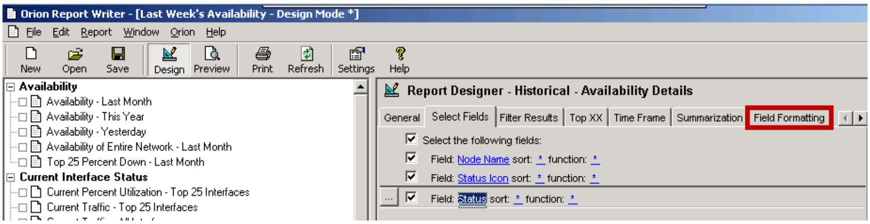
☑ Select the following fields:

☑ Field: Node Name sort: * function: *

☑ Field: Status Icon sort: * function: *

☑ Field: Status sort: * function: *

14. Click Field Formatting.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting

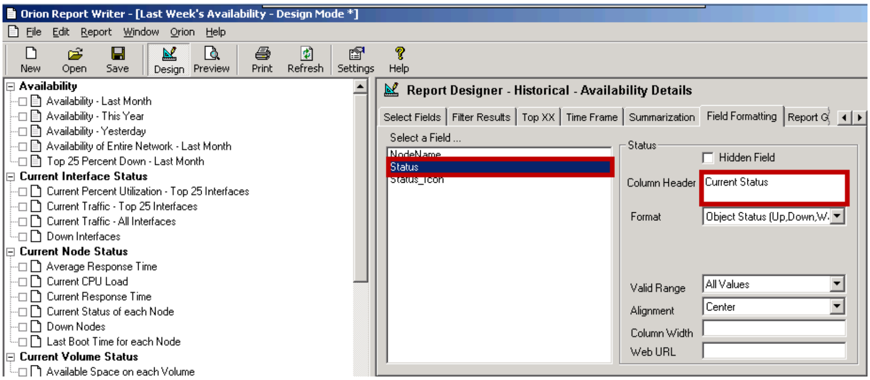
☑ Select the following fields:

☑ Field: Node Name sort: * function: *

☑ Field: Status Icon sort: * function: *

☑ Field: Status sort: * function: *

15. Click Status in the Select a Field list, and then change the Column Header entry to Current Status.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Average Response Time
Current CPU Load
Current Response Time
Current Status of each Node
Down Nodes
Last Boot Time for each Node
Current Volume Status
Available Space on each Volume
Report Designer - Historical - Availability Details
Select Fields Filter Results Top XX Time Frame Summarization Field Formatting Report G

Select a Field ...

NodeName
Status
Status_Icon

Status

□ Hidden Field

Column Header: Current Status

Format: Object Status (Up,Down,W.

Valid Range: All Values

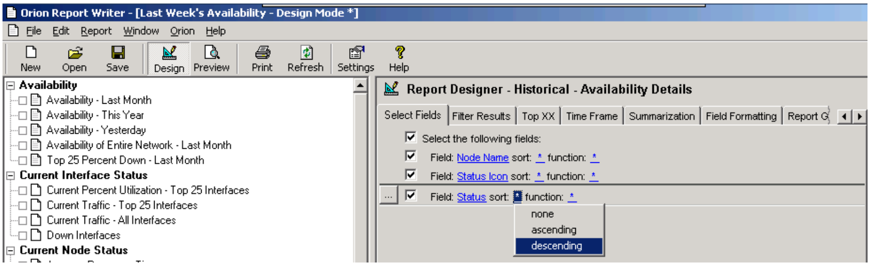
Alignment: Center

Column Width:

Web URL:

16. Click Status_Icon in the Select a Field list, and then change the Column Header entry to Current Status.
17. Click Execute SQL Query.

    Note: Column widths are adjustable. To change a column width, place your cursor on the column divider and drag it to a different position.
18. Click Select Fields.
19. Click the sort asterisk on the Status field line, and then select descending.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Report Designer - Historical - Availability Details
Select Fields Filter Results Top XX Time Frame Summarization Field Formatting Report G

☑ Select the following fields:

☑ Field: Node Name sort: * function: *

☑ Field: Status Icon sort: * function: *

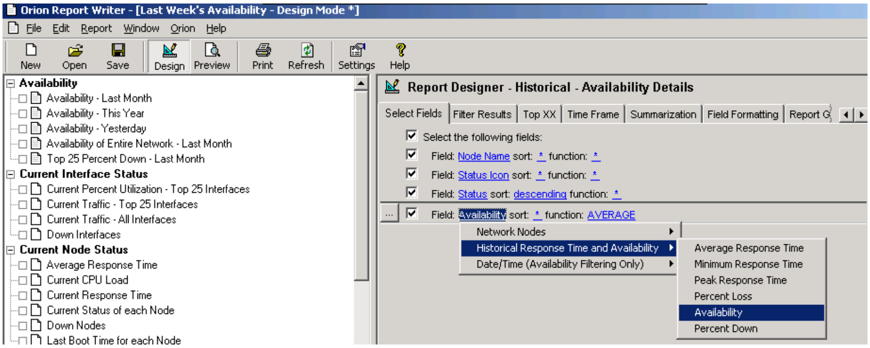
☑ Field: Status sort: * function: *

none
ascending
descending

20. 7. Click Execute SQL Query to confirm your choice.

21. 8. Click Browse (…), and then select Add a new field.

22. Click the Field asterisk, and then select Historical Response Time and Availability > Availability.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Average Response Time
Current CPU Load
Current Response Time
Current Status of each Node
Down Nodes
Last Boot Time for each Node
Report Designer - Historical - Availability Details
Select Fields Filter Results Top XX Time Frame Summarization Field Formatting Report G
Network Nodes
Historical Response Time and Availability
Date/Time (Availability Filtering Only)
Average Response Time
Minimum Response Time
Peak Response Time
Percent Loss
Availability
Percent Down

☑ Select the following fields:

☑ Field: Node Name sort: * function: *

☑ Field: Status Icon sort: * function: *

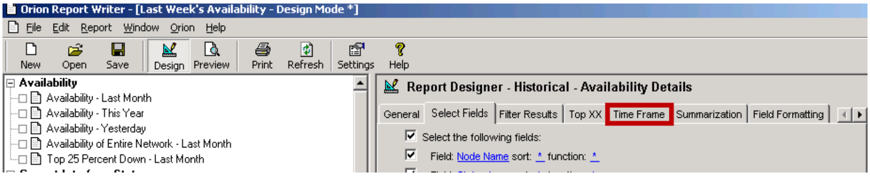
☑ Field: Status sort: descending function: *

☑ Field: Availability sort: * function: AVERAGE

23. Click the sort asterisk on the new line, and then select ascending.

24. Click Execute SQL Query to view the report.

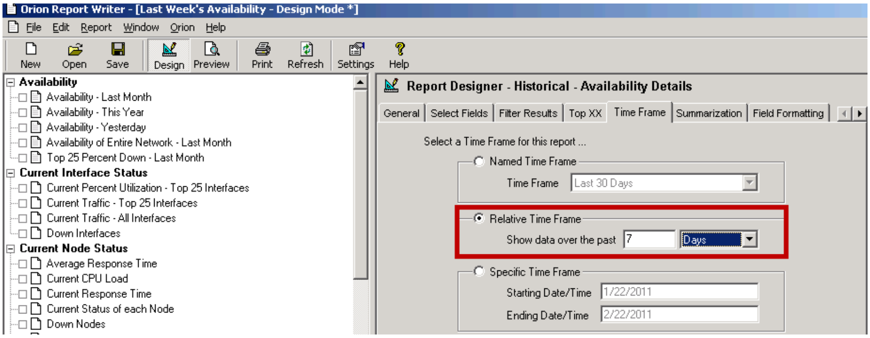
25. Click Time Frame.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting

☑ Select the following fields:

☑ Field: Node Name sort: * function: *

26. Select Relative Time Frame, type 7 in the text field, and then select Days from the list.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Average Response Time
Current CPU Load
Current Response Time
Current Status of each Node
Down Nodes
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting

Select a Time Frame for this report ...

○ Named Time Frame

Time Frame: Last 30 Days

● Relative Time Frame

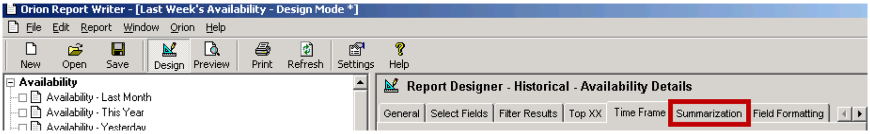
Show data over the past 7 Days

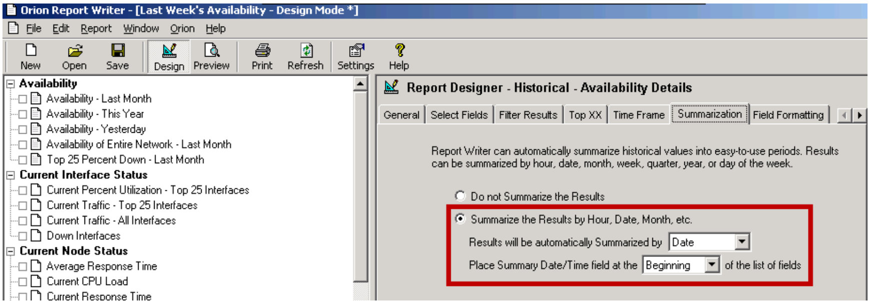
○ Specific Time Frame

Starting Date/Time: 1/22/2011

Ending Date/Time: 2/22/2011

27. If you want to break down the report day-by-day, click Summarization and specify your choices.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Availability of Entire Network - Last Month
Top 25 Percent Down - Last Month
Current Interface Status
Current Percent Utilization - Top 25 Interfaces
Current Traffic - Top 25 Interfaces
Current Traffic - All Interfaces
Down Interfaces
Current Node Status
Average Response Time
Current CPU Load
Current Response Time
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting

Report Writer can automatically summarize historical values into easy-to-use periods. Results can be summarized by hour, date, month, week, quarter, year, or day of the week.

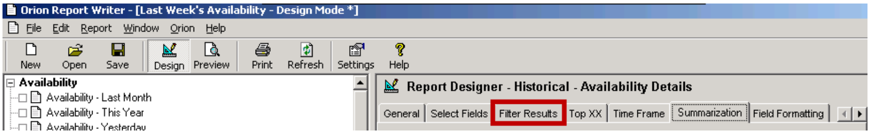
○ Do not Summarize the Results

● Summarize the Results by Hour, Date, Month, etc.

Results will be automatically Summarized by Date

Place Summary Date/Time field at the Beginning of the list of fields

28. If you want to filter your report, click Filter Results and specify filter rules, as on the Select Fields tab.


Orion Report Writer - [Last Week's Availability - Design Mode *]
File Edit Report Window Orion Help
New Open Save Design Preview Print Refresh Settings Help
Availability
Availability - Last Month
Availability - This Year
Availability - Yesterday
Report Designer - Historical - Availability Details
General Select Fields Filter Results Top XX Time Frame Summarization Field Formatting

29. Click File > Save to save your work.

Chapter 17

Configuring TFTP, Secure Copy /SFTP, SMTP Server

The following sections describes how to configure the SolarWinds TFTP Server and Secure Copy SFTP Server.

Using the S

olarWinds TFTP Server

NCM uses the SolarWinds TFTP for file transfers. You can adjust the TFTP Server settings from within the Orion Web Console.

Note: If you have NCM and NPM integrated but installed on separate servers, then you should follow these steps on the NPM server; the settings will automatically apply to NCM.

To adjust TFTP Server settings:

1. Open the Orion Web Console.
2. Click Settings.
3. Click NCM Settings.
4. Click TFTP Server under Network.
5. Select Allow me to specify the IP address of the TFTP server to prevent NCM from resolving the IP address you enter.
6. Enter the IP address of the TFTP Server.
7. Specify the config transfer directory and click Validate.
8. Click Submit.

Using Secure Copy /SFTP Server

The SFTP/SCP server runs as a service, but some basic configuration may be necessary to ensure the SFTP/SCP server behaves in a way that works best within your environment. Complete the following procedure to configure your server.

To configure your SFTP/SCP server:

1. Start SolarWinds SFTP & SCP Server from the SolarWinds SFTP & SCP Server folder.
2. Click File > Configure.
3. Type or browse to the location you want to use as your root folder in the Root Directory field.
4. Select the protocols you want the server to support from the Allowed Protocols list.
5. Select the options you want to enable in the Permitted File Transfer Operations section.
6. Click the TCP/IP Settings tab, and then type the port number you want to use in the TCP Port field.
7. If you want to specify the IP address configuration, click Use Custom IP Address Binding, and then select the IP address you want to use.
8. If you want to enable user authentication on the server, complete the following procedure.
    a. Click the Users tab.
    b. Click New User.
    c. Type the username and password, and then click Apply Changes.
    d. If you want to remove any users, select the username, and then click Remove.
9. Click the Startup and System Tray tab.
10. If you want to start the SFTP/SCP server when Windows starts, select Automatically run this application when I Login on Windows.
11. Specify if you want the application to close or minimize to the system tray in the Clicking the Close Button section.
12. Click OK.

Using a Third-Party SCP server.

The following section details the steps necessary to configure NCM to use a third-party SCP server for config transfers.

To configure NCM to use a third-party SCP server:

1. Open the Orion Web Console.
2. Click Settings.
3. Click NCM Settings.

4. Click SCP Server under Network.
5. Enter a valid Username and Password, confirming the password.
6. Select the Use third-party SCP Server.
7. 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.
8. 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.
9. Click Submit.

   Note: User must have Receive\Transmit permissions configured in the third-party SCP server.

Configuring the SMTP Server for Email Notifications

The settings you enter in the SMPTP Server resource are used to send notifications regarding real-time config changes (RTCD), config change approvals, and running jobs.

To setup an SMTP server:

1. Open the Orion Web Console.
2. Click Settings.
3. Click NCM Settings.
4. Click SMTP Server under Manage Notifications.
5. Enter the FQDN of the server in Email Server Address.
6. Enter the Port Number on which the server handles messages.
7. Select an Authentication type.
8. If you selected Password as your Authentication type, enter a username and password that the server accepts.
9. Click Submit.

   For information on config change approvals, see Chapter 13, “Approving Device Configuration Changes”.

Email Notification Settings

These settings determine the sender, reply address, and subject included in the header of notifications received upon completion of an NCM job.

To define email notification settings:

1. Enter in Sender Name the name you want to appear with a job completion notification.
2. Enter a Reply Address if desired.
3. Enter the Subject to be used in sending a job completion notification.
4. Click Submit.

Chapter 18

Managing EnergyWise Entities

The following sections explore how you can use SolarWinds Network Configuration Manager in conjunction with SolarWinds Network Performance Manager to enable and manage your Cisco EnergyWise entities.

What is EnergyWise?

EnergyWise is Cisco's response to the call to cut energy costs, address environmental concerns, and adhere to government directives around *green* technologies. By purchasing EnergyWise capable devices and enabling their energy-saving features, you can retain business critical systems in a fully powered state while allowing less critical power over ethernet (PoE) devices to power down or drop into standby during off hours.

EnergyWise gives you the ability to control your energy cost. SolarWinds NCM gives you the ability to remotely apply recurrence policies and schedule power usage, helping you use less power. And, SolarWinds NPM allows you to monitor your energy use and power levels. SolarWinds perfectly partners with Cisco and the EnergyWise technologies to help you save more and monitor your savings.

Managing and Enabling EnergyWise Nodes

Cisco devices that support the EnergyWise technology can be enabled and their EnergyWise settings managed through the SolarWinds NCM integration with SolarWinds NPM. Before completing the following procedure, you must have installed SolarWinds NCM and Orion PM in an integrated setup. For more information on integrated setups see Chapter 2, “Installing SolarWinds Network Configuration Manager”. EnergyWise nodes must be managed in both SolarWinds NCM and SolarWinds NPM. For more information about adding nodes to SolarWinds NCM, see “Adding Nodes”. For more information about discovering and adding nodes to SolarWinds NPM, see the *SolarWinds NPM Administrator Guide*.

To enable or manage EnergyWise on an SolarWinds NPM node:

1. Navigate to your Orion Web Console. For example, type http://NameOfOrionServer in the address bar of your web browser.
2. Login on SolarWinds NPM.
3. Click Settings.
4. Click Manage Nodes.

5. Select the Cisco node you want EnergyWise enable, and then click More Actions > Manage EnergyWise.
6. Click enable EnergyWise on these nodes.
7. Specify the appropriate values on the Manage EnergyWise Node page. For more information about a field, click Help.
8. Click Execute Config Actions.

   Note: To manage or modify node-level EnergyWise settings, repeat this procedure omitting Step 6.

Managing Your PoE Ports

Power over ethernet (PoE) devices are connected to your devices on an interface and are managed at the interface level. Before completing the following procedure, you must have installed the SolarWinds NCM Integration for SolarWinds NPM on your SolarWinds NPM server and added your EnergyWise capable nodes to both SolarWinds NCM and SolarWinds NPM. For more information about adding nodes to SolarWinds NCM, see “Adding Nodes”.

The following procedure guides you through enabling and configuring your EnergyWise interfaces. For more information about recurrence policies or the interaction between recurrence importance and entity importance, see the *Help*.

To enable or manage EnergyWise on an SolarWinds NPM interface:

1. Navigate to your SolarWinds NPM Web Console. For example, type http://NameOfOrionServer in the address bar of your web browser.
2. Login on SolarWinds NPM.
3. Click Settings in the Views menu bar.
4. Click Manage Nodes.
5. Expand the Cisco node containing the interface you want to configure.
6. Select the interface you want to EnergyWise enable, and then click More Actions > Manage EnergyWise.
7. Click enable EnergyWise on these nodes.
8. Specify the appropriate values on the Manage EnergyWise Interface page. For more information about a field, click Help.
9. Click Execute Config Actions.

Note: To manage or modify interface-level EnergyWise settings, repeat this procedure omitting **Step 7**.

Chapter 19

Common Tasks

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

Customizing the Login Banner of a Device

You can easily change the login banner for a router, switch, or firewall using SolarWinds Network Configuration Manager. This customization can be rolled out to a single or multiple devices. The following procedure references other sections of the guide:

- Downloading Configuration Files
- Comparing Configurations
- Executing Command Scripts

To modify a login banner:

1. Open the Orion Web Console and navigate to the NCM Jobs view (CONFIGS > Jobs).
2. Click Create New Job, select Execute Command Script on Device, and give the job a title.
3. Select the schedule type.

   Basic gives you Once, Daily, Weekly, and Monthly schedule settings (start, end, recurrence). .

   Advanced gives you more granular control over the schedule, supporting more complex patterns defined with cron expressions.
4. If you are creating a Basic schedule, select the frequency of the job.

   Once: enter a day and time (at least 15 minutes from current NCM server time).

   Daily: Select Every Day or Every Week Day, enter a Start time, and then select start and end dates

   Weekly: Select the days, enter a Start time, and then select start and end dates.

   Monthly: Select the months, days of the month, enter a Start time, and then select start and end dates

5. If you are creating an Advanced schedule, use the five fields to create the appropriate cron expression.

   For example, if you want the job to run once a week over every month at midnight on Sunday morning, the values for the fields would be 0 0 * * 0.

   This transliterates as telling NCM to run the job at 0 minutes and 0 hours, on all valid days of month, in all valid months, on Sunday".

6. Add a comment as needed and then click Next.
7. Select the NCM nodes to target with this job.

   Select Nodes: Click Select Nodes and select the NCM nodes you want the job to target.

   All Nodes: Selects all NCM nodes as targets for the the job.

   Dynamic Selection: Define the criteria that NCM will use to determine the selection of NCM nodes as targets for the job. Nodes defined in legacy job scheduling system: Select the option and then click Yes, change selection.

   Note: Use this option to target the node group of all wireless access points in the database.

8. Select an email notification option.
   a. If you select Email Results, then enter the email from/to information.
   b. Enter the email server address and port number.
   c. If the email server expects credentials, then select Password.
   d. Enter the username and password.
9. Click Next.
10. If you want to load an existing command script, click Load Script, browse to your command script file, and then click Open
11. 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.

12. If you want to save a script, click Save Script, specify a location, and then click Save.
13. Select Filter results that match a pattern if you want to see in the script output only those lines that match a specific regex pattern
14. Select Show commands in output to view what NCM sent to the targeted devices.
15. Click Next.
16. Review the settings for the job.
17. When you are done reviewing the settings, click Finish.
18. After the script executes, to verify the results, complete the following procedure:
    a. Open the NCM application (Start > SolarWinds Network Configuration Manager).
    b. Select a relevant node or relevant nodes from the node tree.
    c. Click the Telnet tool button. A new window or windows open with a Telnet session command prompt, displaying the new login banner.
19. To verify the script executed successfully by comparing the current configuration to the previous configuration, complete the following procedure:
    a. Open the Configuration Management view (CONFIGS > Configuration Management).
    b. Select Compare Selected Configs.
    c. For a relevant device, select relevant configs in the Select Configs tree.
    d. Click Compare Selected.

    A comparison window opens. Changes to the login banner are highlighted in yellow if the banner is different from a previous login banner. If no login banner was previously specified, changes are highlighted in red and green.

Configuring Automated Nightly Backups

A powerful feature of SolarWinds Network Configuration Manager is the ability to schedule daily configuration file backups. SolarWinds Network Configuration Manager installs an example job which downloads the configuration files nightly for all nodes in the database. You can modify the example for your specific needs, or you can create a new job. The following procedure creates a new nightly configuration backup job. For more information on creating jobs, see “Managing Jobs”.

To setup nightly configuration backups for all nodes:

1. Open the Orion Web Console and navigate to the NCM Jobs view (CONFIGS > Jobs).
2. Click Create New Job, select Download Configs from Devices, and give the job a title.
3. Select the schedule type.

   Basic gives you Once, Daily, Weekly, and Monthly schedule settings (start, end, recurrence). .

   Advanced gives you more granular control over the schedule, supporting more complex patterns defined with cron expressions.
4. If you are creating a Basic schedule, select the frequency of the job.

   Once: enter a day and time (at least 15 minutes from current NCM server time).

   Daily: Select Every Day or Every Week Day, enter a Start time, and then select start and end dates

   Weekly: Select the days, enter a Start time, and then select start and end dates.

   Monthly: Select the months, days of the month, enter a Start time, and then select start and end dates
5. If you are creating an Advanced schedule, use the five fields to create the appropriate cron expression.

   For example, if you want the job to run once a week over every month at midnight on Sunday morning, the values for the fields would be 0 0 * * 0.

   This transliterates as telling NCM to run the job at 0 minutes and 0 hours, on all valid days of month, in all valid months, on Sunday”.
6. Add a comment as needed and then click Next.
7. Select the NCM nodes to target with this job.

   Select Nodes: Click Select Nodes and select the NCM nodes you want the job to target.

   All Nodes: Selects all NCM nodes as targets for the the job.

   Dynamic Selection: Define the criteria that NCM will use to determine the selection of NCM nodes as targets for the job.

   Nodes defined in legacy job scheduling system: Select the option and then click Yes, change selection.

   Note: Use this option to target the node group of all wireless access points in the database.

8. Select an email notification option.
    a. If you select Email Results, then enter the email from/to information.
    b. Enter the email server address and port number.
    c. If the email server expects credentials, then select Password.
    d. Enter the username and password.
9. Click Next.
10. Select the configuration types you want to download.
11. If you want to be notified when the downloaded configuration file is different from the last configuration, select Last downloaded config file.
12. If you want to be notified when the downloaded configuration file is different from the baseline configuration, select Baseline config file.
13. If you want to be notified when the downloaded configuration file is different from the startup configuration, select Startup config file.
14. Select Send config change notification details in a separate text email and Send config change notification details in a separate HTML email as appropriate. These options allow you to separate change details from change notification.
15. If you only want to save the configuration file when changes are found, select Only save Configs that have changed.
16. Click Next.
17. Review the settings for the job.
18. When you are done reviewing the settings, click Finish.

Changing the Community String on Multiple Nodes

The following procedure replaces the `public` read-only community string with a new read-only community string on several network nodes at the same time. The procedure references other sections of the guide:

- Downloading Configuration Files
- Comparing Configurations
- Executing Command Scripts

To change the community string on multiple nodes:

1. Open the Orion Web Console and navigate to the NCM Jobs view (CONFIGS > Jobs).
2. Click Create New Job, select Execute Command Script on Device, and give the job a title.

3. Select the schedule type.

   Basic gives you Once, Daily, Weekly, and Monthly schedule settings (start, end, recurrence). .

   Advanced gives you more granular control over the schedule, supporting more complex patterns defined with cron expressions.

4. If you are creating a Basic schedule, select the frequency of the job.

   Once: enter a day and time (at least 15 minutes from current NCM server time).

   Daily: Select Every Day or Every Week Day, enter a Start time, and then select start and end dates

   Weekly: Select the days, enter a Start time, and then select start and end dates.

   Monthly: Select the months, days of the month, enter a Start time, and then select start and end dates

5. If you are creating an Advanced schedule, use the five fields to create the appropriate cron expression.

   For example, if you want the job to run once a week over every month at midnight on Sunday morning, the values for the fields would be 0 0 * * 0.

   This transliterates as telling NCM to run the job at 0 minutes and 0 hours, on all valid days of month, in all valid months, on Sunday".

6. Add a comment as needed and then click Next.

7. Select the NCM nodes to target with this job.

   Select Nodes: Click Select Nodes and select the NCM nodes you want the job to target.

   All Nodes: Selects all NCM nodes as targets for the the job.

   Dynamic Selection: Define the criteria that NCM will use to determine the selection of NCM nodes as targets for the job.

   Nodes defined in legacy job scheduling system: Select the option and then click Yes, change selection.

   Note: Use this option to target the node group of all wireless access points in the database.

8. Select an email notification option.

a. If you select Email Results, then enter the email from/to information.

b. Enter the email server address and port number.

c. If the email server expects credentials, then select Password.

d. Enter the username and password.

9. Click Next.
10. If you want to load an existing command script, click Load Script, browse to your command script file, and then click Open
11. 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.
12. If you want to save a script, click Save Script, specify a location, and then click Save.
13. Select Filter results that match a pattern if you want to see in the script output only those lines that match a specific regex pattern
14. Select Show commands in output to view what NCM sent to the targeted devices.
15. Click Next.
16. Review the settings for the job.
17. When you are done reviewing the settings, click Finish.
18. To verify the script executed successfully by comparing the current configuration to the previous configuration, complete the following procedure:

    a. Open the Configuration Management view (CONFIGS > Configuration Management).

    b. Select Compare Selected Configs.

    c. For a relevant device, select relevant configs in the Select Configs tree.

    d. Click Compare Selected.

    A comparison window opens. Changes to are highlighted in red and green.

Changing 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. Complete the following procedure to modify an interface description. The procedure references other sections of the guide:

- Downloading Configuration Files
- Comparing Configurations
- Executing Command Scripts

To update an interface description on a node:

1. Back up the running configuration prior to making any changes.

    a. Open the Orion Web Console to the NCM configuraiton management view (CONFIGS > Configuration Management).

    b. Select Download Config.

    c. Select Running as the config type.

    d. Select the relevant NCM node(s).

    e. Click Download.

2. Open the NCM Jobs view (CONFIGS > Jobs).
3. Click Create New Job, select Execute Command Script on Device, and give the job a title.
4. Select the schedule type.

    Basic gives you Once, Daily, Weekly, and Monthly schedule settings (start, end, recurrence). .

    Advanced gives you more granular control over the schedule, supporting more complex patterns defined with cron expressions.

5. If you are creating a Basic schedule, select the frequency of the job.

Once: enter a day and time (at least 15 minutes from current NCM server time).

Daily: Select Every Day or Every Week Day, enter a Start time, and then select start and end dates

Weekly: Select the days, enter a Start time, and then select start and end dates.

Monthly: Select the months, days of the month, enter a Start time, and then select start and end dates

6. If you are creating an Advanced schedule, use the five fields to create the appropriate cron expression.

   For example, if you want the job to run once a week over every month at midnight on Sunday morning, the values for the fields would be 0 0 * * 0.

   This transliterates as telling NCM to run the job at 0 minutes and 0 hours, on all valid days of month, in all valid months, on Sunday”.

7. Add a comment as needed and then click Next.
8. Select the NCM nodes to target with this job.

   Select Nodes: Click Select Nodes and select the NCM nodes you want the job to target.

   All Nodes: Selects all NCM nodes as targets for the the job.

   Dynamic Selection: Define the criteria that NCM will use to determine the selection of NCM nodes as targets for the job.

   Nodes defined in legacy job scheduling system: Select the option and then click Yes, change selection.

   Note: Use this option to target the node group of all wireless access points in the database.

9. Select an email notification option.
   a. If you select Email Results, then enter the email from/to information.
   b. Enter the email server address and port number.
   c. If the email server expects credentials, then select Password.
   d. Enter the username and password.
10. Click Next.
11. If you want to load an existing command script, click Load Script, browse to your command script file, and then click Open
12. 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.

13. If you want to save a script, click Save Script, specify a location, and then click Save.
14. Select Filter results that match a pattern if you want to see in the script output only those lines that match a specific regex pattern
15. Select Show commands in output to view what NCM sent to the targeted devices.
16. Click Next.
17. Review the settings for the job.
18. When you are done reviewing the settings, click Finish.
19. Verify the script was executed successfully by complete the following procedure:
    a. Navigate to CONFIGS > Config Summary and click the node in the list.
    b. Click Edit Config under Config List.
    c. Select the running config and click Edit Conifg.
    d. Locate the interface definitions.
    e. Verify that the new description has been applied to the interface you modified.

Upgrading IOS and Firmware

You can upload IOS images uploaded using the SolarWinds Network Configuration Manager internal scripting engine. You can transfer these image files using TFTP, FTP (third party), SCP (third party), HTTP, or any other transfer protocol.

The following example takes advantage of the SolarWinds TFTP Server, included with SolarWinds Network Configuration Manager, to transfer an IOS image to the router. The TFTP Server must be running and configured to send and receive files. Also, the IOS image file must reside in the TFTP Root Directory.

IOS image management can be very complex. SolarWinds recommends you follow the upgrade guidelines outlined by your hardware manufacturer.

The following procedure references other sections of the guide:

- “Downloading Configuration Files” on page 83
- “Executing Command Scripts” on page 147

To push an IOS image to a network device:

1. Back up the running configuration prior to making any changes.
    a. Open the Orion Web Console to the NCM configuraiton management view (CONFIGS > Configuration Management).
    b. Select Download Config.
    c. Select Running as the config type.
    d. Select the relevant NCM node(s).
    e. Click Download.
2. Open the NCM Jobs view (CONFIGS > Jobs).
3. Click Create New Job, select Execute Command Script on Device, and give the job a title.
4. Select the schedule type.

    Basic gives you Once, Daily, Weekly, and Monthly schedule settings (start, end, recurrence). .

    Advanced gives you more granular control over the schedule, supporting more complex patterns defined with cron expressions.
5. If you are creating a Basic schedule, select the frequency of the job.

    Once: enter a day and time (at least 15 minutes from current NCM server time).

    Daily: Select Every Day or Every Week Day, enter a Start time, and then select start and end dates

    Weekly: Select the days, enter a Start time, and then select start and end dates.

    Monthly: Select the months, days of the month, enter a Start time, and then select start and end dates

6. If you are creating an Advanced schedule, use the five fields to create the appropriate cron expression.

   For example, if you want the job to run once a week over every month at midnight on Sunday morning, the values for the fields would be 0 0 * * 0.

   This transliterates as telling NCM to run the job at 0 minutes and 0 hours, on all valid days of month, in all valid months, on Sunday”.

7. Add a comment as needed and then click Next.

8. Select the NCM nodes to target with this job.

   Select Nodes: Click Select Nodes and select the NCM nodes you want the job to target.

   All Nodes: Selects all NCM nodes as targets for the the job.

   Dynamic Selection: Define the criteria that NCM will use to determine the selection of NCM nodes as targets for the job.

   Nodes defined in legacy job scheduling system: Select the option and then click Yes, change selection.

   Note: Use this option to target the node group of all wireless access points in the Orion Platform database.

9. Select an email notification option.

   a. If you select Email Results, then enter the email from/to information.Enter the email server address and port number.

   b. If the email server expects credentials, then select Password.

   c. Enter the username and password.

10. Click Next.

11. If you want to load an existing command script, click Load Script, browse to your command script file, and then click Open

12. 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-l.123-9a.bin

    Y
    ```

    Where 10.10.2.17 is the location of the IOS image to copy using TFTP.

13. If you want to save a script, click Save Script, specify a location, and then click Save.

14. Select Filter results that match a pattern if you want to see in the script output only those lines that match a specific regex pattern
15. Select Show commands in output to view what NCM sent to the targeted devices.
16. Click Next.
17. Review the settings for the job.
18. When you are done reviewing the settings, click Finish.

Blocking All Private Addresses with an Access 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 (ACL) to block all private IP addresses on several devices at the same time. The procedure references other sections of the guide:

- Downloading Configuration Files
- Comparing Configurations
- Executing Command Scripts

To update the ACL for a group of nodes:

1. Back up the running configuration prior to making any changes.
   a. Open the Orion Web Console to the NCM configuraiton management view (CONFIGS > Configuration Management).
   b. Select Download Config.
   c. Select Running as the config type.
   d. Select the relevant NCM node(s).
   e. Click Download.
2. Open the NCM Jobs view (CONFIGS > Jobs).
3. 9Click Create New Job, select Execute Command Script on Device, and give the job a title.
4. Select the schedule type.

   Basic gives you Once, Daily, Weekly, and Monthly schedule settings (start, end, recurrence). .

   Advanced gives you more granular control over the schedule, supporting more complex patterns defined with cron expressions.

5. If you are creating a Basic schedule, select the frequency of the job.

   Once: enter a day and time (at least 15 minutes from current NCM server time).

   Daily: Select Every Day or Every Week Day, enter a Start time, and then select start and end dates

   Weekly: Select the days, enter a Start time, and then select start and end dates.

   Monthly: Select the months, days of the month, enter a Start time, and then select start and end dates

6. If you are creating an Advanced schedule, use the five fields to create the appropriate cron expression.

   For example, if you want the job to run once a week over every month at midnight on Sunday morning, the values for the fields would be 0 0 * * 0.

   This transliterates as telling NCM to run the job at 0 minutes and 0 hours, on all valid days of month, in all valid months, on Sunday".

7. Add a comment as needed and then click Next.

8. Select the NCM nodes to target with this job.

   Select Nodes: Click Select Nodes and select the NCM nodes you want the job to target.

   All Nodes: Selects all NCM nodes as targets for the the job.

   Dynamic Selection: Define the criteria that NCM will use to determine the selection of NCM nodes as targets for the job.

   Nodes defined in legacy job scheduling system: Select the option and then click Yes, change selection.

   Note: Use this option to target the node group of all wireless access points in the Orion Platform database.

9. Select an email notification option.

   a. If you select Email Results, then enter the email from/to information.
   b. Enter the email server address and port number.
   c. If the email server expects credentials, then select Password.
   d. Enter the username and password.

10. Click Next.

11. If you want to load an existing command script, click Load Script, browse to your command script file, and then click Open

12. 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.

13. If you want to save a script, click Save Script, specify a location, and then click Save.
14. Select Filter results that match a pattern if you want to see in the script output only those lines that match a specific regex pattern
15. Select Show commands in output to view what NCM sent to the targeted devices.
16. Click Next.
17. Review the settings for the job.
18. When you are done reviewing the settings, click Finish.
19. If you want to verify the script executed successfully, complete the following procedure:

   a. Right-click the node or group of nodes, and then click Download Configs.
   b. Select Compare to last Config Downloaded.
   c. Click Download.
   d. Review the comparison window. Changes to are highlighted in red and green.

Blocking a MAC Address on a Wireless Access Point

If you discover a device utilizing unauthorized access through your wireless network, you can block the MAC address to prevent future access. The following procedure uses an access control list (ACL) on a wireless access point to block a specific MAC address. The procedure references other sections of the guide:

- Downloading Configuration Files
- Comparing Configurations
- Executing Command Scripts

To block a MAC on a wireless access point:

1. Back up the running configuration prior to making any changes.
   a. Open the Orion Web Console to the NCM configuraiton management view (CONFIGS > Configuration Management).
   b. Select Download Config.
   c. Select Running as the config type.
   d. Select the relevant NCM node(s).
   e. Click Download.
2. Open the NCM Jobs view (CONFIGS > Jobs).
3. Click Create New Job, select Execute Command Script on Device, and give the job a title.
4. Select the schedule type.

   Basic gives you Once, Daily, Weekly, and Monthly schedule settings (start, end, recurrence). .

   Advanced gives you more granular control over the schedule, supporting more complex patterns defined with cron expressions.
5. If you are creating a Basic schedule, select the frequency of the job.

   Once: enter a day and time (at least 15 minutes from current NCM server time).

   Daily: Select Every Day or Every Week Day, enter a Start time, and then select start and end dates

   Weekly: Select the days, enter a Start time, and then select start and end dates.

   Monthly: Select the months, days of the month, enter a Start time, and then select start and end dates

6. If you are creating an Advanced schedule, use the five fields to create the appropriate cron expression.

   For example, if you want the job to run once a week over every month at midnight on Sunday morning, the values for the fields would be 0 0 * * 0.

   This transliterates as telling NCM to run the job at 0 minutes and 0 hours, on all valid days of month, in all valid months, on Sunday”.

7. Add a comment as needed and then click Next.

8. Select the NCM nodes to target with this job.

   Select Nodes: Click Select Nodes and select the NCM nodes you want the job to target.

   All Nodes: Selects all NCM nodes as targets for the the job.

   Dynamic Selection: Define the criteria that NCM will use to determine the selection of NCM nodes as targets for the job.

   Nodes defined in legacy job scheduling system: Select the option and then click Yes, change selection.

   Note: Use this option to target the node group of all wireless access points in the Orion Platform database.

9. Select an email notification option.

   a. If you select Email Results, then enter the email from/to information.

   b. Enter the email server address and port number.

   c. If the email server expects credentials, then select Password.

   d. Enter the username and password.

10. Click Next.

11. If you want to load an existing command script, click Load Script, browse to your command script file, and then click Open

12. 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 ACL you are modifying, and where 000E.0CA1.A2B4 is the MAC address to block. ${EnterConfigMode} is a variable that is equivalent to Config Terminal on Cisco devices.

13. If you want to save a script, click Save Script, specify a location, and then click Save.
14. Select Filter results that match a pattern if you want to see in the script output only those lines that match a specific regex pattern
15. Select Show commands in output to view what NCM sent to the targeted devices.
16. Click Next.
17. Review the settings for the job.
18. When you are done reviewing the settings, click Finish.
19. If you want to verify the script executed successfully, complete the following procedure:
    a. Right-click the node or group of nodes, and then click Download Configs.

    b. Select Compare to last Config Downloaded.

    c. Click Download.

    d. Review the comparison window. Changes are highlighted in red and green.

Appendix A

Node and Archive Variables

SolarWinds Network Configuration Manager uses a variable system that is similar to the one used in SolarWinds Network Performance Monitor. Variables always begin with a dollar sign and a curly brace (`${`), and always end with a curly brace (`}`).

Variables may be used within almost any custom property. They may also be used in any of the user editable system properties.

Variables can also be nested and recursive. That is, a single variable can refer to a Node property that contains more variables that then contain even more variables. The following example demonstrates nested variables.

Node Property	Value of Property
Location	Rack ${Rack} on ${Floor} floor of ${Building} - ${SysLocation}
Building	Building C
SysLocation	Data Center A
Rack	15
Floor	Second

The database value of *Location* is `Rack ${Rack} on ${Floor} floor of ${Building} - ${SysLocation}`. The displayed value of *Location* is `Rack 15 on Second floor of Building C - Data Center A`.

For more information about Syslog, Trap, and Template variables, see the following sections:

- “Command Template Commands” on page 139
- "Pre-Command and Command Template Variables” on page 141
- "Trap Alert Variables” on page 393
- "Syslog Alert Variables” on page 404

Node Variables

All fields in the nodes table may be used as variables, including any custom properties added to your nodes.

Nodes Table Field	Description
NodeID	Unique ID assigned to each Network Node
NodeCaption	Displayed name for the node. The default for NodeCaption is a variable. `${SysName}`
NodeGroup	Group to which this node belongs. Some group examples include `Routers`, `Accounting`, or simply `${Building}`. The last example refers to a custom property named `Building`.
AgentIP	The IP address used when communicating with the node. A router or server may have many IP addresses. This IP address is the one used when SolarWinds Network Configuration Manager makes SNMP requests or transfers configuration files.
AgentIPSort	Numeric equivalent of the AgentIP. Used for sorting by IP address in reports.
ReverseDNS	Reverse lookup of the AgentIP
ResponseTime	Current response time of the node in milliseconds
ResponseError	OK if the node is responding. Returns an error message if the node is not responding.
Status	Numeric status of the node. 1 = Up 2 = Down
Community	SNMP community string
SNMPLevel	The version of SNMP supported by the Node. 0 = SNMP not supported 1 = SNMP V1 2 = SNMP V2 3 = SNMP V3
SysName	System name of the node.
SysDescr	System description of the node.
SysContact	System contact information collected from the node.
SysLocation	System location information collected from the node.
SystemOID	System OID discovered from the node.
Vendor	Hardware vendor of this network node.
VendorIcon	Name of the vendor icon used.
MachineType	Type of hardware. This information is discovered by SolarWinds Discovery Engine.
LastBoot	Last time the node rebooted.
OSImage	Operating system running on the node
OSVersion	Version of the operating system running on the node
ConfigTypes	Types of configuration files supported by this node

Nodes Table Field	Description
NodeComments	Any comments about this node entered by the user.
NextDiscovery	Time for next complete discovery of this node
NextPoll	Time for next poll (up/down and response time)
Username	Login username
Password	Login password
EnableLevel	Enable level used when transferring configs or running scripts
EnablePassword	Enable level password
ExecProtocol	The protocol used when executing scripts. This is set to `${GlobalExecProtocol}` by default.
TransferProtocol	The protocol used when downloading configs. This is set to `${GlobalTransferProtocol}` by default.

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.

Property	Description
DateTime	Local date and time in short date and local time format
Date	Date in short date format
LongDate	Date in long date format
MediumDate	Date in medium date format
Time	Time in short time format
LongTime	Time in long time format
MediumTime	Time in "medium time" format
ShortTime	Time in "short time" format
DOW	Day of the week (spelled out)
D	Day of the month
DD	Day of the month (with leading zero, if needed)
ABREVIATEDDOW	Day of the week in abbreviated format
LocalDow	Day of the week in the local language
Month	Number of the current month
M	Number of the current month
MM	Number of the current month (with leading zeros, if needed)
MMM	Abbreviated name of the month
MMMM	Name of the month
LocalMonthName	Name of the month in the local language
DAYOFYEAR	Day number of the year

Property	Description
YYYY	4 digit year
YY	2 digit year
YEAR2	2 digit year
YEAR4	4 digit year
H	Hour
HH	2 digit hour (with leading zero, if needed)
N	Minute
NN	2 digit minute (with leading zero, if needed)
S	Seconds
SS	2 digit seconds (with leading zero, if needed)
AMPM	AM or PM
CRLF	Carriage return - linefeed combination
ConfigType	Type of configuration (running, startup, etc)
Caption	Caption of the node (NodeCaption)

Appendix B

Regular Expression Pattern Matching

When editing comparison criteria, the following regular expressions can be used for pattern matching. Examples are provided at the end of this section; however, the examples are not and do not intend to be comprehensive. In general, SolarWinds does not offer support in constructing regular expressions and instead expects users of NCM to create expressions valid for their own intended purposes.

Characters

<table>
<tr><th>Character</th><th>Description</th><th>Example</th></tr>
<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>\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>\r\n matches a DOS/Windows CRLF line break.</td></tr>
</table>

Character Classes or Character Sets [abc]

Character	Description	Example
[(opening square bracket)	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	
Any character except ^,-,],\ add that character to the possible matches for the character class.	All characters except the listed special characters.	[abc] matches a, b or c
\ (backslash) followed by any of ^,-,],\	A backslash escapes special characters to suppress their special meaning.	[\^\]] matches ^ or]
- (hyphen) except immediately after the opening [	Specifies a range of characters. (Specifies a hyphen if placed immediately after the opening [)	[a-zA-Z0-9] matches any letter or digit
^ (caret) immediately after the opening [	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 [)	[^a-d] matches x (any character except a, b, c or d)
\d, \w and \s	Shorthand character classes matching digits 0-9, word characters (letters and digits) and whitespace respectively. Can be used inside and outside character classes	[\d\s] matches a character that is a digit or whitespace

Dot

Character	Description	Example
. (dot)	Matches any single character except line break characters \r and \n.	. matches x or most any other character

Anchors

Character	Description	Example
^ (caret)	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.	^. matches a in abc\ndef. Also matches d in "multi-line" mode.
$ (dollar)	Matches at the end of the string to which the regular expression pattern is applied. Matches a position rather than a character. Most regular expression flavors have an option to make the dollar match before line breaks (i.e. at the end of a line in a file) as well. Also matches before the very last line break if the string ends with a line break. Note: If there are some special non-printable characters at the end of the lines in a downloaded config, the $ operator might not match the line end. A test would be to copy lines from a config to a plain text file (in Notepad, for example); if you see extra, empty lines that are not in the pasted content then there are mostly likely non-printable characters in them.	.$ matches f in abc\ndef. Also matches c in "multi-line" mode.
\A	Matches at the start of the string to which the regular expression pattern is applied to. Matches a position rather than a character. Never matches after line breaks.	\A. matches a in abc
\Z	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.	.\Z matches f in abc\ndef
\z	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.	.\z matches f in abc\ndef

Word Boundaries

Character	Description	Example
\b	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.	.\b matches c in abc
\B	Matches at the position between two word characters (i.e the position between \w\w) as well as at the position between two non-word characters (i.e. \W\W).	\B.\B matches b in abc

Alternation

Character	Description	Example
| (vertical bar or “pipe”)	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.	abc|def|xyz matches abc, def or xyz
| (vertical bar or “pipe”)	The vertical bar has the lowest precedence of all operators. Use grouping to alternate only part of the regular expression.	abc(def|xyz) matches abcdef or abcxyz

Quantifiers

Character	Description	Example
? (question mark)	Makes the preceding item optional. The optional item is included in the match, if possible.	abc? matches ab or abc
??	Makes the preceding item optional. The optional item is excluded in the match, if possible. This construct is often excluded from documentation because of its limited use.	abc?? matches ab or abc
* (star)	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.	.* matches "def" "ghi" in abc "def" "ghi" jkl

Character	Description	Example
*? (lazy star)	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.	.*? matches "def" in abc "def" "ghi" jkl
+ (plus)	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.	.+ matches "def" "ghi" in abc "def" "ghi" jkl
+? (lazy plus)	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.	.+? matches "def" in abc "def" "ghi" jkl
{*n*} where *n* is an integer >= 1	Repeats the previous item exactly *n* times.	a{3} matches aaa
{*n*,*m*} where *n* >= 1 and *m* >= *n*	Repeats the previous item between *n* and *m* times. Will try to repeat *m* times before reducing the repetition to *n* times.	a{2,4} matches aa, aaa or aaaa
{*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

Regular Expression Pattern Matching Examples

The following examples illustrate some of the uses of Regular Expression pattern matching.

```
snmp-server community public
```

Finds any line that includes the text `snmp-server community public`. There can be text before and/or after the string on the same line.

```
access-list 105 deny.*tcp any any eq 139 log
```

Finds the line with access-list 105 deny, followed by any number of characters of any type, followed by tcp any any eq 139 Login on the same line. The regular expression string .* finds any character, and any number of characters on the same line. So, this could be used to find spaces, tabs, numbers, letters, or special characters.

```
ntp clock-period \d*
```

Finds any line that includes ntp clock-period followed by any number. The regular expression string \d* will find any number at any length, such as 3, 48, or 2394887.

```
user \x2a
```

Finds any line that includes user *. The regular expression string \x followed by a hexadecimal value specifies an individual character. In this example, \x2a represents the asterisk character, which has a hexadecimal value of 2a.

Appendix C

Using the Database Management Tools

The SolarWinds Database Manager can be used to perform queries, view database and table details.

For other database management tasks, including back-up and restoring a database for SolarWinds NCM and other Orion Platform products, you need to use an appropriate Microsoft utility such as SQL Server Management Studio.

Starting SolarWinds Database Manager

You can use the Database Manager to view your database. Complete the following procedure to start the Database Manager.

To open Database Manager, click **Start > All Programs > SolarWinds Orion > Advanced Features > SolarWinds Database Manager**.

Adding a Server to SolarWinds Database Manager

The following procedure adds a SQL server to the SolarWinds Database Manager.

To add a SQL server:

1. Start Database Manager (SolarWinds Orion > Advanced Features > Database Manager).
2. Click Add Server.
3. Select the SQL server from the list or enter the IP address of the SQL Server machine.
4. Provide the appropriate login type:

   Windows Integrated Security automatically passes Windows account credentials to the SQL server

   SQL Server user ID and password
5. Click Connect to Database Server. The left pane navigation tree populates with your database server information.

Viewing Database Details

Details about your database can be viewed in Database Manager. To maintain peak performance, monitor the value in the **Total Space Used** field. SolarWinds recommends you compact your database as it approaches capacity. If you are using SQL Express, the maximum database size is 4GB.

The **Last Backup** field should also be noted to ensure you are adhering to a regular database maintenance plan. If this field is blank, you do not have a backup of your database.

To view database details:

1. Start Database Manager.
2. Click Add server and enter relevant information if your Orion Platform database server is not already listed in the left pane.
3. Expand the list under your Orion Platform database server.
4. Right-click the Orion Platform database and select Database Details.
5. Review the Properties tab.

Viewing Table Details

Details about a table in a selected database can be viewed in Database Manager. The Properties tab includes general statistics pertaining to table size and creation date. The Columns tab describes table columns, keys, and field types. The Indexes tab provides a list of indexes used within the table.

To view table details:

1. Start Database Manager.
2. Click Add server and enter relevant information if your Orion Platform database server is not already listed in the left pane.
3. Expand the list under your Orion Platform database server.
4. Expand the list of tables under the Orion Platform database.
5. Right-click a table and select Table Details.
6. Click the Properties, Columns, or Indexes tabs to view details about respective aspects of your table.

Managing and Migrating a Database with SQL Server Management Studio

The following procedures walk you through the creation of a backup of your current SolarWinds database(s) and restoring the, if needed, as part of the process of moving the database to a different SQL Server host.

Note: Shutdown the SolarWinds services with the Orion Service Manager (SolarWinds Orion > Advanced Features) service before you begin backing up your database.

Creating a Database Backup File with SQL 2000 Enterprise Manager

Creating a Database Backup File with SQL Server Management Studio Express

Creating a Database Backup File with SQL Server Management Studio

Creating a Database Backup File with SQL 2000 Enterprise Manager

Complete the following procedure if your new database server uses SQL Server 2000.

To backup your Orion database using SQL 2000 Enterprise Manager:

1. Log on to the new database server using an administrator account.
2. Click Start > All Programs > Microsoft SQL Server > Enterprise Manager.
3. Expand Microsoft SQL Servers, and then click SQL Server Group.
4. Click Action > New SQL Server Registration.
5. Specify in the Registered SQL Server Properties window the name of the server where your database is hosted in the format ServerName\database. For example, if your SolarWinds Orion Platform database is called “NCM_database” and it’s hosted on the SQL Server named NCMSQLServer, you would enter NCMSQLServer\NCM_database in the properties winds.
6. If you are using SQL Server Authentication, click SQL Server Authentication in the Connection grouping, and then specify your credentials in the Login name and Password fields.
7. Click OK.
8. Expand the name of your SolarWinds Orion Platform database server and then expand Databases in the left pane.

9. Right-click the name of your SolarWinds Orion Platform database (for example, right-click ‘NCM_database’), and then click All Tasks > Backup Database.
10. Ensure that both Database — Complete and Overwrite existing media are selected on the SQL Server Backup window:
11. Click Add, and then specify and remember the Destination you provide. This is the directory and name of your backup. For example, you might specify c:\NCM_database.bak.

    Note: Remember, this file is created on the remote database server. It is not created locally.
12. Click the Options tab.
13. Check Verify backup upon completion, and then uncheck Check media set name and backup set expiration.
14. Click OK.
15. Copy the .bak file from your current SolarWinds Orion Platform database server to your new database server.

Creating a Database Backup File with SQL Server Management Studio Express

Complete the following procedure if your new database server uses SQL Server 2005 Express edition.

To backup your Orion database using SQL Server Management Studio Express:

1. Log on to the new database server using an administrator account.
2. Click Start > All Programs > Microsoft SQL Server 2005 > SQL Server Management Studio Express.
3. Specify the name of the current Orion SolarWinds Orion Platform database server on the Connect to Server window.
4. If you are using SQL Server Authentication, click SQL Server Authentication in the Authentication field, and then specify your credentials in the User name and Password fields.
5. Click Connect.
6. Expand the name of your SolarWinds Orion Platform database server, and then expand Databases in the left pane.
7. Right-click the name of your SolarWinds Orion Platform database (for example, right-click ‘NCM_database’), and then click Tasks > Backup.

8. Click Add, and then specify and remember the Destination you provide. This is the directory and name of your backup. For example, you might specify c:\NCM_database.bak.

   Note: Remember, this file is created on the remote database server. It is not created locally.

9. Click Options in the Select a page pane on the left.
10. Check Verify backup when finished.
11. Click OK.
12. Copy the .bak file from your current SolarWinds Orion Platform database server to your new database server.

Creating a Database Backup File with SQL Server Management Studio

Complete the following procedure if your new database server uses SQL Server 2005 or 2008.

To backup your Orion database using SQL Server Management Studio:

1. Log on to the new database server using an administrator account.
2. Click Start > All Programs > Microsoft SQL Server 200X > SQL Server Management Studio.
3. Specify the server name of the current SolarWinds Orion Platform database server on the Connect to Server window.
4. If you are using SQL Server Authentication, click SQL Server Authentication in the Authentication field, and then specify your credentials in the User name and Password fields.
5. Click Connect.
6. In the pane on the left, expand the name of the server hosting the SQL instance you are using for SolarWinds NCM, and then expand Databases.
7. Right-click the name of your SolarWinds Orion Platform database (for example, right-click NCM_database), and then click Tasks > Back Up.
8. In the Source area, select Full as the Backup type.
9. In the Backup set area, provide an appropriate Name and Description for your database backup.
10. If there is not already an appropriate backup location listed in the Destination area, click Add, and then specify and remember the destination path and file name you provide. This is the location where your backup is stored.

Note: Remember, if your database is on a remote server, as recommended, this backup file is also created on the remote database server. It is not created locally.

11. Click Options in Select a page pane on the left.
12. In the Reliability area, check Verify backup when finished.
13. Click OK.
14. Copy the .bak file from your current SolarWinds Orion Platform database server to your new database server.

Restoring Backup Files to SQL Server 2005, 2008, and 2012

The following procedures walk you through the restoration of your SolarWinds Orion Platform database backup file on your new database server.

Restoring a Database Backup File for SQL Server 2005

Restoring a Database Backup File for SQL Server 2008

Restoring a Database Backup File for SQL Server 2012

Restoring a Database Backup File for SQL Server 2005

Complete the following procedure if you are restoring your SolarWinds Orion Platform database backup file to a database server running SQL Server 2005.

To restore your database backup file on a server running SQL Server 2005:

1. Log on to the new database server using an administrator account.
2. Click Start > All Programs > Microsoft SQL Server 2005 > SQL Server Management Studio.
3. Click File > Connect Object Explorer.
4. Specify the name of the new SolarWinds Orion Platform database server on the Connect to Server window.
5. If you are using SQL Server Authentication, click SQL Server Authentication in the Authentication field, and then specify your credentials in the User name and Password fields.
6. Click Connect.
7. Click the name of your server to view an expanded list of objects associated with your server, and then right-click Databases.

8. Click Restore Database.
9. Leave To database blank.
10. Click From device, and then browse (…) to the location of your .bak file.
11. Click Add, and then navigate to the .bak file and click OK.
12. Click OK on the Specify Backup window.
13. Check Restore.
14. Select the name of your database from the To database field. It will now be populated with the correct name. For example, select NCM_database.
15. Click Options in the left Select a page pane.
16. Check Overwrite the existing database.
17. For each Original File Name listed, complete the following steps to ensure a successful restoration:
    a. Click Browse (…).
    b. Select a directory that already exists.
    c. Provide a name for the Restore As file that matches the Original File Name, and then click OK.
18. Select Leave the database ready to use by rolling uncommitted transactions…(RESTORE WITH RECOVERY).
19. Click OK.
20. Open and run the SolarWinds NCM Configuration Wizard to update your SolarWinds NCM installation.
21. Select Database and follow the prompts.

    Note: Due to the nature of security identifiers (SIDs) assigned to SQL Server 2005 database accounts, SolarWinds recommends that you create and use a new account for accessing your restored Orion database on the Database Account window of the Orion Configuration Wizard.

Restoring a Database Backup File for SQL Server 2008

Complete the following procedure if you are restoring your SolarWinds Orion Platform database backup file to a database server running SQL Server 2008.

To restore your database backup file on a server running SQL Server 2008:

1. Log on to the new database server using an administrator account.

2. Click Start > All Programs > Microsoft SQL Server 2008 > SQL Server Management Studio.
3. Click File > Connect Object Explorer.
4. Specify the name of the new SolarWinds Orion Platform database server on the Connect to Server window.
5. If you are using SQL Server Authentication, click SQL Server Authentication in the Authentication field, and then specify your credentials in the User name and Password fields.
6. Click Connect.
7. Click the name of your server to view an expanded list of objects associated with your server, and then right-click Databases.
8. Click Restore Database.
9. Leave To database blank.
10. Select From device, and then click Browse (…).
11. Confirm that File is selected as the Backup media.
12. Click Add.
13. Navigate to the .bak file, select it, and then click OK.
14. Click OK on the Specify Backup window.
15. In the Destination for restore area, select the name of your database from the To database field.

    Note: The To database is now populated with the correct name. For example, select NCM_database.
16. Check Restore next to the database backup you are restoring.
17. Click Options in the left Select a page pane.
18. Check Overwrite the existing database (WITH REPLACE).
19. For each Original File Name listed, complete the following steps to ensure a successful restoration:
    a. Click Browse (…).
    b. Select a directory that already exists.
    c. Provide a name for the Restore As file that matches the Original File Name, and then click OK.
20. Select Leave the database ready to use by rolling uncommitted transactions…(RESTORE WITH RECOVERY), and then click OK.
21. Open and run the SolarWinds NCM Configuration Wizard to update your Orion NPM installation.

22. Select Database and follow the prompts.

    Note: Due to the nature of security identifiers (SIDs) assigned to SQL Server 2008 database accounts, SolarWinds recommends that you create and use a new account for accessing your restored Orion database on the Database Account window of the Orion Configuration Wizard.

Restoring a Database Backup File for SQL Server 2012

Microsoft has fully documented the process and requirements for restoring a database backup file to SQL Server 2012. Due to the number of potential database sources and the fact that the database upgrade itself is automatic, consult the Microsoft article, "Restore a Database backup (SQL Server Management Studio)" for fully detailed requirements and instructions.

Updating SolarWinds NCM to Use the New Database Server

After you have restored your SolarWinds Orion Platform database backup file, you must update your SolarWinds NCM server to recognize the restored database on the new database server, as shown in the following procedure.

Note: In general, SolarWinds recommends that you use SQL Server Authentication with the `SA` login and password to ensure that SolarWinds NCM can always access your SQL Server database, even when it is hosted remotely on a separate server.

To update SolarWinds NCM to use a new database:

1. Log on to your SolarWinds NCM server.
2. Click Start > All Programs > SolarWinds Network Configuration Manager > SolarWinds NCM Configuration Wizard..
3. Check Database, and then click Next.
4. Specify your new database server in the SQL Server field.
5. If you want to use SQL authentication, check Use SQL Server Authentication, and then provide the appropriate credentials.

    Note: SolarWinds recommends that you use the SA login and password for your database server to ensure that you are able to properly configure the Orion database user account.
6. Click Next.

7. Select Use an existing database, select or type the Existing Database name, and then click Next.
8. If you are prompted to use the existing database, click Yes.
9. Select Create a new account, and then provide a New Account name.

   Notes:

   Creating a new account ensures that SolarWinds NCM has required access to your database.

   The New Account must be a member of the securityadmin server role.

   The sysadmin role and the SA user account are always members of securityadm.
10. Provide and confirm an account Password.
11. Click Next to start database configuration, and then click Finish to exit the Configuration Wizard.

Appendix D

Monitoring SNMP Traps

SNMP traps signal the occurrence of significant events by sending unsolicited SNMP messages to a monitoring device. The SolarWinds Trap Server listens for incoming trap messages on UDP port 161 and then decodes, displays, and stores the messages in the SolarWinds NCM database. The SolarWinds Trap Service allows SolarWinds NCM to receive and process SNMP traps from any type of monitored network device, and, because the SolarWinds Trap Service is multi-threaded, it can handle large numbers of simultaneously incoming traps.

You can view SNMP traps in the Trap Viewer application. The Trap Viewer application allows you to configure trap-specific alerts, to view and search traps, and to apply powerful trap filtering.

Note: When configuring devices to send SNMP traps, confirm that traps are sent to the IP address assigned to the SolarWinds NCM server. To ensure proper configuration, refer to the documentation supplied by the vendor of your devices.

The SNMP Trap Protocol

SNMPv1 (Simple Network Management Protocol) and SNMPv2c, along with the associated Management Information Base (MIB), allow you to take advantage of trap-directed notification. When monitoring a large number of devices, where each device may have a large number of its own connected objects, it can become impractical to request information from every object on every device. Consider having each managed device notify the SolarWinds NCM SNMP Trap Server of any issues without solicitation. In this configuration, a problem device notifies the server by sending a message. This message is known as a trap of the event. After receiving the event, the Trap Viewer displays it, allowing you to choose to take action or automatically trigger an action based on the nature of the event.

Configuring the Trap Viewer

Before you can monitor SNMP traps, the Microsoft SNMP Trap service must be installed and devices must be configure to send traps to the SolarWinds NCM SNMP Trap Server. To ensure proper configuration, refer to the documentation supplied by the vendor of your network devices.

If you want to use the Trap Viewer tool or trigger Real-time configuration change alerts based on traps, ensure the SNMP Trap Service is running. If the SNMP Trap Service is not listed as a running service in the service control manager (`services.msc`), you can enable Simple Network Management Protocol in the Management and Monitoring Tools through Add/Remove Windows Components in the Add/Remove Programs application.

Note: The SNMP port used to monitor traps is UDP port 162.

Trap Viewer Settings

Use the following procedure to start and configure the Trap Viewer.

To start and configure the Trap Viewer:

1. Click Start > All Programs > SolarWinds SolarWinds Network Configuration Manager > SolarWinds NCM SNMP Trap Server.
2. Click File > Settings.
3. Select the General tab on the Trap Server Settings window.
4. Adjust the Maximum number of traps to display in Current Traps view to the number you want.
5. If you want to automatically refresh the Current Traps view, select the appropriate option, and then adjust the refresh rate.
6. Adjust the Retain Trap messages for how many days? to set the length of time traps remain in the database.
7. Select the Displayed Columns tab.
8. Use the arrow keys to select and order the columns of information that you want to see in the Current Traps view.
9. Click the Message Parsing tab.
10. If you do not need the domain name from your trap messages, select Remove Domain Name from DNS Lookups.
11. Note: Selecting this option will remove the domain name from your trap messages, and this will help to reduce the size of the database.

Configuring Trap Viewer Filters and Alerts

The Trap Viewer can be configured to trigger alert actions when trap messages match defined rules. The following steps establish rules to filter trap messages and initiate alert actions as you determine.

To configure Trap Viewer filters and alerts:

1. Click Start > All Programs > SolarWinds SolarWinds Network Configuration Manager > SolarWinds NCM SNMP Trap Server.
2. Click View > Alerts / Filter Rules.
3. If you are creating a new rule, click Add Rule.
4. If you are editing an existing rule, select the rule, and then click Edit Rule.
5. Select the General tab, and then type a Rule Name.
6. Select Enabled to enable the rule.
7. Select appropriate servers from the Apply this Rule to list.
8. Enter the IP addresses or subnets to which this rule applies.

   Note: Use the examples listed on this tab to format the list properly.
9. If you want the rule to be limited to messages from specific hosts, domains, or hostname patterns, click DNS Hostname, and then enter a DNS Hostname Pattern.

   Note: When Use Regular Expressions in this Rule is selected, regular expressions can be used in place of “like” statements. For more information about regular expressions, see “Regular Expression Pattern Matching” on page 371.
10. If you want the rule to be limited to specific community strings or text within a trap message, click Message, and then enter rules Community String Pattern.

    Notes:

    Use the examples listed on this tab to format the list properly.

    When Use Regular Expressions in this Rule is selected, regular expressions can be used in place of “like” statements. For more information about regular expressions, see “Regular Expression Pattern Matching”.
11. Select the Conditions tab, and then generate trigger conditions for rule application in the text field as follows:

    Select appropriate object identifiers and comparison functions from the linked context menus.

Click Browse (…) to insert an or condition, to insert an and condition, or to delete a condition.

For more information about how to configure conditions, see "Configuring Real-time Configuration Change Detection".

12. If you want to limit rule application to within a specific period of time, select the Time of Day tab, select Enable Time of Day checking, enter the time period, and then select days of the week on which to apply the rule.

    Notes:

    Enabling time of day checking creates more overhead for the CPU.

    Messages received outside the specified timeframe will not trigger alerts.

13. If you want to suppress alert actions until a specified number of traps arrive that match the rule, select the Trigger Threshold tab, select Define a Trigger Threshold for this Rule, and then enter option values as appropriate.

    Note: When Suspend further Alert Actions for is selected, alert actions are not sent until the specified amount of time has expired. Once the time period has expired, only new alerts are sent. All alerts that are suppressed during the time period are discarded.

14. Select the Alert Actions tab.
15. If you are associating a new action to the rule, click Add New Action, and then select an action from the list to configure. For more information about alert actions, see "Available Trap Alert Actions" on page 391.
16. If you are editing an existing action for the rule, select an action from the list, click Edit Action, and then configure the action. For more information about alert actions, see "Available Trap Alert Actions" on page 391.
17. Use the arrow buttons to arrange the order in which actions are performed.

    Note: Actions are processed in the order that they appear in this list, from top to bottom.

18. If you need to delete an action, select the action, and then click Delete Action.
19. Click OK to save all changes and return to Trap Viewer Settings.
20. Use the arrow buttons to arrange the order in which the rules are applied.

    Note: Rules are processed in the order they appear, from top to bottom.

Available Trap Alert Actions

The following list provides definitions of the actions available for each trap alert type. For more information about how to assign alert actions, see “Configuring Trap Viewer Filters and Alerts” on page 389.

Discard the Trap

Allows you to delete unwanted traps sent to the SNMP Trap server.

Tag the Trap

Allows you to add a custom tag to received traps. Ensure you include the Tag column in the viewer when assigning a tag.

Flag the Trap with a specific color

Allows you to assign a specific color to flag traps matching the rule.

Log the Trap to a file

Allows you to specify a file and a series of variables with which to tag traps sent to the file. Ensure you have already created the log file you want to use. The alert cannot create a file.

Windows Event Log

Allows you to write a message to the local Windows Event Log or to a remote Windows Event Log.

Forward the Trap

Allows you to specify the IP address or hostname and the port on which to forward the trap.

Play a sound

Allows you to play a sound when a matching SNMP trap is received.

Text to Speech output

Allows you to define a specific speech engine, the speed, pitch, volume, and message to read.

Execute an external program

Allows you to specify an external program to launch. This action is used when creating Real-time change notifications in SolarWinds NCM.

Execute an external VB Script

Allows you to launch a VB Script using the selected script interpreter engine and a saved script file.

Send a Windows Net Message

Allows you to send a net message to a specific computer or an entire domain or workgroup.

Send an E-mail / Page

Allows you to send an email from a specified account to a specified address, using a specific SMTP server, and containing a customizable subject and message.

Stop Processing Trap Rules

Stops the processing of SNMP trap rules for the matching trap.

Working with Traps

Trap Viewer collects traps from your network and presents them in a readily reviewable and searchable list so that you can easily monitor network health. The following sections provide a guide to working with trap messages within the Trap Viewer.

Viewing Current Traps

Trap Viewer makes it easy to view trap messages.

To view current trap messages:

1. Start > All Programs > SolarWinds Orion > Trap Viewer.
2. Click View > Current Traps.

Searching for Traps

Collected trap messages may be searched within Trap Viewer. The following steps search for trap messages and format the search results list.

To search the trap message list:

1. Click Start > All Programs > SolarWinds SolarWinds Network Configuration Manager > SolarWinds NCM SNMP Trap Server.
2. Click View > Search Traps.
3. Enter appropriate search criteria, and then click Search Database.
4. If you want to group messages for easier navigation, select the type of grouping from the Grouping list.
5. If you want to limit the number of messages that are shown, enter or select a number in the Maximum number of messages to display field.

6. If you want to view messages that meet your search criteria as they arrive, select a number for the Auto Refresh every number seconds field.

   Note: Auto Refresh is only available when you are viewing current messages. The Date/Time Range must be set to Today, Last 24 Hours, Last 2 Hours, or Last Hour.

Trap Alert Variables

The following variables can be used in trap alert messages with the SolarWinds NCM Trap Server. You must begin each variable with a dollar sign and enclose each variable identifier in curly braces as, for example, `${`*`VariableName`*`}`.

Trap Date/Time Variables

Trap Date/Time Variable	**Description**
${AbreviatedDOW}	Current day of the week. Three character abbreviation.
${AbreviatedMonth}	Current month of the year. Three character abbreviation.
${AMPM}	AM or PM corresponding to current time (before or after noon)
${D}	Current day of the month
${DD}	Current day of the month (two digit number, zero padded)
${Date}	Current date. (MM/DD/YYYY format)
${DateTime}	Current date and time. (MM/DD/YYYY HH:MM format)
${Day}	Current day of the month
${DayOfWeek}	Current day of the week.
${DayOfYear}	Numeric day of the year
${H}	Current hour
${HH}	Current hour. Two digit format, zero padded.
${Hour}	Current hour. 24-hour format
${LocalDOW}	Current day of the week. Localized language format.
${LongDate}	Current date. (DAY NAME, MONTH DAY, YEAR format)
${LongTime}	Current Time. (HH:MM:SS AM/PM format)
${M}	Current numeric month
${MM}	Current month. Two digit number, zero padded.
${MMM}	Current month. Three character abbreviation.
${MMMM}	Full name of the current month

Trap Date/Time Variable	Description
${MediumDate}	Current date. (DD-MMM-YY format)
${MediumTime}	Current time. (HH:MM AM/PM format)
${Minute}	Current minute. Two digit format, zero padded.
${MonthName}	Full name of the current month
${S}	Current second.
${Second}	Current second. Two digit format, zero padded.
${Time}	Current Time. (HH:MM format)
${Year}	Four digit year
${Year2}	Two digit year

Other Trap Variables

Trap Variable	Description
${Application}	SolarWinds application information
${Community}	Node community string
${Copyright}	Copyright information
${DNS}	Fully qualified node name
${IP }	IP address of device triggering alert

Appendix E

Monitoring Syslog Messages

Syslog messages are Real-time messages network devices generate to notify you about specific device events. The SolarWinds Syslog Service allows you to receive and process Syslog messages from any type of network device. Because the SolarWinds Syslog Service has the ability to open multiple connections, it can handle large numbers of simultaneously incoming Syslog messages.

The Syslog Server allows you to view, acknowledge, and alert on Syslog messages you receive. By utilizing the built-in flexible message filtering, you can easily create message-specific alerts.

Note: When configuring network devices to send Syslog messages, confirm that messages are sent to the IP address assigned on which the Syslog Server is installed. To ensure proper configuration, refer to the documentation supplied by the vendor for each network device.

Understanding the Syslog Protocol

The Syslog service listens for incoming Syslog messages on UDP port 514 and then decodes, displays, and stores the message in a database. Many network devices can be configured to generate Syslog messages, allowing you to receive and process the messages generated by these network devices. For details on enabling Syslog message on a particular device, refer to the vendor's documentation.

Syslog Priorities

Included at the beginning of each Syslog message is a priority value. The priority value range spans between 0 and 191 and is enclosed in angle bracket (< and >) delimiters. The priority value is calculated using the following formula:

```
Priority = Facility * 8 + Severity
```

Syslog Facilities

The facility value is used to determine which process of the machine created the message. Since the Syslog protocol was originally written on BSD Unix, the

Facilities reflect the names of UNIX processes and daemons. The following tables list Syslog facilities and levels.

Number	Source	Number	Source
0	kernel messages	12	NTP subsystem
1	user-level messages	13	log audit
2	mail system	14	log alert
3	system daemons	15	clock daemon
4	security/authorization messages	16	local use 0 (local0)
5	messages generated internally by Syslog	17	local use 1 (local1)
6	line printer subsytem	18	local use 2 (local2)
7	network news subsytem	19	local use 2 (local3)
8	UUCP subsystem	20	local use 2 (local4)
9	clock daemon	21	local use 2 (local5)
10	security/authorization messages	22	local use 2 (local6)
11	FTP daemon	23	local use 2 (local7)

Note: If you are receiving messages from a UNIX system, consider using the `User` Facility as your first choice. Local0 through Local7 are not used by UNIX and are traditionally used by networking equipment. Cisco routers, for example, use Local6 or Local7.

Syslog Severities

The following table provides a list of Syslog severity levels with descriptions and suggested actions for each.

Number	Severity	Suggested Actions
0	Emergency	A "panic" condition affecting multiple applications, servers, or sites. System is unusable. Notify all technical staff on call.
1	Alert	A condition requiring immediate correction, for example, the loss of a backup ISP connection. Notify staff who can fix the problem.
2	Critical	A condition requiring immediate correction or indicating a failure in a primary system, for example, a loss of a primary ISP connection. Fix CRITICAL problems before ALERT-level problems.
3	Error	Non-urgent failures. Relay errors to developers or administrators. Each item must be resolved within a given time.
4	Warning	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.
5	Notice	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.
6	Informational	Normal operational messages. These may be harvested for network maintenance functions like reporting and throughput measurement. No action is required.
7	Debug	Information useful to developers for debugging an application. This information is not useful during operations.

Configuring Syslog Server

You can use the Syslog Server application for viewing, acknowledging, and triggering alerts in response to Syslog messages on your network.

Syslog Server Settings

Use the following procedure as a guide to starting and configuring the Syslog Server.

To start and configure the Syslog Server:

1. Click Start > All Programs > SolarWinds SolarWinds Network Configuration Manager > Syslog Viewer.
2. Click File > Settings.
3. Select the General tab in the Syslog Server Settings window.
4. Adjust the Maximum number of messages to display in Current Messages view to show the number of messages you want.
5. If you want to Automatically Refresh the Current Messages View, select the option accordingly, and then position the middle slider to set the refresh rate.
6. Adjust Retain Syslog messages for how many days? to set the length of time Syslog messages should stay in the database.
7. Select the Displayed Columns tab, and then use the arrow keys to select and order the fields of information that you want to see in the Current Messages view.

   Note: You can make it easier to acknowledge Syslog messages by selecting the Acknowledged column to add to your view. For more information, see “Viewing and Acknowledging Current Messages” on page 403.
8. If you want to wrap Syslog messages text in the Current Messages view, select Word wrap long messages.
9. If you do not expect to use Syslog Server as your primary viewer for Syslog messages, select the Message Parsing tab, and then complete the following steps:

   Note: The following data points are saved within the Syslog tables in your SolarWinds NCM database, removing the added data from each record helps you proactively reduce the size of your database.

a. Select Remove embedded Date/Time from Syslog Messages.

b. Select Remove Message Type from Syslog Messages.

c. Select Remove Domain Name from DNS Lookups.

Configuring Syslog Viewer Filters and Alerts

The Syslog Viewer can be configured to signal Orion N alert actions when Syslog messages that are received from network devices match defined rules. The steps in the following procedure establish rules that filter Syslog messages and initiate alert actions as you determine.

To configure Syslog Viewer filters and alerts:

1. Click Start > All Programs > SolarWinds SolarWinds Network Configuration Manager > Syslog Viewer.
2. Click File > Settings.
3. Click View > Alerts/Filter Rules.
4. If you are creating a new rule, click Add New Rule.
5. If you are editing an existing rule, select the rule, and then click Edit Rule.
6. Select the General tab.
7. Type a Rule Name, and then select Enabled to enable the rule.
8. Select appropriate servers from the Apply this Rule to list.
9. Enter the IP addresses or subnets to which this rule applies.

   Note: Use the examples listed on this tab to properly format the list.
10. If you want to limit the rule to only messages from specific hosts, domains, or hostname patterns, select the DNS Hostname tab, and then enter a DNS Hostname Pattern.

    Note: When Use Regular Expressions in this Rule is selected, regular expressions can be used in place of “like” statements. For more information about regular expressions, see “Regular Expression Pattern Matching” on page 371.
11. If you want to limit the rule to only specific message types or text within a Syslog message, select the Message tab, and then enter rules for one or both of Message Type Pattern and Syslog Message Pattern.

    Notes:

    Use the examples listed on this tab to format the list properly.

When Use Regular Expressions in this Rule is selected, regular expressions can be used in place of “like” statements. For more information about regular expressions, see “Regular Expression Pattern Matching” on page 371.

12. Select the Severity / Facility tab, and then select the severity and facility types you want to apply.

    Note: By default, all message severities and facilities are selected.

13. If you want to limit rule application to within a specific period of time, select the Time of Day tab, select Enable Time of Day checking, enter the time period, and then select days of the week on which to apply the rule.

    Notes:

    Enabling Time of Day checking creates more overhead for the CPU.

    Messages received outside the specified timeframe will not trigger alerts.

14. If you want to suppress alert actions until a specified number of messages arrive that match the rule, complete the following procedure:

    a. Select the Trigger Threshold tab.

    b. Select Define a Trigger Threshold for this Rule.

    c. Enter option values as appropriate.

    Note: When Suspend further Alert Actions for is selected, alert actions are not sent until the specified amount of time has expired. Once the time period has expired, only new alerts are sent. All alerts suppressed during the time period are discarded.

15. Select the Alert Actions tab.

16. If you are associating a new action to the rule, click Add New Action, and then select an action from the list to configure. For more information about available actions, see “Available Syslog Alert Actions” on page 401.

    Note: Syslog alerts use a unique set of variables. For more information about available Syslog variables, see “Syslog Alert Variables” on page 404.

17. If you are editing an existing action for the rule, complete the following steps:

a. Select an action from the list.

b. Click Edit Selected Action.

c. Configure the action as appropriate. For more information about available actions, see “Available Syslog Alert Actions” on page 401.

Note: Syslog alerts use a unique set of variables. For more information about available Syslog variables, see “Syslog Alert Variables” on page 404.

18. If you need to delete an action, select the action, and then click Delete Action.
19. Use the arrow buttons to arrange the order in which actions are performed.

    Note: Actions are processed in the order that they appear in this list, from top to bottom.
20. Click OK to save all changes and return to Syslog Viewer Settings.
21. Use the arrow buttons to arrange the order in which the rules are applied.

    Note: Rules are processed in the order they appear, from top to bottom.

Available Syslog Alert Actions

The following list provides definitions of the actions available for each Syslog alert type. For more information about how to assign alert actions, see “Configuring Syslog Viewer Filters and Alerts” on page 399.

Discard the Syslog Message

Allows you to delete unwanted Syslog messages sent to the Syslog server.

Tag the Syslog Message

Allows you to add a custom tag to received Syslog messages. Ensure you include the Tag column in the viewer when assigning a tag.

Modify the Syslog Message

Allows you to modify severity, facility, type and contents of a Syslog message.

Log the Message to a file

Allows you to specify a file and a series of variables with which to tag Syslog messages sent to the file. Ensure you have already created the log file you want to use. The alert cannot create a file.

Windows Event Log

Allows you to write a message to the local Windows Event Log or to a remote Windows Event Log.

Forward the Syslog message

Allows you to specify the IP address or hostname and the port on which to forward the Syslog event.

Send a new Syslog message

Allow you to trigger a new Syslog message to a specific IP address or hostname, on a specific port, with a customizable severity, facility, and message.

Send an SNMP Trap

Allows you to send a trap to an IP address following a specific trap template and using a specific SNMP community string.

Play a sound

Allows you to play a sound when a matching Syslog message is received.

Text to Speech output

Allows you to define a specific speech engine, the speed, pitch, volume, and message to read.

Execute an external program

Allows you to specify an external program to launch. This action is used when creating Real-time change notifications in SolarWinds NCM.

Execute an external VB Script

Allows you to launch a VB Script using the selected script interpreter engine and a saved script file.

Send a Windows Net Message

Allows you to send a net message to a specific computer or an entire domain or workgroup.

Send an E-mail / Page

Allows you to send an email from a specified account to a specified address, using a specific SMTP server, and containing a customizable subject and message.

Stop Processing Syslog Rules

Stops the processing of Syslog rules for the matching Syslog message.

Using Syslog Server

Syslog Server collects Syslog messages from your network and presents them in a readily reviewable and searchable list so that you can easily monitor your network. The following sections provide a guide to working with Syslog messages within the Syslog Server application.

Viewing and Acknowledging Current Messages

The main Syslog Server window, Syslog Viewer, makes it easy to view and acknowledge messages. The following procedure views and then acknowledges current Syslog messages.

To view and acknowledge current Syslog messages:

1. Click View > Current Messages.
2. Acknowledge current messages by either of the following methods:

   Right-click any message, and then select Acknowledge Selected.

Add an Acknowledged column to the Syslog Viewer, and then select each message that you want to acknowledge. For more information, see “Syslog Server Settings” on page 398.

Searching for Syslog Messages

Collected Syslog messages may be searched within Syslog Viewer. The following steps both search for Syslog messages and format search results.

To search the Syslog message list:

1. Click View > Search Messages.
2. Enter appropriate search criteria, and then click Search Database.
3. If you want to group messages for easier navigation, select the type of grouping from the Grouping list.

   Note: Messages can be acknowledged in the search results just as they can be acknowledged in the Current Messages view. For more information, see “Viewing and Acknowledging Current Messages” on page 403.
4. If you want to limit the number of messages that are shown, enter or select a number in the Maximum number of messages to display field.

5. If you want to view messages that meet your search criteria as they arrive, select a number for the Auto Refresh every number seconds field.

   Note: Auto Refresh is only available when you are viewing current messages. The Date/Time Range must be set to Today, Last 24 Hours, Last 2 Hours, or Last Hour.

Syslog Alert Variables

The following variables can be used in Syslog alert messages. You must begin each variable with a dollar sign and enclose each variable identifier in curly braces as, for example, `${`*`VariableName`*`}`.

Syslog Date/Time Variables

Syslog Date/Time Variable	**Description**
${AbreviatedDOW}	Current day of the week. Three character abbreviation.
${AMPM}	AM or PM corresponding to current time (before or after noon)
${D}	Current day of the month
${DD}	Current day of the month (two digit number, zero padded)
${Date}	Current date. (Short Date format)
${DateTime}	Current date and time. (Windows control panel defined “Short Date” and “Short Time” format)
${DayOfWeek}	Current day of the week.
${DayOfYear}	Numeric day of the year
${H}	Current hour
${HH}	Current hour. Two digit format, zero padded.
${Hour}	Current hour. 24-hour format
${LocalDOW}	Current day of the week. Localized language format.
${LongDate}	Current date. (Long Date format)
${LocalMonthName}	Current month name in the local language.
${LongTime}	Current Time. (Long Time format)
${M}	Current numeric month
${MM}	Current month. Two digit number, zero padded.
${MMM}	Current month. Three character abbreviation.
${MediumDate}	Current date. (Medium Date format)
${Minute}	Current minute. Two digit format, zero padded.

Syslog Date/Time Variable	Description
${Month}	Full name of the current month
${N}	Current month and day
${S}	Current second.
${Second}	Current second. Two digit format, zero padded.
${Time}	Current Time. (Short Time format)
${Year2}	Two digit year
${Year}	Four digit year

Other Syslog Variables

Syslog Variable	Description
${Application}	SolarWinds application information
${Copyright}	Copyright information
${DNS}	Fully qualified node name
${Hostname}	Host name of the device triggering the alert
${IP_Address}	IP address of device triggering alert
${Message}	Status of device triggering alert
${MessageType}	Assigned alert name
${Release}	Release information
${Severity}	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.
${Version}	Version of the SolarWinds software package

Appendix F

Orion Variables and Examples

SolarWinds NCM product components, including the Advanced Alert Manager, both the Traps Viewer and 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. For example, the variable `${ResponseTime}` will parse with the current response time of the node that is triggering the alert.

Note: In some cases, the database table name may be required for alert variables, as in `${Nodes.CPULoad}`. If a variable does not respond as intended, include the relevant table name for the desired variable.

Variable Modifiers

The variables in the following sections can be modified by appending any of the variable modifiers in the following table.

Variable Modifier	Description
-Raw	Displays the raw value for the statistic. For example, if Transmit Bandwidth is set to 10 Mbps, then the raw value would be“10000000”. The cooked value would be “10 Mbps”.
-Previous	Displays the previous value for the statistic before the Alert was triggered
-Cooked	Displays the cooked value for the statistic. For example, if Transmit Bandwidth is set to 10 Mbps, then the raw value would be “10000000” and cooked value would be “10 Mbps”.
-PreviousCooked	Displays the previous cooked value for the statistic before the Alert was triggered

Advanced Alert Engine Variables

The following variables can be used in alert messages within SolarWinds NCM and Orion Modules. You must begin each variable with a dollar sign and enclose each variable identifier in braces as, for example, `${ObjectName}`.

General

The following are valid, general advanced alert variables.

General Variable	Description
${Acknowledged}	Acknowledged status
${AcknowledgedBy}	Who the alert was acknowledged by
${AcknowledgedTime}	Time the alert was acknowledged
${AlertTriggerCount}	Count of triggers
${AlertTriggerTime}	Date and time of the last event for this Alert. (Windows control panel defined “Short Date” and “Short Time”)
${Application}	SolarWinds application information
${CR}	Line Feed – Carriage Return
${Copyright}	Copyright information
${ObjectName}	Description/Name of the object in the alert
${Release}	Release information
${Version}	Version of the SolarWinds software package

Date/Time

The following are valid date and time variables.

Date/Time Variable	Description
${AMPM}	AM/PM indicator
${AbreviatedDOW}	Current day of the week. Three character abbreviation.
${D}	Current day of the month
${DD}	Current day of the month (two digit number, zero padded)
${Date}	Current date. (Short Date format)
${DateTime}	Current date and time. (Windows control panel defined “Long Date” and “Long Time” format)
${DayOfWeek}	Current day of the week.
${DayOfYear}	Numeric day of the year
${H}	Current hour
${HH}	Current hour. Two digit format, zero padded.
${Last2Hours}	Last two hours
${Last24Hours}	Last 24 hours
${Last7Days}	Last seven days (Short Date format)
${LastHour}	Last hour
${LocalDOW}	Current day of the week. Localized language format.
${LocalMonthName}	Current month name in the local language.
${LongDate}	Current date. (Long Date format)
${M}	Current numeric month
${MM}	Current month. Two digit number, zero padded.
${MMM}	Current month. Three character abbreviation.
${MMMM}	Full name of the current month
${MediumDate}	Current date. (Medium Date format)
${Minute}	Current minute. Two digit format, zero padded.
${S}	Current second.
${Second}	Current second. Two digit format, zero padded.
${Time}	Current Time. (Short Time format)
${Today}	Today (Short Date format)
${Year}	Four digit year
${Year2}	Two digit year
${Yesterday}	Yesterday (Short Date format)

Group Variables

The following are valid group variables.

Group Variable	Description
${GroupDetailsURL}	URL of the Group Details view for a selected group
${GroupFrequency}	Interval on which group membership is evaluated and group snapshots are taken.
${GroupID}	Designated identifier for a defined group
${GroupMemberDisplayName}	Display name of group member type: Node, Volume, Component, Application, etc.
${GroupMemberDisplayNamePlural}	Display name of multiple group members of a type: Nodes, Components, Applications, etc.
${GroupMemberFullName}	Full name of a group member, including location
${GroupMemberName}	Name of a group member
${GroupMemberPercentAvailability}	Percent availability of a group member when group member status is Up, Warning, or Critical and 0% if status is anything else.
${GroupMemberSnapshotID}	Unique identifier of group member snapshot.
${GroupMemberStatusID}	Identifier assigned to a group member indicating its status. For more information see “Status Variables” on page 410.
${GroupMemberStatusName}	Name of group member status. For more information see “Status Variables” on page 410.
${GroupMemberUri}	Uri used by SolarWinds Information Service (SWIS) to refer to the selected group member within the web console.
${GroupName}	Name of the group.
${GroupOwner}	Orion Platform product appropriate to the group type
${GroupPercentAvailability}	100% when group status is Up, Warning, Critical and 0% if status is anything else.
${GroupStatusCalculatorID}	Name of roll-up logic calculator that evaluates status of group based on member statuses. (`0` = Mixed, `1` = Worst, `2` = Best)
${GroupStatusCalculatorName}	Name of roll-up logic calculator that evaluates status of group based on member statuses. (`Mixed`, `Worst`, `Best`)
${GroupStatusID}	Identifier assigned to a group indicating its status. For more information see “Status Variables” on page 410.
${GroupStatusName}	Name of group status. For more information see “Status Variables” on page 410.
${GroupStatusRootCause}	A list of all group members that are not Up
${NodeID}	NULL every time - just for legacy support.

SQL Query

Any value you can collect from the database can be generated, formatted, or calculated using a SQL query as a variable. To use a SQL query as a variable in SolarWinds NCM, use `${SQL:{query}}` as shown in the following example that returns the results of the SQL query `Select Count(*) From Nodes`:

```
${SQL:Select Count(*) From Nodes}
```

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.

Status Value	Description
0	Unknown
1	Up
2	Down
3	Warning
4	Shutdown
5	Testing
6	Dormant
7	Not Present
8	Lower Layer Down
9	Unmanaged
10	Unplugged
11	External
12	Unreachable
14	Critical
15	Mixed Availability
16	Misconfigured
17	Could Not Poll
19	Unconfirmed
22	Active
24	Inactive
25	Expired
26	Monitoring Disabled
27	Disabled
28	Not Licensed

Node Variables

The following are valid node variables.

Node Variable	Description
${AgentPort}	Node SNMP port number
${Allow64BitCounters}	Node allows 64-bit counters (1), or not (0)
${AvgResponseTime}	Average node response time , in msec, to ICMP requests
${BlockUntil}	Day, date, and time until which node polling is blocked
${BufferBgMissThisHour}	Device-dependent count of big buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.30
${BufferBgMissToday}	Device-dependent count of big buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.30
${BufferHgMissThisHour}	Device-dependent count of huge buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.62
${BufferHgMissToday}	Device-dependent count of huge buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.62
${BufferLgMissThisHour}	Device-dependent count of large buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.38
${BufferLgMissToday}	Device-dependent count of large buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.38
${BufferMdMissThisHour}	Device-dependent count of medium buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.22
${BufferMdMissToday}	Device-dependent count of medium buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.22
${BufferNoMemThisHour}	Count of buffer errors due to low memory on node in current hour
${BufferNoMemToday}	Count of buffer errors due to low memory on node in current day
${BufferSmMissThisHour}	Device-dependent count of small buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.14
${BufferSmMissToday}	Device-dependent count of small buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.14
${Caption}	User friendly node name
${Community}	Node community string
${Contact}	Contact information for person or group responsible for node
${CPULoad}	Node CPU utilization rate at last poll
${CustomPollerLastStatisticsPoll}	Day, date, and time of last poll attempt on node

Node Variable	Description
${CustomPollerLastStatisticsPollSuccess}	Day, date, and time that node was last successfully polled
${Description}	Node hardware and software
${DNS}	Fully qualified node name
${DynamicIP}	If node supports dynamic IP address assignment via BOOTP or DHCP (1); static IP address return (0)
${EngineID}	Internal unique identifier of the polling engine to which node is assigned
${GroupStatus}	Filename of status icon for node and, in SolarWinds NPM, its interfaces
${IOSImage}	Family name of Cisco IOS on node
${IOSVersion}	Cisco IOS version on node
${IP_Address}	Node IP address
${LastBoot}	Day, date and time of last node boot
${LastSync}	Time and date of last node database and memory synchronization
${Location}	Physical location of node
${MachineType}	Node manufacturer or distributor and family or version information
${MaxResponseTime}	Maximum node response time , in msec, to ICMP requests
${MemoryUsed}	Total node memory used over polling interval
${MinResponseTime}	Minimum node response time , in msec, to ICMP requests
${NextPoll}	Day, date and time of next scheduled node polling
${NextRediscovery}	Time of next node rediscovery
${NodeID }	Internal unique identifier of node
${ObjectSubType}	States if node supports SNMP or is ICMP-only
${PercentLoss}	ICMP packet loss percentage when node last polled
${PercentMemoryUsed}	Percentage of total node memory used over polling interval
${PollInterval}	Node polling interval, in seconds
${RediscoveryInterval}	Node rediscovery interval, in minutes
${ResponseTime}	Node response time, in milliseconds, to last ICMP request
${RWCommunity}	Node read/write community string; acts as security code for read/write SNMP access
${RWSNMPV3AuthKey}	SNMPv3 read/write credential authentication key
${RWSNMPV3AuthKeyIsPwd}	States if the SNMPv3 read/write credential authentication key is the password

Node Variable	Description
${RWSNMPV3AuthMethod}	SNMPv3 read/write credential authentication method
${RWSNMPV3Context}	SNMPv3 read/write security context information
${RWSNMPV3PrivKey}	SNMPv3 read/write credential key
${RWSNMPV3PrivKeyIsPwd}	States if the SNMPv3 read/write credential privacy key is the password
${RWSNMPV3PrivMethod}	SNMPv3 read/write credential privacy encryption method
${RWSNMPV3Username}	User friendly name for SNMPv3 read/write credential
${Severity}	A network health score determined additively by scoring the status of monitored objects. In Orion 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 Orion APM, 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.
${SNMPV2Only}	States if node only supports SNMPv1 or SNMPv2
${SNMPV3AuthKey}	SNMPv3 authentication key
${SNMPV3AuthKeyIsPwd}	States if node SNMPv3 authentication key is password
${SNMPV3AuthMethod}	SNMPv3 authentication type
${SNMPV3Context}	Group or domain of user with SNMPv3 access to node
${SNMPV3PrivKey}	SNMPv3 credential key
${SNMPV3PrivKeyIsPwd}	States if node SNMPv3 credential key is the password
${SNMPV3PrivMethod}	SNMPv3 credential key type
${SNMPV3Username}	User friendly name for SNMPv3 credential
${SNMPVersion}	States the version of SNMP used by the node
${StatCollection}	Statistics collection frequency, in minutes
${Status}	Numerical node status. For more information, see “Node Status Variables” on page 410.
${StatusDescription}	User friendly node status
${StatusLED}	Filename of node status icon
${SysName}	String reply to SNMP SYS_NAME OID request
${SysObjectID}	Vendor ID of the network management subsystem in OID form. Clearly determines the type of node.
${SystemUpTime}	Time, in hundredths of a second, since network monitoring started

Node Variable	Description
${TotalMemory}	Total node memory available
${UnManaged}	States if node is currently unmanaged
${UnManageFrom}	Day, date, and time when node is set to “Unmanaged”
${UnManageUntil}	Day, date, and time when node is scheduled to be managed
${Vendor}	Node manufacturer or distributor
${VendorIcon}	Filename of node vendor logo

Volume Variables

The following are valid volume variables.

Volume Variable	Description
${Caption}	User friendly volume name
${FullName}	User friendly volume name including captions of parent node and, in SolarWinds NPM, interface
${LastSync}	Time and date volume last synchronized in database and memory models
${NextPoll}	Day, date and time of next scheduled volume polling
${NextRediscovery}	Scheduled time of next volume rediscovery
${NodeID}	Internal unique identifier of parent node
${PollInterval}	Volume status polling interval, in seconds
${RediscoveryInterval}	Volume rediscovery interval, in minutes
${StatCollection}	Statistics collection frequency, in minutes
${Status}	Numerical volume status: (0=”Unknown”, 1=”Up”, 2=”Shutdown”, 3=”Testing”)
${StatusLED}	Filename of volume status icon
${VolumeAllocationFailuresThisHour}	Number of volume allocation errors for this volume in last hour
${VolumeAllocationFailuresToday}	Number of volume allocation errors for this volume in current day
${VolumeDescription}	User friendly volume description
${VolumeID}	Internal unique identifier of volume
${VolumeIndex}	Unique index of this volume within the parent node
${VolumePercentUsed}	Percentage of volume currently in use
${VolumeResponding}	(Y) = volume is currently responding to SNMP queries
${VolumeSize}	Size of volume, in bytes
${VolumeSpaceAvailable}	Total space available on volume, in bytes
${VolumeSpaceUsed}	Total space used on volume, in bytes
${VolumeType}	Volume type, as reported by hrStorageType OID (Removable Disk/Fixed Disk/Compact Disc/Virtual Memory/RAM/etc)
${VolumeTypeIcon}	Filename of icon for volume type

Example Messages Using Variables

The following examples illustrate some of the uses of variables.

- `Previous reboot was at ${LastBoot-Previous}.`
- `Alert: ${NodeName} has exceptionally high response time. Average Response Time is ${AvgResponseTime} and is varying from ${MinResponseTime} to ${MaxResponseTime}.`
- `Current packet loss for ${NodeName} is ${%Loss}. Average Response time is ${AvgResponseTime} and is varying from ${MinResponseTime} to ${MaxResponseTime}.`
- `Alert: The SNMP Community string used to query ${NodeName} has been changed from ${Community-Previous} to ${Community}.`
- `SolarWinds NCM uses the new Community String to query ${NodeName}.`

Syslog Alert Variables

The following variables can be used in Syslog alert messages within SolarWinds Network Configuration Manager applications. You must begin each variable with a dollar sign and enclose each variable identifier in curly braces as, for example, `${ObjectName}`.

Syslog Date/Time Variables

Syslog Date/Time Variable	Description
${AbreviatedDOW}	Current day of the week. Three character abbreviation.
${AMPM}	AM or PM corresponding to current time (before or after noon)
${D}	Current day of the month
${DD}	Current day of the month (two digit number, zero padded)
${Date}	Current date. (Short Date format)
${DateTime}	Current date and time. (Windows control panel defined “Short Date” and “Short Time” format)
${DayOfWeek}	Current day of the week.
${DayOfYear}	Numeric day of the year
${H}	Current hour
${HH}	Current hour. Two digit format, zero padded.
${Hour}	Current hour. 24-hour format
${LocalDOW}	Current day of the week. Localized language format.
${LongDate}	Current date. (Long Date format)
${LocalMonthName}	Current month name in the local language.
${LongTime}	Current Time. (Long Time format)
${M}	Current numeric month
${MM}	Current month. Two digit number, zero padded.
${MMM}	Current month. Three character abbreviation.
${MediumDate}	Current date. (Medium Date format)
${Minute}	Current minute. Two digit format, zero padded.
${Month}	Full name of the current month
${N}	Current month and day
${S}	Current second.
${Second}	Current second. Two digit format, zero padded.
${Time}	Current Time. (Short Time format)
${Year2}	Two digit year
${Year}	Four digit year

Other Syslog Variables

Syslog Variable	Description
${Application}	SolarWinds application information
${Copyright}	Copyright information
${DNS}	Fully qualified node name
${IP_Address}	IP address of device triggering alert
${Message}	Status of device triggering alert
${MessageType}	Assigned alert name
${Release}	Release information
${Severity}	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.
${Version}	Version of the SolarWinds software package

Trap Alert Variables

The following variables can be used in trap alert messages within Orion Platform products.

General Trap Variables

Trap Variable	Description
${Application}	SolarWinds application information
${Community}	Node community string
${Copyright}	Copyright information
${DNS}	Fully qualified node name
${Hostname}	Host name of the device triggering the trap
${IP}	IP address of device triggering alert
${IP_Address}	IP address of device triggering alert
${Message}	Message sent with triggered trap and displayed in Trap Details field of Trap Viewer
${MessageType}	Name or type of trap triggered
${Raw}	Raw numerical values for properties sent in the corresponding incoming trap
${RawValue}	Raw numerical values for properties sent in the corresponding incoming trap. The same as ${Raw}

Trap Date/Time Variables

Trap Date/Time Variable	Description
${AbbreviatedDOW}	Current day of the week. Three character abbreviation.
${AbbreviatedMonth}	Current month of the year. Three character abbreviation.
${AMPM}	AM or PM corresponding to current time (before or after noon)
${D}	Current day of the month
${DD}	Current day of the month (two digit number, zero padded)
${Date}	Current date. (MM/DD/YYYY format)
${DateTime}	Current date and time. (MM/DD/YYYY HH:MM format)
${Day}	Current day of the month
${DayOfWeek}	Current day of the week.
${DayOfYear}	Numeric day of the year
${H}	Current hour
${HH}	Current hour. Two digit format, zero padded.
${Hour}	Current hour. 24-hour format
${LocalDOW}	Current day of the week. Localized language format.
${LongDate}	Current date. (DAY NAME, MONTH DAY, YEAR format)
${LongTime}	Current Time. (HH:MM:SS AM/PM format)
${M}	Current numeric month
${MM}	Current month. Two digit number, zero padded.
${MMM}	Current month. Three character abbreviation.
${MMMM}	Full name of the current month
${MediumDate}	Current date. (DD-MMM-YY format)
${MediumTime}	Current time. (HH:MM AM/PM format)
${Minute}	Current minute. Two digit format, zero padded.
${MonthName}	Full name of the current month
${S}	Current second.
${Second}	Current second. Two digit format, zero padded.
${Time}	Current Time. (HH:MM format)
${Year}	Four digit year
${Year2}	Two digit year

Appendix G

Creating Custom Properties

Along with all other SolarWinds Orion Platform products, SolarWinds NCM now uses a web-based version of the Custom Property Editor.

NCM only supports custom properties written in English.

The following sections provide steps required to manage custom properties.

- Creating a Custom Property
- Assigning Values to a Custom Property
- Importing Custom Property Data
- Removing Custom Properties
- Exporting a Custom Property

Notes:

- Older versions of SolarWinds Orion Core Services used the Custom Property Editor application to create and manage custom properties. The Custom Property Editor is no longer available NCM version 7.1.1 and higher..
- Custom properties are stored in the SolarWinds database. SQL Server treats `NULL` and `0` differently, so, if you are creating a custom property to trigger an alert, confirm that the alert trigger conditions account for this difference. For more information, see the SolarWinds Knowledge Base article, "Unexpected results when you use advanced alerts on custom properties with NULL values".

Creating a Custom Property

The following procedure provides steps required to create a custom property.

To create a custom property:

1. Log on to the Orion Web Console as an administrator.

2. Click Settings in the top right corner of the web console, and then click Manage Custom Properties in the Node & Group Management grouping.
3. Click Add Custom Property.
4. Select the object type for the property you are creating, and then click Next.

   Note: Available object types will vary depending on the SolarWinds Orion products you have installed, but all installations will allow you to create both Node and Volume custom properties.
5. If you want to create a property based on a predefined template, click the appropriate Property Template.

   Note: Property templates provide generic suggestions in the Property Name and Description fields and an appropriate custom property Format.
6. Enter or Edit the Property Name and Description fields, as appropriate.

   Notes:

   To ensure full custom property functionality, do not leave the Property Name field empty.

   Only English custom property names are supported.

   Although most non-alphanumeric characters used in custom property names are replaced by underscores (_) when names are stored in the Orion database, SolarWinds recommends against using non-alphanumeric characters in custom property names. Hash characters (#) are not allowed in any property name.
7. Select a custom property Format, as appropriate.
8. If you want to restrict the possible values that other, non-administrative users can use for the selected property, check Restrict values, and then provide values, as follows:
   a. Enter an appropriate value for Value X.
   b. Click Add Value.
   c. If you need to delete a provided property value, click X next to the property to delete.
   d. Repeat, as needed, until you have supplied all valid property values.
9. Select how the property will be used in NCM. Contexts include Alerts, Filtering, Grouping, Reports, Object Details Views.
10. Click Next.

11. Click Select Objects, and then, using either of the following methods, sort the objects to which you can apply the selected property:

    Select an appropriate Group by: criterion, and then click the appropriate group including the objects to which you want the selected property to apply.

    Use the search tool to search your SolarWinds database for the objects to which you want the selected property to apply.

12. Check all monitored objects to which you want the selected custom property to apply.

    Note: Click > to expand listed objects to view available child objects.

13. Click Add to add checked objects to the Selected Objects list.
14. In the Selected Objects list, check all objects to which you want the selected property to apply.
15. If you have selected all objects to which you want the selected property to apply, click Select Objects.
16. For each selected object, select or enter an appropriate property value.
17. If you are editing a property with defined values, you are an administrator, and you want to add a new property value, select Add new value in the dropdown menu, and then provide the New value.
18. If you want to apply the selected property to a different group of objects, click Add more, and then select objects as indicated above.
19. If you have selected values for all objects to which you want the selected property to apply, click Submit.

Assigning Values to a Custom Property

The following procedure provides steps required to assign new values to an existing custom property.

To assign custom property values:

1. Log on to the Orion Web Console as an administrator.
2. Click Settings in the top right corner of the web console, and then click Manage Custom Properties in the Node & Group Management grouping.
3. Select the custom property for which you want to assign values, and then click Assign values.
4. Click Select Objects, and then, using either of the following methods, sort the objects to which you can apply the selected property:

Select an appropriate Group by: criterion, and then click the appropriate group including the objects to which you want the selected property to apply.

Use the search tool to search your SolarWinds database for the objects to which you want the selected property to apply.

5. Check all monitored objects to which you want the selected custom property to apply.

   Note: Click > to expand listed objects to view available child objects.

6. Click Add to add checked objects to the Selected Objects list.
7. In the Selected Objects list, check all objects to which you want the selected property to apply.
8. If you have selected all objects to which you want the selected property to apply, click Select Objects.
9. For each selected object, select or enter an appropriate property value.
10. If you are editing a property with defined values, you are an administrator, and you want to add a new property value, select Add new value in the dropdown menu, and then provide the New value.
11. If you want to apply the selected property to a different group of objects, click Add more, and then select objects as indicated above.
12. If you have selected values for all objects to which you want the selected property to apply, click Submit.

Importing Custom Property Data

Once you have defined custom properties, it is possible to import corresponding values from an external document, if it is correctly formatted. For example, you may already possess a spreadsheet listing the asset tags of all your network nodes, and you would like to have this information available for reporting and publication in the web console. In this scenario, Asset Tag is added as a custom property, and then the import wizard is used to populate the asset tag values from the spreadsheet. The following steps outline the process for importing custom properties data.

To import custom property data:

1. Log on to the Orion Web Console as an administrator.
2. Click Settings in the top right corner of the web console, and then click Manage Custom Properties in the Node & Group Management grouping.
3. Click Import.
4. Click Browse, and then navigate to your custom property data file.

5. Select the type of object for which you are importing values.

   Note: For best results, format your data as tables and provide titles in your data file that match the existing custom properties you are populating.

6. Click Next.
7. For each detected Spreadsheet Column, select the corresponding Orion Database Column, and then select the appropriate Relationship between the indicated columns.

   Notes:

   At least one column must match, for corresponding entries, between your spreadsheet and the Orion database column. Select the matches Relationship option for this key data.

   The imports to Relationship option overwrites any existing data in the corresponding Orion Database Column.

8. Click Import.

Removing Custom Properties

Custom properties are easily removed, as shown in the following procedure.

To remove a custom property:

1. Log on to the Orion Web Console as an administrator.
2. Click Settings in the top right corner of the web console, and then click Manage Custom Properties in the Node & Group Management grouping.
3. Check each property you want to remove, and then click Delete.
4. Confirm your selection by clicking Delete when prompted.

Exporting a Custom Property

With the Export Custom Properties feature, you can download a spreadsheet of any selected custom property, as it is stored in your SolarWinds database.

To export a custom property:

1. Log on to the Orion Web Console as an administrator.
2. Click Settings in the top right corner of the web console, and then click Manage Custom Properties in the Node & Group Management grouping.
3. Check the property you want to export, and then click Export.

4. If you want to select values for only a subset of all monitored objects for which the selected custom property is defined, click Select Objects, select the objects for which you want property values, and then click Select Objects.
5. Select the columns you would like to export.
6. Choose a file type for the exported file, and then click Export.
7. The exported file is saved with the filename exportCP in the localy designated downloaded files folder for your web console browser.

Appendix H

Configuring Automatic Login

The SolarWinds NCM Web Console allows you to log in using any of the following methods:

- Windows Active Directory Authentication, available in all Orion Platform products released after SolarWinds NPM version 10.1.
- Windows Pass-through Security. If you choose to employ Windows Pass-through Security, SolarWinds NCM users can be authenticated through Windows Security, with no need to log in using a separate SolarWinds NCM Account or User Name and Password. For more information, see "Using Windows Pass-through Security".
- DirectLink. If a DirectLink account is activated, any URL referring directly to an Orion Web Console page will bypass the Orion Web Console login page by logging the user into the DirectLink account. For more information, see "Using the DirectLink Account".
- URL Pass-through. For more information, see "Passing Login Information Using URL Parameters".

SolarWinds NCM prioritizes user login in the following manner:

1. Windows Active Directory Authentication is enabled. To enable Windows Active Directory Authentication, select the Windows Authentication option when configuring the Orion Web Console in the Configuration Wizard.
2. The Account or User ID and Password passed on the URL.
3. The Account or User ID and Password entered on the login.aspx page.
4. The Windows User if IIS NT Security is enabled, logging the user in using NT Security.
5. The Windows Domain to which the User belongs, for example, Development\Everyone.
6. The presence of a DirectLink Account.

Using Windows Pass-through Security

On all Orion Platform products released before SolarWinds NPM version 10.1, you may take advantage of the Windows Pass-through Security functionality when IIS NT Security is enabled. SolarWinds NCM users can be authenticated through Windows Security, with no need to log in using a separate SolarWinds

NCM account or User Id and Password. Pass-through Security can be configured to employ either Domain or Local computer security. Both may also be used at the same time. The SolarWinds Network Configuration Manager Account or User ID and Passwords must then be set up to match the Account or User ID and Passwords that are used for the Domain and/or Local computer security. Use the following procedure to enable IIS NT Security for logging in to the Orion Web Console with Windows Pass-through Security.

Notes:

With the release of SolarWinds NPM 10.1, Orion Web Console users may be authenticated using Active Directory.

When authenticating users with Windows Security, ensure your Orion server uses the NetBIOS domain name, instead of the fully qualified domain name.

To enable IIS NT security for Windows Pass-through Security:

1. If you are using NT Domain Authentication Format for pass-through accounts, create these pass-through accounts in the Orion Web Console Account Manager using Domain\UserID as the User Name, as follows:

   Washington\Edward

   StLouis\Bill

   Note: For more information about creating accounts using the Orion Web Console Account Manager, see “Creating New Accounts” on page 69.

2. If you are using Local Computer Authentication Format for pass-through accounts, create these accounts in the Orion Web Console Account Manager using Computer\UserID as the User Name, as follows:

   SolarWindsS2\Edward

   Server3\JonesR

   Note: For more information about creating accounts using the Orion Web Console Account Manager, see “Creating New Accounts” on page 69.

3. Click Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager.

4. If you are using Windows Server 2003, complete the following steps:

a. Expand Internet Information Services > Local Computer > Web Sites in the left pane.

b. Select SolarWinds NetPerfMon.

c. Click Action > Properties.

d. Click the Directory Security tab.

e. Click Edit within the Authentication and access control area.

f. Clear Enable anonymous access.

g. Select Integrated Windows authentication in the Authenticated access group.

h. Click OK to close the Authentication Methods window.

i. Click Apply, if available, and then click OK to close the SolarWinds NetPerfMon Properties window.

j. Collapse Internet Information Services > Local Computer > Web Sites.

k. Collapse Internet Information Services > Local Computer in the left pane.

l. Click Action > All Tasks > Restart IIS.

m. Confirm that Restart Internet Services on Local Computer is selected, and then click OK.

n. Close the IIS Manager.

5. If you are using Windows Server 2008, complete the following steps:

a. Click Start > Administrative Tools > Server Manager.

b. Expand Roles.

c. Click Web Server (IIS).

d. In the Role Services area, confirm that Web Server > Security > Windows Authentication is installed.

e. If Windows Authentication is not installed, click Add Role Services, select Web Server > Security > Windows Authentication, click Next, and then complete the service installation.

f. Click Start > Administrative Tools > Internet Information Services (IIS) Manager.

g. Select your Orion server in the left pane.

h. Click Authentication in the IIS group of the main pane.

i. Right-click Anonymous Authentication, and then click Disable.

j. Right-click Windows Authentication, and then click Enable.

k. Click your Orion server, and then click Restart in the Actions pane.

6. Close the IIS Manager.
7. Log in to the Orion Web Console using the Windows account credentials you have already established.

Passing Login Information Using URL Parameters

The user ID and password can be passed as parameters within the URL. This allows you to create a favorite or bookmark within a browser, or on your desktop. Create a favorite with a link in the following form to pass the login information:

```
http://DOMAIN/Orion/Login.aspx?AccountID=USER&Password=PASSWORD
```

Provide the hostname or IP address of your Orion server as the `DOMAIN`. Provide your Orion User ID as the `USER`, and then provide your Orion user account password as the `PASSWORD`.

Warning: HTTP requests are not encrypted, so User IDs and Passwords sent in HTTP requests are not secure. For more information about enabling HTTPS on your Orion server, consult www.microsoft.com.

Using the DirectLink Account

Enabling a DirectLink account allows you to make direct hyperlinks to specific web console views available to individuals who do not already have Orion Web Console user accounts. Any URL referring directly to an SolarWinds NCM web page bypasses the login screen, logging the user into the DirectLink account. The DirectLink account is created like any other account, and it can include custom views and account limitations. For more information web console accounts, see “Creating New Accounts”.

To enable a DirectLink account for the Orion Web Console:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings in the top right of the web console, and then click Manage Accounts in the Accounts grouping.
3. Click Add.
4. Type DirectLink as the new User Name.
5. Type a Password, confirm it, and then click Submit.
6. Edit DirectLink account options, as necessary, for your installation of SolarWinds Network Performance Monitor. For more information about editing account options, see “Editing User Accounts”.
7. Create a custom view to be used as the home page of the DirectLink account. For more information, see “Creating New Views”.
8. Specify the new DirectLink view as a default view in Account Manger. For more information, see “Editing User Accounts”.
9. If you would like to limit the DirectLink account to specific devices or device types, see “Setting Account Limitations”

Appendix I

Browsing MIBs

SolarWinds Network Configuration Manager Inventory functions use SNMP to communicate with the MIBs on your managed devices. If you are running into issues or are interested in learning more about the type of changes supported and values reported by your devices, the MIB Browser allows you to find and explore MIBs.

The SolarWinds Engineer's Toolset provides a fully functional MIB Browser tool that allows you to Login on devices and change values using a read-write SNMP string. For more information, see the SolarWinds website (www.solarwinds.com)

Browsing a MIB Tree

Complete the following procedure to begin browsing the MIB tree.

To browse the MIB tree for a specific device:

1. Click MIBs > Add/Edit MIBS.
2. Click New on the Configuration Management Customization window.
3. Click Browse (…).
4. Select an OID from the MIB Tree on the left.
5. If you are not sure which OID to select, complete the following procedure to view a number of useful values:
    a. Expand iso > org > dod > internet > mgmt > mib-2.
    b. Expand system.
    c. If you do not see the OID information you want, consider browsing the Interfaces folder.

Searching the MIB Tree

The MIB Browser incorporates a powerful MIB Tree OID search capability. This search capability allows you to search for a specific OID, OID name pattern, or keyword in the descriptions.

To search the MIB Tree:

1. Click MIBs > Add/Edit MIBS.
2. Click New on the Configuration Management Customization window.

3. Click Browse (…).
4. Click Search MIB Tree.
5. Select the appropriate tab:

   Search by OID

   Search by Name

   Search Descriptions
6. You can use asterisks (*) as a wildcard character. For example, sys* finds all OIDs that start with sys, and *number finds all OIDs that end with number.
7. Type the search criteria, and then click Search.
8. Click Show in MIB Tree to view the OID in the MIB tree.
9. If you want to copy or print the OID information you find, click the appropriate button.

   Note: When using the description tab, the first 500 OIDs that match the pattern will be displayed. Click the OID to display details about it.

Index