

SolarWinds Orion

Network Configuration Manager QuickStart Guide



NETWORK CONFIGURATION MANAGER

Copyright© 2005-2009 SolarWinds.net, Inc., all rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds All right, title and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its licensors. SolarWinds Orion™, SolarWinds Orion Network Configuration Manager™, and SolarWinds Toolset™ are trademarks of SolarWinds and SolarWinds.com® and the SolarWinds logo are registered trademarks of SolarWinds All other trademarks contained in this document and in the Software are the property of their respective owners.

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 OR 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.

Microsoft® and Windows 2000® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Graph Layout Toolkit and Graph Editor Toolkit © 1992 - 2001 Tom Sawyer Software, Oakland, California. All Rights Reserved.

Portions Copyright © ComponentOne, LLC 1991-2002. All Rights Reserved.

SolarWinds Orion Network Configuration Manager 05.11.2009 version 5.5

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	1.866.530.8100 www.solarwinds.com
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.
<i>Italics</i>	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

Orion Network Configuration Manager Documentation Library

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

Document	Purpose
Administrator Guide	Provides detailed setup, configuration, and conceptual information.
Quick Start Guide	Provides installation, setup, and common scenarios for which Orion 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

<i>About SolarWinds</i>	<i>iii</i>
<i>Contacting SolarWinds</i>	<i>iii</i>
<i>Conventions</i>	<i>iii</i>
<i>Orion Network Configuration Manager Documentation Library</i>	<i>iv</i>

Chapter 1

Introduction	1
<i>Why Install SolarWinds Orion Network Configuration Manager</i>	<i>1</i>
<i>Benefits of Orion Network Configuration Manager</i>	<i>2</i>
<i>Key Features of Orion Network Configuration Manager</i>	<i>3</i>

Chapter 2

Installing Orion Network Configuration Manager	5
<i>Licensing Orion Network Configuration Manager</i>	<i>5</i>
<i>Requirements</i>	<i>5</i>
<i>Server Sizing</i>	<i>8</i>
<i>About the Orion Network Configuration Manager Database</i>	<i>9</i>
<i>SNMP Communication</i>	<i>9</i>
<i>Installing Orion Network Configuration Manager</i>	<i>9</i>
<i>Obtaining a Software License Key</i>	<i>10</i>
<i>Configuring Orion Network Configuration Manager</i>	<i>11</i>
<i>Configuring User Access Control</i>	<i>14</i>
<i>Enabling User Access Control</i>	<i>14</i>
<i>Adding Windows Active Directory Account Users</i>	<i>15</i>
<i>Modifying Account Properties</i>	<i>16</i>
<i>Setting Node Communication Defaults</i>	<i>17</i>
<i>Configuring Event Logging</i>	<i>18</i>
<i>Installing the Orion NCM Integration for NPM</i>	<i>19</i>
<i>Configuring the Orion NPM Website Integration</i>	<i>20</i>

Chapter 3

Getting Started	21
<i>Adding Nodes.....</i>	<i>21</i>
<i>Adding Nodes with the Discovery Engine.....</i>	<i>22</i>
<i>Adding Individual Nodes.....</i>	<i>24</i>
<i>Adding Nodes Connected through a Serial Terminal Server</i>	<i>26</i>
<i>Importing Nodes</i>	<i>26</i>
<i>Exploring the Web Console.....</i>	<i>28</i>
<i>Launching and Logging On to the Web Console.....</i>	<i>29</i>
<i>Configuring Automated Nightly Backups</i>	<i>29</i>
<i>Changing the Community String on Multiple Nodes</i>	<i>30</i>
<i>Blocking a MAC Address on a Wireless Access Point.....</i>	<i>31</i>

Chapter 1

Introduction

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

Out of the box, SolarWinds Orion 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)
- Generate detailed configuration reports for inventory, change, and policy management
- Receive notification of device configuration changes
- Identify configuration violations through policy management reporting
- 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
- Web access to your device configurations and configuration changes

Orion Network Configuration Manager allows you to easily manage configurations on heterogeneous, multi-vendor networks. Orion 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, Netscaler, Juniper and Foundry. You gain a single point of management. Whether you are faced with managing network configurations for 50 or 5,000 devices, Orion Network Configuration Manager provides you with an intuitive solution that immediately impacts the bottom line.

Benefits of Orion Network Configuration Manager

Consider some of the following benefits of Orion Network Configuration Manager.

Out-of-the-box productivity

Within minutes of installing Orion NCM you will be able to backup your device configurations and collect detailed inventories. Orion NCM includes several wizards, such as setting up a new database or scheduling a job (to get you started right away).

Easy to understand and use

Orion Network Configuration Manager Configuration Manager is the most intuitive configuration management product available. Orion Network Configuration Manager is designed for daily use by staff with other responsibilities. The Orion Network Configuration Manager interface provides what you need where you expect to find it and offers advanced capabilities with minimal configuration overhead.

Affordable value

While Orion Network Configuration Manager provides comparable functionality, cost and maintenance of your Orion Network Configuration Manager installation is less than the initial cost of most other solutions.

Scalable

Orion Network Configuration Manager is friendly enough for even the smallest networks but powerful enough to manage the largest, most complex multi-vendor networks.

Key Features of Orion Network Configuration Manager

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

Scheduled Configuration Backups

Using the scheduled job feature, 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

Allows you to 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

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

Multivendor Support

Provides support for network devices from multiple hardware vendors. As a monitor and manager of routers, switches, firewalls, VPN concentrators, wireless access points and more, Orion NCM is a robust solution that is fully capable of managing your hybrid vendor network.

Bulk Changes

Enables quick changes to community strings, passwords, and black lists. With Orion NCM, you can execute bulk changes either in realtime 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

Reports 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 Configuration Viewing, Tracking, and Comparing

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

Orion Web Console Integration

An extension for the Orion Web Console comes with the Orion NCM application. This module-like extension provides five important new resources to the Device Details view for the Orion Web Console:

- Recent Configurations
- Recent Configuration Changes
- Node Configuration History
- Last 10 Conf Changes
- Last X Config Changes
- Last XX Configurations

Chapter 2

Installing Orion Network Configuration Manager

Orion Network Configuration Manager provides a simple, wizard-driven installation process. For an enterprise-class product, the requirements are nominal.

Licensing Orion Network Configuration Manager

Orion 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 Orion Network Configuration Manager. You license Orion 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 Orion 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)

Requirements

The requirements for Orion 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 Orion Network Configuration Manager installation.

Software/Hardware	Requirements	
Operating System	Windows 2003 Server SP2 or later (32-bit and 64-bit) including R2, with IIS installed and running in 32-bit mode. Windows 2008 Server Enterprise or Standard (32-bit or 64-bit) Note: SolarWinds does not support installation of Orion NCM on Windows Vista in production environments. See below.	
Orion NCM Server Hardware	CPU Speed	3GHz dual core dual processor
	Memory	3GB
	Hard Drive Space	20GB
Installing Windows Account	Requires administrator permission on the target server	
File System Access Permissions	Ensure the Network Service account has modify access to the system temp directory (%systemroot%\temp).	
SolarWinds Orion NCM Syslog Service Account	If you want realtime change detection triggered through devices sending Syslog messages, the account must have read-write access to the Orion NCM database. For more information, see "Enabling Realtime Configuration Change Detection" on page Error! Bookmark not defined. and "Monitoring Syslog Messages" on page Error! Bookmark not defined.	
SolarWinds Orion NCM Trap Service Account	If you want realtime change detection triggered through devices sending SNMP traps, the account must have read-write access to the Orion NCM database. For more information, see "Enabling Realtime Configuration Change Detection" on page Error! Bookmark not defined. and "Monitoring SNMP Traps" on page Error! Bookmark not defined.	
Microsoft SNMP Trap Service	Must be installed if you want realtime change detection triggered through devices sending SNMP traps. For more information, see "Enabling Realtime Configuration Change Detection" on page Error! Bookmark not defined. and "Monitoring SNMP Traps" on page Error! Bookmark not defined.	
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 <i>RFC 952</i> . Note: SolarWinds neither recommends nor supports the installation of Orion 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	Version 3.5 or later (if this is not found on the target computer, the setup program downloads and installs the component)	

Software/Hardware	Requirements
Database	<p>The following database servers are supported as the Orion Network Configuration Manager datastore:</p> <ul style="list-style-type: none"> • SQL Server 2008 Standard or Enterprise <p>SQL Server 2005 SP1 or later of Express, Standard, or Enterprise</p> <p>You can use the following database select statement to check your SQL Server version, service pack or release level, and edition:</p> <pre>select SERVERPROPERTY ('productversion'), SERVERPROPERTY ('productlevel'), SERVERPROPERTY ('edition')</pre> <p>Your database server must support mixed-mode authentication or SQL authentication and have the following protocols enabled:</p> <ul style="list-style-type: none"> • Shared memory • TCP/IP <p>Named Pipes</p> <p>SQL Server 2005 Express Edition does not enable these protocols.</p> <p>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):</p> <ul style="list-style-type: none"> • SQL Server System Common Language Runtime (CLR) Types • Microsoft SQL Server Native Client <p>Microsoft SQL Server Management Objects</p> <p>Enabling Full-Text Search on your Orion NCM database significantly increases search performance.</p>
Browser	<p>To access the Orion Network Configuration Manager website, use one of the following browsers:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer 6 or later • Mozilla Firefox 3 or later

Notes:

-  By default, Windows 2008 sets scheduled tasks to run only when the user context it is set to run under is logged on and requires Windows credentials for every change. Any job changes made through the NCM client application may require the entering of credentials on the Security tab prior to saving. You may also use the Windows Task Scheduler to directly enable/disable jobs, execute jobs, and update schedules.
-  SolarWinds does not support installation of Orion NCM on Windows Vista in production environments. If you are installing Orion NCM on Windows Vista, ensure you enable the appropriate database protocols. See the database section of the requirements.
- The Orion Network Configuration Manager Information Service requires the `Net. Tcp Port Sharing Service` to be enabled and port 17777 open for TCP traffic to the Orion NCM computer. By default, this service is disabled. The setup program sets the service to manual. Resetting the service setting to disabled will adversely affect your installation.

- To take advantage of the numerous integration points in Orion 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.

Server Sizing

Orion Network Configuration Manager can perform configuration management for any sized network, from small corporate LANs to large enterprise and service provider networks. Most Orion NCM implementations perform well on Pentium-class 2GHz systems with 2GB 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.

About the Orion Network Configuration Manager Database

A copy of Microsoft SQL Server 2005 Express Edition is distributed with each copy of Orion Network Configuration Manager. SQL Server 2005 Express Edition supports a maximum database size of 4GB, 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>.

If you are installing Orion NCM on the same server as Orion NPM, consider using a remote database server for your databases. You will gain a number of performance enhancements through implementing this installation scenario, as the Orion server will no longer need to share resources with SQL Server.

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

Orion 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.

Installing Orion Network Configuration Manager

Complete the following procedure to install Orion Network Configuration Manager.

Note: If you are installing on Windows XP and want to use the Orion NCM Web Console, ensure you have installed Microsoft Internet Information Server 6 or later. The setup program stops the default website and starts the Orion NCM Web Console. Only one website can be active on IIS when installed on Windows XP.

To install Orion Network Configuration Manager:

1. Log on with a local administrator account to the computer on which you want to install Orion Network Configuration Manager.
Note: To ensure that Orion Network Configuration Manager runs properly, do not install Orion Network Configuration Manager on a domain controller.
2. Navigate to your download location and launch the executable.
3. Review the Welcome text, and then click **Next**.
4. Accept the license agreement displayed on the License Agreement window, and then click **Next**.
5. Type the user name and organization on the Customer Information window.
6. Select whether you want to limit Orion Network Configuration Manager to the currently logged in account, and then click **Next**.
7. Click **Typical**, and then click **Next**. If you need to change the installation path, click **Custom**.
8. Click **Install**.
9. **If you are prompted to license Orion NCM**, provide the appropriate information on the Install Software License Key window, and then click **Continue**. You need a customer ID and password to successfully install the key. For more information, see “Obtaining a Software License Key” on page 10.
10. Click **Finish** on the InstallShield Wizard Completed window.

Obtaining a Software License Key

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

To license your product:

1. **If the computer on which you are installing Orion Network Configuration Manager is connected to the Internet**, complete the following procedure:
 - a. Enter the required information on the Install Software License Key window.
 - b. Click **Continue**. The SolarWinds license registration server will issue a license key that will allow Orion Network Configuration Manager to operate.

2. **If the computer on which you are installing Orion Network Configuration Manager is not connected to the Internet**, your system can not be authenticated by the SolarWinds license registration server. Complete the following procedure:
 - a. Click **Skip This and Enter Software License Key Now** on the Install Software License Key window.
 - b. Obtain a license using a computer that is connected to the Internet. Login to the customer area of the SolarWinds website at www.solarwinds.com/support, and then click **Software Keys** in the left navigation of the customer portal. Choose the product for which you need a key and follow the instructions on the page to obtain a key. The key can then be entered in the **Enter Software License Key** text box on the Install Software License Key window.
 - c. Click **Continue** to complete your software license key installation.

Configuring Orion Network Configuration Manager

After installing Orion NCM, the configuration wizard launches automatically. If it does not start automatically or you need to rerun the wizard, start it from the SolarWinds Orion Network Configuration Manager program group in the Start menu.

Warning: If you install the Web Console, the Configuration wizard will reboot your IIS server. Any websites hosted by the server will be stopped and restarted during this process.

To configure Orion Network Configuration Manager:

1. Review the Welcome window, and then click **Next**.
2. Specify the SQL Server instance you want to use for storing configurations and node details and the authentication method used to communicate with the instance, and 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.
3. If this is the first time you are installing Orion NCM, click **Create a new database**, and then click **Next**. Otherwise, select the existing Orion NCM database you want to use, and then click **Next**.

4. Create a new database account and password or select an existing account with owner rights on the database you created or selected.

Note: You must supply a strong password. For more information about strong passwords, see <http://msdn.microsoft.com/en-us/library/ms143705.aspx>.

5. **If you need to specify a particular IP Address for your Orion NCM Web Console installation**, provide the IP address you want to use for the Web Console.

Note: SolarWinds recommends that you retain the default IP address setting of **All Unassigned**, unless your environment requires the designation of a specific IP address for your Orion NCM Web Console.

6. Specify both the port through which you want to access the Web Console and the volume and folder in which you want to install the Web Console files. By default, this port is set to 8888 to avoid conflicts with other websites on the server.

Note: If you accept the default port or you specify any port other than 80, you must include that port in the URL used to access the Web Console. For example, if you specify an IP address of 192.168.0.3 and port 8080, the URL used to access the Web Console is `http://192.168.0.3:8080`.

7. Click **Next**.

8. Review the services the wizard will install, and then click **Next**

Note: If you want to use the Trap Viewer tool or trigger realtime 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. For more information, see the *Administrator Guide*.

9. Read the summary of what the configuration wizard will configure, and then click **Next**.

10. Review the information on the System Defaults window. This section of the wizard allows you to specify a number of default values used when accessing devices in your network. For example, this section of the wizard allows you to set default SNMP community strings.

11. Type the default read-only and read-write community strings for nodes on your network, and then click **Next**. This default string is tried first, before interactively requesting one.

12. **If your network devices use SNMPv3**, check **Specify SNMP v3**, provide the appropriate values, and then click **Next**.

13. Provide the default user name, password, enable level, and password for your network devices, and then click **Next**.
14. Specify how you would like to group you nodes in the Orion NCM Client node tree and in the Web Console.
15. Type a Windows user account to use when running scheduled jobs installed with Orion NCM, and then click **Next**. Use the following syntax:
domain\username.
16. Click **OK** on the Credentials Set dialog.
17. **If you want to populate the Node List with your network devices**, check **Populate the Node List with devices**, and then select a method to populate the list:
 - Import devices
 - Discover devices.

A separate wizard launches to guide you through importing or discovering devices. For more information about importing or adding devices, see “Adding Nodes” on page 21.

Note: If you choose not to import or discover devices, Orion NCM provides the ability to import or discover devices from within the application also. For more information, see “Adding Nodes” on page 21.

18. **If you want to synchronize your Orion NPM nodes with those you have in Orion NCM**, check **Do you have Orion NPM and want to synchronize the nodes into Orion NCM**, and then specify your Orion NPM database information. Click **Next**.

Note: Ensure the SQL Server Browser service is running on your Orion NPM database server.

19. Review the Configuration Summary, and then click **Finish**.
20. Click **LOGIN** on the First-Time Login Prompt window, and then provide an administrator password. This password controls administrator-level access to the user interface. For more information, see “Configuring User Access Control” on page 14.

Configuring User Access Control

Orion Network Configuration Manager provides role-based user access control to manage permissions for each user. User access control allows you to limit access to the application through enabling access control and through the assignment of the following access roles:

Administrator

Grants access to the entire Orion Network Configuration Manager application. All Web resources are available to this user role.

Engineer

Grants access to the Orion Network Configuration Manager application excluding the ability to create, modify, or delete user accounts, modify security settings, or alter device connectivity methods. All Web resources are available to this user role.

WebDownloader

Grants access to the Web Console, Download, and View Transfer Status operations. No access is granted to the native application installed on the Orion NCM server.

WebUploader

Grants access to the Web Console, Download, Upload, View Transfer Status, Execute Script, and Edit Config operations. No access is granted to the native application installed on the Orion NCM server.

WebViewer

Grants access to the Orion Network Configuration Manager Web Console only. No access is granted to the native application installed on the Orion NCM server.

Enabling User Access Control

Complete the following task to limit access to Orion NCM through the definition of application-based users and Windows Active Directory users.

To enable user access control:

1. Click **File > Settings > Security**.
2. Check **Require a login to use Orion Network Configuration Manager**.

3. **If you want to assign device login credentials to user accounts**, complete the following procedure:
 - a. Click **Device Connectivity Method**.
 - b. Click **Manage devices using a combination of individual login credentials per device and user account device login credentials**.
 - c. Click **OK** in the Warning window
4. Click **OK** in the Orion Network Configuration Manager Settings window.

Adding Windows Active Directory Account Users

Orion NCM integrates with Windows Active Directory and local system accounts to simplify the user management process.

To add Windows Active Directory Account users:

1. Click **File > Manage Orion NCM Users**.
2. Click **Add**.
3. Click **Locations**, browse to the domain that includes the user, and then click **OK**.
4. Type the user name including the domain, for example `domain\username`.
5. Click **Check Names** to ensure the user name is typed properly.
6. Click **OK**.

7. Select a role from the **Role** list on the Manage Orion NCM Users window

Administrator

Grants access to the entire Orion Network Configuration Manager application.

Engineer

Grants access to the Orion Network Configuration Manager application excluding the ability to create, modify, or delete user accounts, modify security settings, or alter device connectivity methods.

WebDownloader

Grants access to the Web Console, Download, and View Transfer Status operations. No access is granted to the native application installed on the Orion NCM server.

WebUploader

Grants access to the Web Console, Download, Upload, View Transfer Status, Execute Script, and Edit Config operations. No access is granted to the native application installed on the Orion NCM server.

Web Viewer

Grants access to the Orion Network Configuration Manager Web Console only. No access is granted to the native application installed on the local computer.

8. *If you are assigning device login credentials to user accounts*, type the user name and password used to access nodes for this user, and then type the enable level and enable password, if necessary.
9. *If you want to add another user*, click **Apply**, and then restart the procedure at **Step 2**.
10. Click **OK**.

Modifying Account Properties

You can change a number of properties associated with your defined Orion NCM user accounts. For Windows accounts provided access to the applications, you can change the following:

- Role
- Associated device user name and password
- Associated device enable level and password

For built-in Orion NCM devices, you can modify the following:

- Account password
- Associated device user name and password
- Associated device enable level and password

To edit a user account:

1. Click **File > Manage Orion NCM Users**.
2. **If you want to modify access or roles assigned to a Windows user account**, complete the following procedure.
 - a. Select the Windows user account you want to modify in the **Users** list.
 - b. In the Manage Orion NCM Users window, select a role from the **Role** list.
 - c. Type the user name and password used to access nodes for this user, and then type the enable level and enable password, if necessary.
 - d. **If you want to modify another user account**, click **Apply**, and then repeat this procedure.
3. **If you want to modify a built-in Orion Network Configuration Manager user account**, complete the following procedure.
 - a. Click the Built-In Orion NCM Users tab.
 - b. Select the user account you want to modify in the **Users** list.
 - c. **If you want to change the password**, click **Change Password**, type and verify the new password, and then click **OK**.
 - d. Type the user name and password used to access nodes for this user, and then type the enable level and enable password, if necessary.
 - e. **If you want to modify another user account**, click **Apply**, and then repeat this procedure.
4. Click **OK**.

Setting Node Communication Defaults

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

To set default node configuration parameters:

1. Click **File > Settings**.
2. Navigate to and expand **Global Macro Settings**.

3. Select one of the following tree options and specify the appropriate default values:
 - Community String
 - SNMPv3 Settings
 - Login Information
 - Transfer Protocols
 - Transfer Ports

Configuring Event Logging

Logging events associated with a specific function of Orion 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 Orion NCM provide verbose logging options, including the following:

Database Updates

Logs database events, including backup and connectivity events.

Inventory Monitor

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

Node Monitor

Logs node events, including ICMP timeouts and node status changes.

Realtime Config Change Detection

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

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.

Security

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

To enable logging for Orion Network Configuration Manager events:

1. Click **File > Settings**.
2. Click **Advanced > Logging**.
3. Check the Orion Network Configuration Manager events you wish to monitor, and then click **OK**.

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\`.

Installing the Orion NCM Integration for NPM

Orion Network Configuration Manager provides a module-like integration for your current Orion Network Performance Monitor website. If you want to add Orion Network Configuration Manager-specific information to your Node Details and other views, complete the following procedure.

Note: The integration requires Orion NPM version 9.5 or later.

To install the integration:

1. Log on to your Orion server with a local administrator account.
2. **If you downloaded Orion NCM from the SolarWinds website**, navigate to your download location and launch the executable.
3. **If you received physical media**, navigate to the Orion NCM Integration for the Orion Web Console or browse to the `SolarWinds-Orion-NCM-version#-NPM-Integration.exe` executable file and launch it.
4. Review the Welcome window, and then click **Next**.
5. Read and accept the license agreement, and then click **Next**.
6. Click **Install**.
7. Click **Finish** when the setup wizard completes.
8. Complete the Orion Configuration Wizard, launched automatically after the extension installs.

The integration adds all the functionality of the Orion NCM Web Console to the Orion NPM Web Console, with the exception of search. For more information about the resources, click **Help** on the individual resource. Functionality remains the same, including the need to be in the appropriate Orion NCM roles. For more information, see "Configuring User Access Control" on page 14. The integration is also governed by configurable account and view limitations in Orion NPM. For more information about account limitation, see the *Orion NPM Administrator Guide*.

Configuring the Orion NPM Website Integration

After installing the extension, you need to point the Orion website to your Orion NCM location. Complete the following procedure to update the website with your Orion NCM location.

To configure the Orion NCM Extension:

1. Log on to the Orion NPM website with an administrator account, and then click **Admin** in the Views toolbar.
2. Locate the Settings grouping, and then click **NCM Settings**.
3. Click **Connection Information**.
4. Type the hostname or IP address of the server hosting the Orion NCM information service in the **Hostname or IP Address** field. Do not designate a port in this field.
5. Type the URL, including the port number, in the **Website URL** field, and then click **Submit**. For example, type `http://192.168.1.45:8888`, ensure you include the port number when designating the URL.
6. Click **Network Configuration Manager** in the Modules menu bar.
7. Click **Credentials** in the Node List resource, and then specify a user name and password used to access the Orion NCM Web Console. For example, type `Administrator` and the administrator password used to access the Orion NCM client application. For more information, see "Configuring User Access Control" on page 14.

Chapter 3

Getting Started

A significant amount of time spent managing your network devices can be cut using Orion Network Configuration Manager. The following section steps you through four common use cases. By stepping through this quick introduction, you learn how to add network devices, how to configure nightly backups, how to block private addresses on several devices, and how to update devices with a new community string.

1. Adding network devices
2. Configuring automated nightly backups
3. Changing the community strings on multiple nodes
4. Blocking a MAC address on a wireless access point

Adding Nodes

You can add nodes using the SolarWinds Discovery Engine, add them individually, or import a list of nodes from a file. The following procedures guide you through these methods:

- “Adding Nodes with the Discovery Engine” on page 22
- “Adding Individual Nodes” on page 24
- “Adding Nodes Connected through a Serial Terminal Server” on page 26
- “Importing Nodes” on page 26

Adding Nodes with the Discovery Engine

SolarWinds Discovery Engine is a high performance network discovery tool, allowing you to build a database of the structure and devices found in your TCP/IP network.

To start the wizard:

1. Click **File > Discover Devices**.
2. Specify your SNMP community strings in the **New SNMP Community String** field, and then click **Add**.

Note: The more community strings you add, the longer you may have to wait for your network discovery. Ensure the most frequently used community strings appear first in the list. Use the arrows to arrange the order of the strings.

3. **If you want to modify Discovery settings**, click **File > Settings**, and then select the following tabs:

Subnet Auto-Selection

Allows you to select whether subnets, other than those you specify, that are discovered should be automatically added to the network scan.

Network Scan

Allows you to specify the following settings:

- Delay between PINGs
- PINGs per IP Address
- PING Timeout
- Maximum number of concurrent PINGs

PING is used to identify responding devices before attempting an SNMP connection.

SNMP

Allows you to specify the following settings:

- SNMP Retries
- SNMP Packet Timeout
- Maximum number of concurrent SNMP sessions

4. Click **Next Step**.

5. Click one of the following:

Add Subnets

Allows you to manually add a subnet using a subnet address and subnet mask.

Discover Subnets using Seed Routers

Allows you to specify a router IP address and use the specified router to discover subnets and devices. A seed router is any router in your network. A server, switch, or workstation that supports SNMP can also be used. Though for best results, use a core router.

Note: Discovering the network topology may take a few minutes. If a small number of subnets are missing from the list, Network Sonar can pick them up during the network discovery. If entire networks are missing, rerun the topology discovery using a seed router in the missing network. Click **Previous** to get back to the Discover subnets from a seed router window.

6. Check the subnets you want to include, and then click **Next Step**.
Note: If you are planning on discovering a portion of the Internet, such as a national or local ISP network, add the networks or subnets manually and set limits on the discovery. If you do specify desired subnets, Network Sonar may attempt to discover the entire Internet.
7. Click **Start Network Discovery**. The faster you set the discovery slider, the more traffic generated. If you are discovering a network across a dial-up line or low bandwidth circuits, increasing the discovery speed will also increase the chances of congestion and dropped packets.
8. Click **Close** when the Discover completes.
9. Click **File > Exit**.
10. Specify the columns you want to import to Orion NCM by clicking on the column headings and selecting the appropriate name. The default columns are already named. Click **Next**.
11. Check the devices you want to import on the Select Import Rows window.
12. Check the appropriate options on the Import Options window, and then click **Import**. You can use these options to skip previously defined nodes and discover device details immediately after the import.
13. Click **Done**.

Adding Individual Nodes

Complete the following procedure to add one of your network devices as a managed node.

To add individual nodes:

1. Click **Nodes > Add New Node**.
2. Type the hostname or IP address of the node.
3. Select the SNMP version of the node, and then type the SNMP read-only and read-write community strings.
4. **If the device uses SNMPv3**, expand the SNMPv3 category, and then provide the appropriate values needed to login to the device.
5. Click **Verify SNMP Community**.
6. Select the device template from the list.

Note: Try **Auto Detect** first. If Orion Network Configuration Manager is unable to determine the appropriate device command template, or assigns the wrong template, then select the template from the list.

7. **If you want to add the node to a group**, type or select a node group from the list. If you do not select a group, your new node is grouped in the `Unknown` group.
8. **If you are using individual device login credentials**, set the **Login Credentials** field to `Device`, and then type the user name and password used to access the node. Type the enable level and enable password, if necessary.

Notes:

- Use the Telnet or Web Browse buttons to connect to the node and view node information.
 - When typing the login information, type values just as they would be typed during manual login. For example, if 15 represents enable level 15, then type `15` for the value.
9. If you want to use Orion NCM user account device login credentials, set the **Login Credentials** field to `User`.

10. Select the protocol you want to use to run scripts in the **Execute scripts using list**.

Notes:

- Four options are available: TELNET, SSH1, SSH2, and SSH Auto. When selecting SSH Auto, Orion NCM will first attempt to negotiate an SSH2 connection. If SSH2 is not supported, Orion NCM defaults to SSH1.
- If your SSH connection requires user credential authentication after certificate negotiation, ensure you define device login credentials or associate login credentials with your user account.

11. Select the protocol you want to use to send requests for transfers to your device. The following options are available: TELNET, SNMP, SSH1, SSH2, and SSH Auto.

Notes: When selecting SSH Auto, Orion NCM will first attempt to negotiate an SSH2 connection. If SSH2 is not supported, Orion NCM defaults to SSH1. SNMP is only supported on Cisco devices.

12. Select the protocol you want to use to transfer configuration files to Orion Network Configuration Manager.

Note:

- Five options are available for the command execution protocol and the config transfer protocol: TELNET, TFTP, SSH1, SSH2, and SSH Auto. When selecting SSH Auto, Orion NCM will first attempt to negotiate an SSH2 connection. If SSH2 is not supported, Orion NCM defaults to SSH1.
- If your SSH connection requires user credential authentication after certificate negotiation, ensure you define device login credentials or associate login credentials with your user account.

13. Specify the Telnet port and SSH port, as appropriate. You can override the global setting or accept the default. For more information about global settings, see "Setting Node Communication Defaults" on page 17.

14. Click **Verify Login Information**.

15. *If the node uses HTTPS to connect to the web interface*, select **Yes** in the **Browse via HTTPS** field.

16. *If you want the device to reflect property updates made in Orion NPM*, select **Yes** in the **Orion Node Import** field.

17. Click **OK** to add the node.

Note: To keep the window open and add additional nodes, check **Keep this window open so I can add more nodes**.

Adding Nodes Connected through a Serial Terminal Server

When adding devices connected through a serial terminal server, you need to specify certain information that is specific to the terminal server device and other information that is specific to the device attached to the terminal server to which you want to connect. Complete the following procedure, paying close attention to the credential sections.

To add a device connected through a serial terminal server:

1. Click **Nodes > Add New Node**.
2. Type the IP address of the node assigned through the terminal server. For example, the Cisco terminal server device used in the SolarWinds lab, a Cisco 2500 Access Server, uses ports appended to the end of the loopback IP address to specify different devices. In this case, type `10.10.29.1 2001`. Some devices allow you to specify unique IP addresses, in which case, specify the assigned IP address in this field.
3. Ignore the community string information, as it does not apply when connecting through a terminal server device.
4. Select the device template for the connected device, not for the terminal server device.
5. **If you want to add the node to a group**, type or select a node group from the list. If you do not select a group, your new node is grouped in the `Unknown` group.
6. Specify the login credentials, enable level, and enable password for the target device. Again, do not specify the password for the terminal server device.
7. Select **Yes** in the **Terminal Server Support** field.
8. Click **OK**. When the Add Device dialog states that the IP address does not respond to SNMP queries, click **Yes**.

Importing Nodes

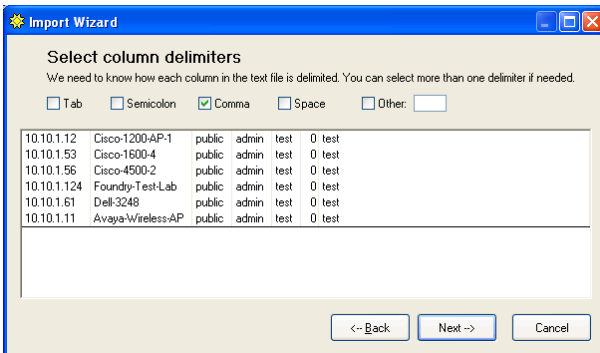
You can import a list of nodes using several different file formats. Nodes can be imported from the following file formats:

- Text files
- Excel spreadsheets
- Network Sonar Discovery Database
- SolarWinds Orion Network Performance Monitor databases

- SolarWinds Engineer's Edition Network Performance Monitor databases
- Cirrus Configuration Management Database – Enterprise Edition – SQL Server
- Cirrus Configuration Management Database – Desktop Edition – Access
- SQL Server databases
- Microsoft Access databases
- CiscoWorks database exports
- Kiwi CatTools database exports

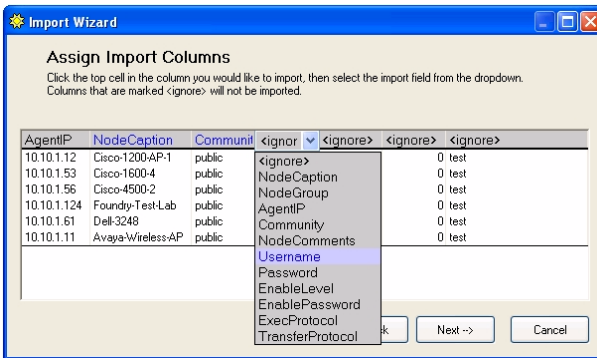
To import nodes:

1. Click **File > Import Devices**.
2. Select the file type from the list, and then click **Next**.
3. Type or browse to the path and filename, and then click **Next**.
4. **If you are importing a text file**, check the column delimiters used to separate each field, and then click **Next**. Columns align based on the selections made.



5. **If you are importing an Excel spreadsheet**, select the worksheet from the list, and then click **Next**.
6. **If you are importing a SQL database**, complete the following steps:
 - a. Select the SQL server from the list, or type the server IP address
 - b. Type or select the database name.
 - c. Select the type of authentication required for the connection, and then click **Next**.

7. Assign each column a field name. Click on the column header, and then select a field from the list. Selecting **<ignore>** allows you to bypass the column.



8. Ensure you are importing the appropriate data, and then click **Next**.
9. **If you want to exclude certain nodes**, clear the associated checkbox, and then click **Next**.
10. **If you want exclude previously added nodes**, check **Do not import nodes with IP addresses that already exist in the Configuration Management database**.
11. **If you are importing a large list of nodes**, uncheck **Discover device details immediately after Import**.
12. Click **Import**.
13. Click **Done** after the process completes.

Exploring the Web Console

The Web Console, provided with Orion Network Configuration Manager, offers you access to your device configs without requiring physical access to your Orion 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
- Check configuration backup status
- Compare configurations and view differences.

Launching and Logging On to the Web Console

To launch the Web Console, you can either log on to the Orion NCM server and click **Start > Program Files > SolarWinds Orion Network Configuration Manager > Orion NCM Web Console** or point any remote browser to the Orion NCM server: `http://hostnameOrIPAddress:port`. Where, `hostnameOrIPAddress` is either the hostname or IP address of the Orion NCM server and `port` is the Web Console port defined for the website. By default, the port is 8888.

To log on to the Web Console, you can use either Windows credentials or an Orion 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. For more information, see “Configuring User Access Control” on page 14. For more information about any resource, click **Help**.

Configuring Automated Nightly Backups

A powerful feature of Orion Network Configuration Manager is the ability to schedule daily configuration file backups. Orion Network Configuration Manager ships with 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.

To setup nightly configuration backups for all nodes:

1. Click **Schedule > Create New Job**.
2. Click **Download Configs from Devices**, and then click **Next**.
3. Type a name for the job, and then click **Continue**.
4. Select **Daily** in 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. Click **Continue**.
9. Type the Windows account name that will be used to run the job.
10. Type the password for the Windows account in the appropriate password fields.
11. Click **Finish**.
12. Type any comments in the **Comments** field.
13. Click the **Download Config** tab.

14. Check the configuration types you want to download.
15. Check **Last Config** to be notified when the downloaded configuration file is different from the last configuration.
16. Check **Baseline Config** to be notified when the downloaded configuration file is different from the baseline configuration.
17. Click **OK**.

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.

To update the community string for a group of nodes:

1. Back up the running configuration prior to making any changes.
2. Click the node or group of nodes you want to update, and then click **Nodes > Download Configs**.
3. Click **Download**.
4. Right-click a node or group of nodes, and then click **Execute Command Script**.
5. Type the following command script:

```
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.

6. Click **Execute Command Script**.
7. To verify that the script executed successfully,
 - a. Click the node or group of nodes you updated, and then click **Nodes > Download Configs**.
 - b. Check **Compare to last Config Downloaded**.
 - c. Click **Download**. When the download completes, a comparison window opens. Changes to the community string are highlighted in red and green.

Blocking a MAC Address on a Wireless Access Point

If you discover a device utilizing unauthorized access to 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.

To update the ACL for a node:

1. Back up the running configuration prior to making any changes.
2. Click the group of routers that are to be updated, and then click **Nodes > Download Configs**.
3. Click **Download**.
4. Click the group of routers that you want to update, and then click **Nodes > Execute Command Script**.
5. Type the following command script:

```
#{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.

6. Verify the script executed successfully by complete the following procedure:
 - a. Click the node or group of nodes, and then click **Download Configs**.
 - b. Check **Compare to last Config Downloaded**.
 - c. Click **Download**.
 - d. When the download completes, a comparison window opens automatically. Changes to the access list are highlighted in red and green.

