SolarWinds

Network Performance Monitor Administrator Guide

solarwinds

Unexpected Simplicity

SolarWinds NPM Administrator Guide, Version 11.5.2.2, 11/16/2015

About SolarWinds

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

Contacting SolarWinds

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

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	www.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

Convention	Specifying
`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

Documentation Library

The following documents are included in the documentation library:

Document	Purpose
Administrator Guide	Provides detailed setup, configuration, and conceptual information.
Page Help	Provides help for every window in the user interface
Release Notes	Provides late-breaking information, known issues, and updates. The latest release notes can be found at www.solarwinds.com.

Table of Contents

Chapter 1: Introduction

SolarWinds Network Performance Monitor (NPM) delivers comprehensive fault and network performance management that scales with rapid network growth and expands with your network monitoring needs, allowing you to collect and view availability and real-time and historical statistics directly from your web browser. While monitoring, collecting, and analyzing data from routers, switches, firewalls, servers, and any other SNMP-, ICMP-, or WMI-enabled devices, SolarWinds NPM successfully offers you a simple-to-use, scalable network monitoring solution for IT professionals juggling any size network.

SolarWinds users have also found that it does not take a team of consultants and months of unpleasant surprises to get a full SolarWinds NPM installation up and running because the overall SolarWinds NPM experience is far more intuitive than conventional, unnecessarily complex enterprise-level network, systems, and storage monitoring and management systems. Because it can take less than an hour to deploy and no consultants are needed, NPM provides quick and cost-effective visibility into the health of network devices, servers, and applications on your network, ensuring that you have the real-time information you need to keep your systems running at peak performance.

Benefits of Orion Network Performance Monitor

Consider the following benefits of Orion Network Performance Monitor.

Out-of-the-box Productivity

Automatic discovery and wizard-driven configuration offer an immediate return on your investment. Within minutes of installation, you can be monitoring your critical network elements and applications.

Easy to Understand and Use

SolarWinds NPM is designed for daily use by staff that also have other responsibilities. The Orion Web Console provides what you need where you expect to find it and offers advanced capabilities with minimal configuration overhead.

Affordable Value

While SolarWinds NPM provides functionality that is comparable, if not superior, to most other solutions, the cost and maintenance of your SolarWinds NPM installation is less than the initial cost of most other network and systems monitoring solutions.

Scalability

By adding individual polling engines, you can scale your SolarWinds NPM installation to any environment size. By sharing the same database, you can also share a unified user interface, making the addition of polling engines transparent to your staff.

thwack.com Online Community

thwack.com is a community site that SolarWinds developed to provide SolarWinds users and the broader networking community with useful information, tools and valuable resources related to SolarWinds network management solutions. Resources that allow you both to see recent posts and to search all posts are available from the Orion Web Console, providing direct access to the thwack.com community.

Key Features of SolarWinds NPM

Considering the previously listed benefits of SolarWinds NPM and the following features, SolarWinds NPM is a simple choice to make for monitoring your network.

Automatic and Scheduled Device Discovery

Wizard-driven device discovery further simplifies the addition of devices and interfaces to SolarWinds NPM. Answer a few general questions about your devices, and the discovery application takes over, populating your Orion database and immediately beginning network analysis. You can also create network discovery schedules to independently and automatically run Network Sonar Discovery jobs whenever you need them.

Interface Monitoring

NPM helps you collect, analyze and visually display data polled for monitored interfaces, such as information about possible duplex mismatches or interface downtime.

Quality of Experience Monitoring

A new Quality of Experience (QoE) dashboard allows you to monitor network and application traffic by collecting and analyzing packet-level data directly from the Orion Web Console. With the QoE Monitoring component, you can do all of the following, directly from the Orion Web Console:

- Monitor traffic by collecting and analyzing packets locally or on a SPAN/mirror interface or tap.
- Determine if traffic bottlenecks are on the network or at the server by comparing network (TCP Handshake) and application (Time of First Byte) response times.
- Choose from over 1000 pre-defined applications (such as FTP, RDP, CIFS, SQL, Exchange, etc.) or create your own custom HTTP application to monitor.
- Deploy Packet Analysis Sensors to analyze network data. Use Network Sensors to monitor traffic through network interfaces using dedicated Windows nodes connected to SPAN/mirror interfaces or taps, and use Server Sensors deployed on any Windows server to monitor traffic locally.
- Characterize applications as either business-related or purely social so you can keep tabs on how your bandwidth is used.

- Use application categories, such as web services, network monitoring, and file transfer, to better understand and manage your network's traffic profile.
- Specify application risk levels, from "No Risk" to "Evades Detection/Bypasses Firewalls", to be alerted whenever there is unwanted, risky traffic on your network.

  For more information, see "Monitoring Quality of Experience" in the Orion Common Components Guide.

Network Operations Console (NOC) View Mode

Customize web console views for optimal display on large network operations center screens. With NOC View enabled, a web console view can cycle through its network monitoring resources for continually updated, shared viewing.

Customizable and Flexible Orion Web Console

You can easily customize the web console to meet your individual needs. If you want to segregate use, you can custom design views of your data and assign them to individual users. You can also create web console accounts for departments, geographic areas, or any other user-defined criteria.

Open Integration

Enterprise-tested standards, including a Microsoft® SQL Server database and industry-standard MIBs and protocols, are the backbone of the SolarWinds NPM monitoring solution.

Network Atlas with ConnectNow

Network Atlas, the Orion network mapping application, gives you the ability to create multi-layered, fully customizable, web-based maps of your network to visually track the performance of any device in any location across your network in real time. The ConnectNow feature automatically draws links between directly-connected physical nodes discovered on your network using both Layer 2 and Layer 3 topology data. In addition to interface status, map links are now capable of providing both interface connection speed and interface utilization information.

Unpluggable Port Mode

SolarWinds NPM enables you to designate selected ports as unpluggable, so unnecessary alerts are not triggered when users undock or shutdown connected devices. This feature is particularly useful for distinguishing low priority ports connected to laptops and PCs from more critically important infrastructure ports.

Data Center Monitoring

SolarWinds NPM offers predefined reports and web console views and resources specifically tailored to provide performance data about Cisco Unified Computing Systems (UCS) and Fiber Channel devices manufactured by Cisco MDS, Brocade, and McData.

VMware Infrastructure Monitoring

SolarWinds NPM enables you to monitor your VMware servers, datacenters, and clusters, including VMware ESX and ESXi, Virtual Center, and any virtual machines (VMs) hosted by ESX servers on your network. Available resources include lists of VMs on selected ESXi and ESX servers, performance details for ESXi and ESX servers and hosted VMs, and relevant charts and reports.

Groups and Dependencies

Groups give you the ability to logically organize monitored objects, regardless of device type or location, and dependencies allow you to more faithfully represent what can actually be known about your network, eliminating “false positive” alert triggers and providing more accurate insight into the status of monitored network objects.

Incident Alerting

You can configure custom alerts to respond to hundreds of possible network scenarios, including multiple condition checks. SolarWinds NPM alerts help you recognize issues before your network users experience productivity hits. Alert delivery methods and responses include email, paging, SNMP traps, text-to-speech, Syslog messaging, and external application execution.

Detailed Historical Reports

Easily configure reports of data from the Orion database over custom time periods. Data is presented in an easily reviewed format in the web console or in the Orion Report Writer application. With over 40 built-in reports available, you can project future trends and capacity needs, and immediately access availability, performance, and utilization statistics. Using the Web-based Report Scheduler, you can email, print or save reports on a regularly scheduled basis, directly from the web console.

Product Update Notifications

Receive regular, automatic notification of updates to your installed Orion monitoring and management applications in the Orion Web Console as soon as they are available from SolarWinds. Product updates can include upgrade opportunities, service packs, and hotfixes.

Orion Product Team Blog

Stay in touch with the people who bring you the products in the Orion family by following the Orion Product Team Blog on thwack, the SolarWinds online user community. Read posts from Orion product managers and developers to learn how to extend and optimize your Orion installation to best meet the needs of your network.

Routing Information

Discover and view routing table information, including VRF data, for monitored nodes, identify flapping routes, and create alerts for detected routing table changes. RIP v2, OSPF v2, OSPF v3/EIGRP, and BGP are currently supported protocols.

Multicast Routing Status and Performance Monitoring

Multicast-specific resources provide group status and real-time monitoring of multicast traffic for Hewlett-Packard (HP) and Cisco devices. Web console resources allow you to see multiple routing table levels. You can also configure alerts to trigger on route changes and traffic thresholds.

Web Console User Auditing

Audit events for web console users are stored in the SolarWinds database, allowing you to keep track of which users are making changes to your network monitoring profile.

Hardware Health Monitoring

Get immediate, visual insight into the operational state of your network with hardware health charts and alerts that show you the number of devices on your network that are functioning in Warning and Critical states.

F5 BIG-IP Monitoring

NPM now specifically supports performance monitoring for F5 devices and interfaces. NPM monitoring for F5 devices and interfaces includes device status and availability, CPU and memory performance statistics, interface performance details, and related graphs and charts.

Interactive Charting for Node and Interface Statistics

SolarWinds NPM charting not only provides historical performance data; the new interactive charting package enables you to zoom in on your charted data, using either fixed time periods or custom date ranges

Training View

The Training view on the Home tab of the SolarWinds Web Console provides a variety of helpful documents and videos that are regularly updated to help you optimize your SolarWinds monitoring environment.

Intuitive SolarWinds NPM Administration

Using the award-winning, intuitive web interface, you can now conduct administrative tasks, such as adding new devices, both individually and in groups, establish unique user accounts, and customize web console displays from anywhere on your network. These administration features allow you to save time by administering NPM tasks remotely without having to RDP directly into your SolarWinds server.

Integrated Wireless Poller

An integrated wireless device poller enables you to leverage proven NPM alerts, reports, and web console resources as you monitor and manage wireless thin and autonomous access points in the same views in which you are already monitoring your wired network devices.

Cisco EnergyWise Monitoring

Cisco EnergyWise technology allows you to responsibly manage energy usage across the enterprise. With NPM, you can view EnergyWise device management data to measure, report, and reduce the energy consumption of any devices connected to EnergyWise-enabled switches.

Universal Device Pollers

The Universal Device Poller allows you to easily add any SNMP-enabled device into the local monitoring database and collect any statistics or information that are referenced in device MIB tables. Using poller transforms available in the Universal Device Poller Wizard, you can also manipulate data collected from multiple Universal Device Pollers to create your own custom statistics and then choose your own customized data display. You may also use Network Atlas to map your Universal Device Pollers.

Integrated Trap and Syslog Servers

SolarWinds NPM allows you to save time when investigating network issues by giving you the ability to use traps and Syslog messages to access network information from a single interface instead of requiring that you poll multiple machines. You can use SolarWinds NPM to easily set up alerts and then receive, process, forward, and send syslog and trap messages.

Coordinated Network, Application, and Configuration Management

SolarWinds provides a complete network management and monitoring solution when SolarWinds NPM is installed with SolarWinds Server & Application Monitor (SAM, formerly Application Performance Monitor, APM), SolarWinds IP Address Manager (IPAM), and the SolarWinds Network Configuration Manager (NCM) integration to monitor network applications, manage IP address and subnet allocations, and manage network device configuration, respectively.

Extensible SolarWinds NPM Modules

With additional SolarWinds modules NetFlow Traffic Analyzer (NTA) and IP SLA Manager (formerly Orion VoIP Monitor) SolarWinds NPM can analyze network traffic and monitor VoIP and WAN traffic using Cisco IP SLA, respectively. NPM modules save time by leveraging the existing SolarWinds NPM deployment to add feature functionality without requiring additional standalone software.

Wireless Heat Maps

NPM allows you to monitor and visualize the wireless signal strength in your office. Create wireless heat maps with the Network Atlas and add them to your Orion Web Console. Wireless heat maps help you identify blind spots and locate your wireless clients.

Device Studio

Create new customized CPU/memory pollers, custom property, or node detail pollers. You can also import pollers created and used by your peers from thwack.com.

Capacity Forecasting

NPM can also provide you with the information when the capacity of your nodes, interfaces and volumes will be fully used, and help you take appropriate measures before full usage issues occur.

Networking Concepts and Terminology

The following sections define the networking concepts and terminology that are used within NPM.

Internet Control Message Protocol (ICMP)

SolarWinds NPM uses the Internet Control Message Protocol (ICMP) to poll for status using **ping** and **echo** requests of managed devices. When SolarWinds NPM polls a managed device using ICMP, if the device is operationally up, it returns a response time and record of any dropped packets. This information is used by SolarWinds NPM to monitor status and measure average response time and packet loss percentage for managed devices.

Note: SolarWinds NPM only uses ICMP to poll devices for status, average response time, and packet loss percentage. Other information displayed in the Orion Web Console may be obtained using SNMP and WMI requests or VMware and UCS APIs.

Simple Network Management Protocol (SNMP)

For most network monitoring and management tasks, NPM uses the Simple Network Management Protocol (SNMP).

SNMP-enabled network devices, including routers, switches, and PCs, host SNMP agents that maintain a virtual database of system status and performance information that is tied to specific Object Identifiers (OIDs). This virtual database is referred to as a Management Information Base (MIB), and SolarWinds NPM uses MIB OIDs as references to retrieve specific data about a selected, SNMP-enabled, managed device. Access to MIB data may be secured either with SNMP Community Strings, as provided with SNMPv1 and SNMPv2c, or with optional SNMP credentials, as provided with SNMPv3.

Notes:

- To properly monitor devices on your network, you must enable SNMP on all devices that are capable of SNMP communications. The steps to enable SNMP differ by device, so you may need to consult the documentation provided by your device vendor.
- If SNMPv2c is enabled on a device you want Orion to monitor, by default, Orion will attempt to use SNMPv2c to poll the device for performance information. If you only want Orion to poll using SNMPv1, you must disable SNMPv2c on the device to be polled.

For more information about MIBs, see Management Information Base (MIB). For more information about SNMP credentials, see SNMP Credentials.

SNMP Credentials

SNMP credentials secure access to SNMP-enabled managed devices. SNMPv1 and SNMPv2c credentials serve as a type of password that is authenticated by confirming a match between a cleartext SNMP Community String provided by an SNMP request and the SNMP Community String stored as a MIB object on an SNMP-enabled, managed device.

SNMPv3 provides a more secure interaction by employing the following fields:

- The **User Name** is a required cleartext string that identifies the agent or poll request that is attempting to access an SNMP-enabled device. **User Name** functions similarly to the SNMP Community String of SNMP v1 and v2c.
- The **Context** is an optional identifying field that can provide an additional layer of organization and security to the information available in the MIB of an SNMP-enabled device. Typically, the context is an empty string unless it is specifically configured on an SNMP-enabled device.
- SNMPv3 provides two optional **Authentication Methods**: Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA1). Both methods, MD5 and SHA1, include the **Authentication Key** with the SNMPv3 packet and then generate a digest of an entire SNMPv3 packet that is then sent. MD5 digests are 16 bytes long, and SHA1 digests are 20 bytes long. When the packet is received, the User Name is used to recreate a packet digest using the appropriate method. Both digests are then compared to authenticate.
- SNMPv3 provides two optional **Privacy/Encryption Methods**:

- Data Encryption Standard (DES56). DES56 uses a 56-bit key with a 56-bit salt to encrypt the SNMP v3 packet data. All packet headers are sent in clear-text.
- Advanced Encryption Standards (AES128, AES192, and AES256) using 128-, 192-, or 256-bit keys, respectively, with 128-, 192-, or 256-bit salts. All packet headers are sent in clear-text.

Password is a Key

The "password is a key" feature, also known as "localized key" means that the hash is computed using a combination of the user defined password and from the SNMP agent's engine ID. This feature can be used instead of plain text authentication on SNMP devices.

Each SNMPv3 agent has an engine ID that uniquely identifies the agent on the device. If a device gets compromised, no other managed or managing devices are affected by it.

If your devices support localized keys and the SNMP settings on your device are set up for authentication with the localized key (hash), you must also make appropriate changes in the Orion node settings.

To set the localized key:

1. Log into the Orion Web Console using an account with administrator privileges.
2. Go to the Edit Node view. Select **Settings > Manage Nodes**, select the node, and then click **Edit Properties**.
3. In the Edit Node view, select the **SNMPv3** polling method.
4. Make sure the **Password is a key** box is selected for **SNMPv3 Authentication** or **Privacy/Encryption**, as appropriate.

Management Information Base (MIB)

A Management Information Base (MIB) is the formal description of a set of objects that can be managed using SNMP. MIB-I refers to the initial MIB definition, and MIB-II refers to the current definition. Each MIB object stores a value such as **sysUpTime**, **bandwidth utilization**, or **sysContact** that can be polled to provide current performance data for any selected device. For example, when polling your network for performance data, Orion Network Performance Monitor sends an **SNMP GET** request to each network device to poll the specified MIB objects. Received responses are then recorded in the Orion database for use in Orion products, including within Orion Web Console resources.

Most network devices can support several different types of MIBs. While most devices support the standard MIB-II MIBs, they may also support any of a number of additional MIBs that you may want to monitor. Using a fully customizable Orion Universal Device Poller, you can gather information from virtually any MIB on any network device to which you have access.

Windows Management Instrumentation (WMI)

Windows Management Instrumentation (WMI) is a proprietary technology used to poll performance and management information from Windows-based network devices, applications, and components. When used as an alternative to SNMP, WMI can provide much of the same monitoring and management data currently available with SNMP-based polling with the addition of Windows-specific communications and security features. For more information about WMI, see the Microsoft article, About WMI.

Notes:

- Due to specific characteristics of WMI polling requests, polling a single WMI-enabled object uses approximately five times the resources required to poll the same or similar object with SNMP on the same polling frequency.
- SolarWinds NPM does not currently use WMI to monitor interfaces.

Agents

You can also poll information about your network devices using agents.
An agent is software that provides a communication channel between the Orion server and a Windows computer. Agents are used to provide packet-level traffic information about key devices and applications that you specify.

The agent allows you to monitor servers hosted by cloud based services such as Amazon EC2, Rackspace, Microsoft Azure, or virtually any other Infrastructure as a Service (IaaS).

Once deployed, all communication between the Orion server and the agent occur over a single fixed port. This communication is fully encrypted using 2048 bit TLS encryption. The agent protocol supports NAT traversal and passing through proxy servers that require authentication.

For more information, see SolarWinds Orion Agents.

How Network Performance Monitor Works

Through ICMP, SNMP, WMI, and Syslog communication and data collection, SolarWinds NPM continuously monitors the health and performance of your network, and it does this without interfering with the critical functions of your network devices. Unlike many other network monitoring products, SolarWinds NPM helps you maintain the overall performance of your network in the following ways:

- NPM does not install outside agents on your mission-critical servers
- NPM does not employ services that take vital resources from critical applications
- NPM does not install any code on monitored network devices. Unmanaged or outdated code can open security holes in your network.

After installing SolarWinds NPM, you can automate the initial discovery of your network, and then simply add new devices for monitoring as you add them to your network. SolarWinds NPM stores all gathered information in a SQL database and provides the highly customizable web console in which to view current and historical network status.

Chapter 2: Installing SolarWinds Network Performance Monitor

SolarWinds Network Performance Monitor (SolarWinds NPM) provides a simple, wizard-driven installation process. For an enterprise-class product, licensing, hardware and software requirements are nominal.

This chapter provides more information about the following topics:

SolarWinds NPM Requirements

SolarWinds recommends installing SolarWinds NPM on its own server, with the Orion database hosted separately, on its own SQL Server. Installations of multiple Orion servers, including SolarWinds NPM, Orion Server & Application Monitor, and Orion Network Configuration Manager using the same database are not supported.

Note: Any and all installed Additional Polling Engines and Additional Web Servers must use the same version that is installed on the primary Orion server.

The following sections provide specific requirements:

- Orion Server Hardware Requirements
- Orion Server Software Requirements
- Requirements for the Orion Database Server (SQL Server)
- Requirements for Virtual Machines and Servers
- Additional Requirements
- SNMP Requirements for Monitored Devices

For recommendations and best practices, consult the following sections:

- Server Sizing
- SQL Server Configuration Best Practices

Orion Server Software Requirements

The following table lists minimum software requirements and recommendations for a SolarWinds Orion installation.

Software	Requirements
Operating System	Windows Server 2003 R2 SP2 (32- or 64-bit) Windows Server 2008, 2008 SP2, 2008 R2, 2008 R2 SP1 Windows Server 2012 and 2012 R2 **Notes:**

Software	Requirements
	• IIS and MSMQ must be installed. SolarWinds recommends that Orion administrators have local administrator privileges to ensure full functionality of local Orion tools. Accounts limited to use of the Orion Web Console do not require administrator privileges. • SolarWinds does not support production installations of Orion products on Windows XP, Windows Vista, Windows 7, or Windows 8 systems. • Evaluation versions of SolarWinds products are supported on Windows 7, Windows 7 SP1, Windows 8 (except for Standard Edition), Windows 8.1 (except for Standard Edition), and Windows 8.1 Update 1 (except for Standard Edition). • SolarWinds products are not compatible with installations of Internet Information Services version 6.0 (IIS6) that make use of web gardens. • SolarWinds SAM installations on Windows Server 2008 require R2. For more information, see "Additional SAM Requirements" in the SolarWinds Server & Application Monitor Administrator Guide. • Installing SolarWinds NPM on Windows Server 2012 R2 Essentials is not supported.
Operating System Languages	English (UK or US), German, Japanese, or Simplified Chinese
IP Address Version	IPv4 or IPv6 implemented as a dual stack. For more information, see RFC 4213 - Basic Transition Mechanisms for IPv6 Hosts and Routers. **Note:** CIDR notation is not currently supported for IPv6 addresses.
Application Ports	**25** (TCP) SMTP port for non-encrypted messages. **161** (UDP) for NPM statistics collection

Software	Requirements
	162 (UDP) for NPM Trap Server listening for incoming messages. **443** (TCP) default port for https binding. Also used for bi-directional ESX/ESXi server polling and for Cisco UCS monitoring. **465** (TCP) for SSL-enabled email alert actions **587** (TCP) for TLS-enabled email alert actions **1801** (TCP) for MSMQ WCF binding. For more information, consult appropriate Microsoft online help. **17777** (TCP) open for Orion module traffic **17778** (HTTPS) open to access the SolarWinds Information Service API **17779** (HTTP and HTTPS) for the SolarWinds Toolset Integration
Web Server	Microsoft IIS, version 6.0 or higher, in 32-bit mode. DNS specifications require that hostnames 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 - DOD Internet Host Table Specification. **Warning:** The following Windows accounts, as configured by IIS 6.0 on Windows Server 2003 with their default security settings, are required: • **IUSR_<hostname>**, as a member of the Guests group ONLY. • **IWAM_<hostname>**, as a member of the IIS_WPG group ONLY. Disabling these accounts or changing any default settings of these accounts may negatively affect the operation of your Orion installation. SolarWinds strongly recommends against altering these accounts or their settings. **Notes:** • SolarWinds does not support installing SolarWinds NPM on domain controllers.

Software	Requirements
	• SolarWinds neither recommends nor supports the installation of any Orion product on the same server or using the same database server as a Research in Motion (RIM) Blackberry server.
.NET Framework	.NET 3.5 SP1 and .NET 4.0.3 **Note:** Both versions 3.5 SP1 and 4.0.3 are required.
Web Console Browser	Microsoft Internet Explorer version 8 or higher with Active scripting Firefox 32.0 or higher (Toolset Integration is not supported on Firefox) Chrome 40.0 or higher Safari for iPhone

Orion Server Hardware Requirements

The following table lists minimum hardware requirements and recommendations for your Orion server.

Note: Hardware requirements are listed by SolarWinds NPM license level.

Hardware	SL100, SL250, or SL500	SL2000	SLX
CPU Speed	2.0 GHz	2.4 GHz	3.0 GHz
	Note: For production environments, quad core is recommended. Physical Address Extension (PAE) should not be enabled.		

Hardware	SL100, SL250, or SL500	SL2000	SLX
Hard Drive Space	2.5 GB	5 GB	20 GB
	Note: A RAID 1 drive for server operating system, Orion installation, and tempdb files is recommended. Orion requires at least 1.5 GB for job engine, information service, collector service, MIB database and other required files. The Orion installer needs 1 GB on the drive where temporary Windows system or user variables are stored. Per Windows standards, some common files may need to be installed on the same drive as your server operating system. For more information, see Working with Temporary Directories.		
Memory	3 GB	4 GB	8 GB

Server Sizing

SolarWinds NPM is capable of monitoring networks of any size, ranging from small corporate LANs to large enterprise and service provider networks. Most SolarWinds NPM systems perform well on 3.0 GHz systems with 3 GB of RAM, using default polling engine settings. However, when monitoring larger networks, you should give additional consideration to the hardware used and the system configuration.

There are three primary variables that affect scalability:

Number of monitored elements

The most important consideration. An element is defined as a single, identifiable node, interface, or volume. Systems monitoring more than 10,000 elements may require tuning for optimal performance.

Polling frequency

The second variable to consider. If you are collecting statistics every five minutes instead of the default nine, the system will have to work harder and system requirements will increase.

Number of simultaneous users

The number of simultaneous users accessing NPM directly impacts system performance.

Recommendations

When planning an SolarWinds NPM installation, there are four main factors to keep in mind with respect to polling capacity: CPU, memory, number of polling engines, and polling engine settings. Be aware of these variables, and consider the following SolarWinds recommendations:

Install NPM and SQL Server on different servers

In most situations, installing NPM and SQL Server on different servers is highly recommended, particularly if you are planning to monitor 2,000 elements or more. If you experience performance problems or you plan to monitor a very large network, you should certainly consider this option. This scenario offers several performance advantages, as the NPM server does not perform any database processing, and it does not have to share resources with SQL Server.

Use additional polling engines for 10,000+ monitored elements

If you plan to monitor 10,000 or more elements, SolarWinds recommends that you install additional polling engines on separate servers to help distribute the work load.

For more information about sizing SolarWinds NPM to your network, contact the SolarWinds sales team or visit www.solarwinds.com.

For minimum hardware recommendations, see SolarWinds NPM Requirements.

For more information about polling engines, see Configuring an Additional Polling Engine.

Requirements for the Orion Database Server (SQL Server)

The following table lists software and hardware requirements for your Orion database server. SolarWinds NPM license levels are provided as a reference.

Requirements	SL100, SL250, or SL500	SL2000	SLX
SQL Server	SolarWinds supports Express, Standard, or Enterprise versions of the following: • SQL Server 2008 without SP, 2008 SP1, 2008 SP2, 2008 SP3, or 2008 SP4		

Requirements	SL100, SL250, or SL500	SL2000	SLX
	• SQL Server 2008 R2 without SP, 2008 R2 SP1, 2008 R2 SP2, 2008 R2 SP3 • SQL Server 2012 without SP, 2012 SP1 (also with AlwaysOn Availability Groups), or with SP2 • SQL Server 2014 (also with AlwaysOn Availability Groups) **Notes:** • The **FullWithSQL** NPM installer package automatically installs SQL Server 2008 R2 SP1 Express. This is recommended for evaluations. • SolarWinds strongly recommends maintaining SolarWinds servers as physically separate from your SQL server. • The recovery model of the database should be set to Simple. SolarWinds does not support other methods. • SQL Server Compact Edition 3.5 SP2 is only supported for NPM evaluations. • Due to latency effects, SolarWinds does not recommend installing your SQL Server and your Orion server or additional polling engine in different locations across a WAN. For more information, see SolarWinds Knowledge Base article, Can I install my Orion server or Additional Polling Engine and my Orion database (SQL Server) in different locations across a WAN? • Either mixed-mode or SQL authentication must be supported. • If you are managing your Orion database, SolarWinds recommends you install the SQL Server Management Studio component.		

Requirements	SL100, SL250, or SL500	SL2000	SLX
	• 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')**		
SQL Server Collation	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		
CPU Speed	2.0 GHz	2.4 GHz	3.0 GHz
Hard Drive Space	2 GB	5 GB	20 GB
	Note: Due to intense I/O requirements, a RAID 1+0 drive is strongly recommended for the SolarWinds database, and data and log files. RAID 5 is not recommended for the SQL Server hard drive. The Orion installer needs at least 1 GB on the drive where temporary Windows system or user variables are stored. Per Windows standards, some common files may need to be installed on drive as your server operating system. For more information, see Working with Temporary Directories.		

Requirements	SL100, SL250, or SL500	SL2000	SLX
Memory	2 GB	3 GB	4 GB
	Note: SolarWinds recommends additional RAM, up to 8 GB, for SolarWinds SAM installations including more than 1000 monitors.		
.NET Framework	.NET is not required if your database is on a separate server.		

SQL Server Configuration Best Practices

This topic provides recommendations about how best to manage the SQL server you are using with your Orion installation.

The standard SQL environment for Orion products contains the following components:

- A dedicated SQL Standard or Enterprise Server
- Directly attached (DAS), RAID 10 storage (I/O subsystem)
- LAN attachment between the main Orion server and any additional components

Maximizing SQL server performance

When planning your SQL server configuration, consider the following information:

- SQL Express is only suitable for very small Orion installations without NTA. NetFlow can be a major factor in database sizing, depending on the incoming flow rates.
- WAN connections should never be used between the SQL server and the Orion server. This includes any additional Orion pollers.
- The SQL Server should not be installed on the Orion server.
- The performance of an SQL server is dependent on the performance of the I/O subsystem.
- The more disks there are in a RAID 10 array, the better.
- Many RAID controllers do not handle RAID 01 well.

Hardware settings for SQL servers

The following section contains the recommended hardware settings for SQL servers, taking different scenarios and the number of logical disks you use.

The following table contains the recommended data storage settings which provide maximum performance.

Component	Recommendation
Orion database	• A dedicated hard drive for data files (.mdf, .ndf). RAID 1+0 is recommended. • A dedicated hard drive for transaction files (.ldf). A disk with fast sequential writing is recommended. A RAID 1+0 setup is recommended.
SQL Server temporary directory (tempdb) database	• A dedicated hard drive for data files (.mdf, .ndf). RAID 1+0 is recommended. • A dedicated hard drive for transaction files (.ldf). A disk with fast sequential writing is recommended. A RAID 1+0 setup is recommended.
SQL Server host system (Windows)	• A dedicated hard drive of any type.

The following table contains the recommended data storage settings with four HDDs on the database server.

Component	Recommendation
Orion database	• A dedicated hard drive for data files (.mdf, .ndf). RAID 1+0 is recommended. • A dedicated hard drive for transaction files (.ldf). A disk with fast sequential writing is recommended. A RAID 1+0 setup is recommended.
SQL Server temporary directory	• A dedicated hard drive for data files (.mdf, .ndf) and the transaction log (.ldf)

Component	Recommendation
(tempdb) database	
SQL Server host system (Windows)	• A dedicated hard drive of any type. This hard drive should be the slowest of the four available disks.

The following table contains the recommended data storage settings with three HDDs on the database server.

Component	Recommendation
Orion database	• A dedicated hard drive for data files (.mdf, .ndf). RAID 1+0 is recommended. • A dedicated hard drive for transaction files (.ldf). A disk with fast sequential writing is recommended. A RAID 1+0 setup is recommended.
SQL Server temporary directory (tempdb) database and SQL Server host system (Windows)	• A dedicated hard drive for tempdb data files (.mdf, .ndf), tempdb transaction log (.ldf), and host system.

If you have two hard drives on your database server, the following setup is recommended:

- Use the disk with the faster sequential writing for the host system and for the transaction log files (.ldf).
- Use the other disk for data files (.mdf, .ldf), for the tempdb data files, and for the tempdb log files.

Note: If there are more databases on a given SQL server, it is strongly recommended that you use dedicated hard drives for the tempdb database. Use at least one hard drive for data files, and one hard drive for the transaction log. The reason for this is that all databases use only one tempdb, therefore the tempdb can be the biggest bottleneck in the I/O subsystem.

Recommendations for multi-CPU systems and the optimal settings of the I/O subsystem

On multi-CPU systems, the performance of some operations can be increased by creating more data files on a single hard drive.

Note: Every logical CPU is considered to be one CPU.

The following example shows the original settings of a system with 16 CPU cores:

- One hard drive for data with the `SolarWindsOrionDatabase.MDF` file in the PRIMARY filegroup.
- One hard drive for the transaction log with the `SolarWindsOrionDatabase.LDF` file.
- One hard drive for the tempdb data with the `tempdb.MDF` file in the PRIMARY filegroup.
- One hard drive for the tempdb transaction log with the `tempdb.LDF` file.

The previous settings can be improved in the following way:

- One hard drive for data, with the following files in the PRIMARY file group:
  - `SolarWindsOrionDatabase01.MDF`
  - `SolarWindsOrionDatabase02.MDF`
  - `SolarWindsOrionDatabase03.MDF`
  - `SolarWindsOrionDatabase04.MDF`
- One hard drive for the transaction log with the `SolarWindsOrionDatabase.LDF` file.
- One hard drive for tempdb data, with the following files in the PRIMARY filegroup:
  - `tempdb01.MDF`
  - `tempdb02.MDF`
  - `tempdb03.MDF`
  - `tempdb04.MDF`
- One hard drive for the tempdb transaction log with the `tempdb.LDF` file.

Notes:

- Having more files in the filegroup help the SQL server to distribute the load generated by multiple threads while working with files.
- The recommended ratio between the number of cores and the files in the filegroup is typically 4:1 or 2:1 (for example, 16 cores and four files, or 16 cores and eight files).
- The size and growth setting for all files in a filegroup must be set to identical values in order to distribute the load evenly.
- For the transaction log, it is not effective to create more files, because the SQL server can only use the first file.
- For the tempdb database, a RAM disk or an SSD disk can be used.
- An SSD disk can be used for data files, but it is not effective for the transaction log where sequential access is most important.

Database file setting recommendations

- It is recommended to pre-allocate as much disk space as possible, because the allocation process can be time-consuming.
- Define an absolute auto-growth setting with a reasonable size (500 MB, 1 GB, and so on), instead of an auto-growth percentage.

Memory setting recommendations

- Do not reserve all memory to the SQL server, because this can lead to a lack of memory for the host operating system.
- Reserve 1 GB of memory to the host operating system if there are no additional services running on the given host system.
- If additional resource-intensive services are running on the host operating system, reserve sufficient memory for the host operating system. SolarWinds does not recommend such configuration.

CPU setting recommendations

- Make sure that power-saving technologies are disabled on the CPU.

Requirements for Virtual Machines and Servers

Orion installations on VMware Virtual Machines and Microsoft Virtual Servers are fully supported if the following minimum configuration requirements are met for each virtual machine.

Note: SolarWinds strongly recommends that you maintain your SQL Server database on a separate physical server.

VM Configuration	Orion Requirements by License Level		
	SL100, SL250, or SL500	SL2000	SLX
CPU Speed	2.0 GHz	2.4 GHz	3.0 GHz
Allocated Hard Drive Space	2 GB	5 GB	20 GB
	Note: Due to intense I/O requirements, SQL Server should be hosted on a separate physical server configured as RAID 1+0. RAID 5 is not recommended for the SQL Server hard drive.		
Memory	3 GB	4 GB	8 GB
Network Interface	Each virtual machine on which Orion is installed should have its own, dedicated network interface card. **Note**: Since Orion uses SNMP to monitor your network, if you are unable to dedicate a network interface card to your Orion server, you may experience gaps in monitoring data due to the low priority generally assigned to SNMP traffic.		

Additional Requirements

The following requirements must also be met to ensure a fully functional monitoring environment.

SysObjectID Access

In order to fully monitor network objects, the SysObjectID of any device to be monitored by SolarWinds must be accessible from the SolarWinds server.

Additional Required SQL Server Components

The Orion Installation Wizard installs the following required x86 components if they are not found on your Orion database server:

- SQL Server System Common Language Runtime (CLR) Types. Orion products use secure SQL CLR stored procedures for selected, non-business data operations to improve overall performance.
- Microsoft SQL Server Native Client
- Microsoft SQL Server Management Objects

SNMP Requirements for Monitored Devices

SolarWinds NPM can monitor the performance of any SNMPv1-, SNMPv2c-, or SNMPv3-enabled device on your network. Consult your device documentation or a technical representative of your device manufacturer to acquire specific instructions for configuring SNMP on your device.

When configuring your SNMP-enabled network devices for monitoring, consider the following points:

- To properly monitor devices on your network, you must enable SNMP on all devices that are capable of SNMP communications.
- Monitored devices must allow access to the `SysObjectID` for correct device identification.
- Unix-based devices should use the configuration of Net-SNMP version 5.5 or higher that is specific to the type of Unix-based operating system in use.
- SolarWinds NPM is capable of monitoring VMware ESX and ESXi Servers versions 4.0 and higher with VMware Tools installed. For more information about enabling SNMP and VMware Tools on your VMware device, consult your VMware documentation or technical representative.
- If SNMPv2c is enabled on a device you want SolarWinds NPM to monitor, by default, SolarWinds NPM will attempt to use SNMPv2c to poll the device for performance information. If you only want SolarWinds NPM to poll using SNMPv1, you must disable SNMPv2c on the device to be polled.

Licensing SolarWinds Network Performance Monitor

SolarWinds NPM can collect data and detailed information from any of your version 3 or earlier SNMP-enabled devices, including routers, switches, firewalls, and servers.

SolarWinds NPM is licensed in accordance with the largest number of the following three types of monitored network elements:

Nodes

Nodes include entire devices, for example, routers, switches, virtual and physical servers, access points, and modems.

Interfaces

Interfaces include switch ports, physical interfaces, virtual interfaces, sub-interfaces, VLANs, and any other single point of network traffic.

Volumes

Volumes are equivalent to the logical disks you are monitoring.

SolarWinds NPM Licensing Levels

The following list provides the different types of SolarWinds Network Performance Monitor licenses that are available:

- An SL100 license allows you to monitor up to 100 nodes, 100 interfaces, and 100 volumes (300 elements in total).
- An SL250 license allows you to monitor up to 250 nodes, 250 interfaces, and 250 volumes (750 elements in total).
- An SL500 license allows you to monitor up to 500 nodes, 500 interfaces, and 500 volumes (1500 elements in total).
- An SL2000 license allows you to monitor up to 2000 nodes, 2000 interfaces, and 2000 volumes (6000 elements in total).
- An SLX license allows you to monitor a virtually unlimited number of elements.

Database size increases with the addition of monitored elements. Depending on the number of elements and the amount of traffic on your network, monitoring more than 10,000 elements can require additional polling engines.

Licensing SolarWinds NPM with Other SolarWinds Products

Your SolarWinds NPM license interacts additively with your other SolarWinds licenses. For example, if you have an NPM SL500 (500 nodes and 500 volumes) installed with SAM AL50, you can monitor a total of 550 nodes (500 NPM nodes + 50 SAM nodes), 550 interfaces, 550 volumes (matching the node count), and 50 application monitors.

Maintaining Licenses

After you finish an Orion product installation, you are automatically prompted to activate your license. You can either activate your product straight away, or if you are under active maintenance, you can activate the license later, using the SolarWinds License Manager.

SolarWinds License Manager is an easily installed, free utility that gives you the ability to manage Orion licenses without contacting SolarWinds Customer Service.

SolarWinds License Manager provides the following capabilities:

- Deactivating licenses on one computer and activating them on another computer without contacting SolarWinds Customer Service
- Upgrading from one production license level to another
- Upgrading from evaluation licenses to production licenses

Note: To be able to use the License Manager, you need to have an active maintenance.

License Manager Requirements

The following table lists the requirements for SolarWinds License Manager.

Item	Requirement
Install Location	SolarWinds License Manager must be installed on the same computer as the products to be migrated.
Connectivity	Computer must have access to the Internet.
.NET Framework	2.0 or later, links to the framework are included in the installation
Operating System	The following operating systems are supported: • Windows Server 2008 and higher, including R2 • Windows Server 2012 • Windows Vista • Windows 7

Item	Requirement
	• Windows 8
Browser	The following browsers are supported: Internet Explorer 8 or later Firefox 2.0 or later Chrome latest version

Notes:

- SolarWinds License Manager does not reset Storage Manager, Virtualization Manager, Mobile Admin, Log & Event Manager, Web Help Desk, and DPA/Confio licenses.
- ipMonitor versions 10 or later are now supported by License Manager. You can reset ipMonitor licenses previous to version 10 by launching the ipMonitor Configuration Program, clicking Software Licensing, and then clicking Park License.
- License Manager must be installed on a computer with the correct time. If the time on the computer is off 24 hours in either direction from the Greenwich Mean Time clock, 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 on which you want to activate, upgrade or synchronize your license or on which you want to deactivate currently licensed products.

Warning: You must install License Manager on a computer with the correct time. If the time on the computer is even slightly off, in either direction, from Greenwich Mean Time (GMT), you cannot reset licenses without contacting SolarWinds Customer Service. Time zone settings neither affect nor cause this issue.

To install License Manager via SolarWinds UI:

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

Note: If problems with License Manager occur, download and install the latest version of License Manager.

2. Click **Next** to accept the SolarWinds EULA.
3. ***If you are prompted to install the SolarWinds License Manager application,*** click **Install**.

Downloading the License Manager from the Internet

To download and install the latest version of the License Manager:

1. Navigate to http://solarwinds.s3.amazonaws.com/solarwinds/Release/LicenseManager/LicenseManager.zip.
2. Unzip the downloaded file, and then run LicenseManager.exe.

Activating Licenses with the License Manager

Activating licenses with the License Manager allows you to manage licenses for multiple SolarWinds products.

You need to activate your license after you have purchased and installed your Orion product, or after you purchase a license key for a currently installed evaluation version of your product.

To activate licenses with the License Manager:

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

   Note: If the License Manager is not installed on the computer, install it first. For more information, see Installing License Manager.

2. Click **Activate** next to the appropriate SolarWinds product.
3. Select whether you have access to the Internet or whether you want to activate your license offline.

Activating Licenses with Internet Access

If you have installed your SolarWinds product on a computer which is connected to the Internet, the license key will be activated via the Internet.

To activate the license, launch the Activation Wizard, and complete the following steps:

i. Select **I have Internet access...**

ii. Find out your activation key in the customer portal, and provide it in the **Activation Key** field.

   a. Browse to https://customerportal.solarwinds.com, and then log in using your Customer ID and password, or your individual user account information.

      Note: If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support at http://www.solarwinds.com/support/ticket/serviceticket.aspx.

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

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

   d. Copy your unregistered activation key for the appropriate SolarWinds product to the clipboard, and then paste it into the **Activation Key** field on the Activate NPM window.

iii. ***If you are using a proxy server to access the Internet***, select **I access the Internet through a proxy server**, and then type the proxy address and port number.

iv. Click **Next** and complete the Activation Wizard.

Activating Licenses Offline

If the computer on which you are installing your Orion product is not connected to the Internet, you need to provide the unique machine ID in the SolarWinds customer portal, download the license key, and complete the activation on the offline computer.

To activate your SolarWinds license for an offline computer, launch the Activation Wizard and complete the following procedure:

i. On the Activate NPM screen, select **This server does not have Internet access**, and click **Next**.

ii. On the Activate Product window to finalize your registration, click **Copy Unique Machine ID**.

iii. Paste the copied data into a new document in a text editor, and then save the text document.

iv. Transfer the document to a computer with Internet access. For example, transfer the document to a shared location.

v. Log on to the SolarWinds customer portal and find out your activation key:

   a. Browse to https://customerportal.solarwinds.com from a computer with Internet access, and then log in using your Customer ID and password, or your individual user account information.

      Note: If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support at http://www.solarwinds.com/support/ticket/serviceticket.aspx.

   b. Click **License Management**.

   c. Browse to the appropriate SolarWinds product, such as Network Performance Monitor, and then click **Manually Register License**.

   d. Provide the Unique Machine ID you transferred earlier, and then download your license key.

   e. Transfer the license key to a shared location.

vi. Return to the offline computer where you have been running the activation wizard, and browse to the shared License Key File location from the Activate Product window.

vii. Click **Next** to continue.

4. Provide your customer data, and then complete the Activation Wizard.
    a. Provide your **First Name**, **Last Name**, **Email** address, and **Phone Number** to register your Orion product, and then click **Next**.
    b. Click **Finish** when your license is activated.
    c. Review and record the information provided on the License Status window, and then click **Close**.

Deactivating and Registering Licenses with the License Manager

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

To be able to deactivate and reuse a license without contacting SolarWinds Customer Service, your product needs to be under active maintenance.

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

    The deactivated licenses are now available to activate on a new computer.

If you deactivated a license on an offline computer, or if you do not have active maintenance, contact Customer Support at maintenance@solarwinds.com to reuse the available license.

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

Upgrading and Synchronizing Licenses

To upgrade a currently installed license:

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

Synchronizing Licenses

For most NPM licenses (Gen3 licenses), you can synchronize the data available on your customer portal with the data in the License Manager.

Synchronizing might include:

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

To synchronize a currently installed license with the SolarWinds Customer Portal:

1. Start the License Manager from the SolarWinds Program group.
2. Select the product whose license you want to synchronize, and then click **Synchronize**.
3. Click **Synchronize** again in the Synchronize Licenses window.

Antivirus Directory Exclusions

To ensure that all Orion products have access to all required files, exclude the following directories, listed by operating system, from antivirus protection.

Windows Server 2003 and Windows XP:

C:\Documents and Settings\All Users\Application Data\SolarWinds

Windows Server 2007, Windows Vista, and Windows 2008

C:\ProgramData\SolarWinds

Notes:

- Do not exclude executable files.
- We assume that C:\ is the default install volume.

Enabling Microsoft Internet Information Services (IIS)

To host the Orion Web Console, Microsoft Internet Information Services (IIS) must be installed and enabled on your Orion server. Windows Server 2003 requires IIS version 6, and Windows Server 2008 requires IIS version 7, as detailed in the following sections:

Enabling IIS on Windows Server 2003

The following procedure enables IIS on Windows Server 2003.

To enable IIS on Windows Server 2003:

1. Click **Start > Control Panel > Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. Click **Application Server**, confirm it is checked, and then click **Details**.
4. Click **Internet Information Services (IIS)**, confirm it is checked, and then click **Details**.
5. Click **World Wide Web Service**, confirm it is checked, and click **Details**.
6. Select **World Wide Web Service**, confirm it is checked, and then click **OK**.
7. Click **OK** on the **Internet Information Services (IIS)** window, and then click **OK** on the **Application Server** window.
8. Click **Management and Monitoring Tools**, confirm it is checked, and then click **Details**.
9. Confirm that both **Simple Network Management Protocol** and **WMI SNMP Provider** are checked, and then click **OK**.
10. Click **Next** on the Windows Components window, and then click **Finish** after completing the Windows Components Wizard.
    Note: You may be prompted to install additional components, to provide your Windows Operating System media, or to restart your computer. Restart your server if prompted, but Orion does not require the Phone Book Service.

11. ***If you are currently enabling IIS as part of an Orion installation,*** restart the Orion installer. For more information, see the installation instructions in the Administrator Guide for your specific Orion product.

Enabling IIS on Windows Server 2008

The following procedure enables IIS on Windows Server 2008.

To enable IIS on Windows Server 2008:

1. Click **Start > All Programs > Administrative Tools > Server Manager**.
2. Click **Roles** in the left pane, and then click **Add Roles** in the main pane.
3. Click **Next** to start the Add Roles Wizard.
4. Check **Web Server (IIS)**.
5. ***If you are prompted to add features required for Web Server (IIS),*** click **Add Required Features**.
6. Click **Next** on the Select Server Roles window, and then click **Next** on the Web Server (IIS) window.
7. Confirm that **Common HTTP Features > Static Content** is installed.
8. Check **Application Development > ASP.NET**, and then click **Add Required Role Services**.
9. Check both **Security > Windows Authentication** and **Security > Basic Authentication**.
10. Check **Management Tools > IIS 6 Management Compatibility**, and then click **Next** on the Select Role Services window.
11. Click **Install** on the Confirm Installation Selections window, and then click **Close** on the Installation Results window.
12. ***If you are currently enabling IIS as part of an Orion installation,*** restart the Orion installer. For more information, see the installation instructions in the Administrator Guide for your specific Orion product.

Enabling IIS on Windows Server 2012

The following procedure enables IIS on Windows Server 2012.

To enable IIS on Windows Server 2012:

1. Click **Start > All Programs > Administrative Tools > Server Manager**.
2. Click **Manage** in the top right, and then click **Add Roles and Features**.
3. Select **Role-based or feature-based installation** as the Installation Type, and then click **Next**.
4. Select the server on which you are enabling IIS, and then click **Next**.
5. Check **Web Server (IIS)** in the list of Server Roles, and then click **Next**.
6. IIS does not require any additional Features. Click **Next**.
7. Review the provided Web Server Role (IIS) notes, and then click **Next**.
8. Confirm that **Common HTTP Features > Static Content** is installed.
9. Check **Application Development > ASP.NET**, and then click **Add Required Role Services**.
10. Check both **Security > Windows Authentication** and **Security > Basic Authentication**.
11. Check **Management Tools > IIS 6 Management Compatibility**.
12. Click **Next** on the Select role services window.
13. Click **Install** on the Confirm installation selections window, and then click **Close** on the Installation Results window.
14. ***If you are currently enabling IIS as part of an Orion installation,*** restart the Orion installer. For more information, see the installation instructions in the Administrator Guide for your specific Orion product.

Enabling and Requiring Secure Channels with SSL

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

The following sections provide procedures for enabling SSL connections to the Orion Web Console:

- Enabling SSL Connections on Windows Server 2008
- Enabling SSL Connections on Windows Server 2012
- Configuring the Orion Web Console for SSL
- Configuring the Web Console to Require SSL

Enabling SSL Connections on Windows Server 2003

The following procedure enables SSL/TLS connections to an Orion Web Console installed on Windows Server 2003.

Notes:

- Secure SSL/TLS communications are conducted over port 443.
- The following procedure does not describe the processes either of obtaining a required certificate or of generating a certificate signing request for a third-party certificate authority. Your server must already have the required SSL certificate installed.
- Due to security concerns, you may want to disable SSL v3.0 and earlier. See Microsoft KBs 187498 or 245030.

To enable SSL connections to the web console on Windows Server 2003:

1. Log on to your NPM server using an account with administrative privileges.
2. Click **Start > Control Panel > Administrative Tools > Computer Management**.
3. Expand **Services and Applications > Internet Information Services (IIS) Manager > Web Sites**.
4. Click **SolarWinds NetPerfMon**, and then click **Action > Properties**.

5. Open the Web Site tab, confirm that **SSL port** is set to **443**, and then click **Apply**.
6. Click **Advanced**.
7. ***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**.
8. Click the Directory Security tab, and then click **Edit** in the Secure communications section.
9. Check **Require secure channel (SSL)**, and then select Accept client certificates in the Client certificates area.
10. Click **OK** on the Secure Communications window.
11. Click **Apply**, and then click **OK** to exit.

Enabling SSL Connections on Windows Server 2008

The following procedure enables SSL/TLS connections to an Orion Web Console installed on Windows Server 2008.

Notes:

- Secure SSL/TLS communications are conducted over port 443.
- The following procedure does not describe the processes either of obtaining a required certificate or of generating a certificate signing request for a third-party certificate authority. Your server must already have the required SSL certificate installed.
- Due to security concerns, you may want to disable SSL v3.0 and earlier. See Microsoft KBs 187498 or 245030.

To enable SSL connections to the web console on Windows Server 2008:

1. Log on to your NPM server using an account with administrative privileges.
2. Click **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
3. In the Connections pane, expand the name of your Orion server, and then expand **Sites**.
4. Click **SolarWinds NetPerfMon**, and then click **Bindings** in the Actions pane on the right.
5. Click **Add** in the Site Bindings window.
6. In the Type: field, select **https**, and then confirm that **Port** is set to **443**.
7. In the SSL Certificate field, select a certificate, and then click **OK**.
8. Click **Close** on the Site Bindings window.
9. In the IIS group, click **SSL Settings**, and then check **Require SSL**.
10. Click **Apply** in the Actions group on the right.
11. In the Connections pane, click **SolarWinds NetPerfMon**.
12. Click **Restart** in the Manage Web Site group on the right.

Enabling SSL Connections on Windows Server 2012

The procedure to enable SSL connections to an Orion Web Console installed on Windows Server 2012 is currently provided in the SolarWinds Knowledge Base article Enabling SSL Connections on Windows Server 2012.

Configuring the Orion Web Console for SSL

The following procedure enables Secure Sockets Layer (SSL) security (https) for the Orion Web Console.

To enable SSL for the Orion Web Console:

1. Log on to your Orion server using an account with administrative rights.
2. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Orion Service Manager**, and then click **Shutdown Everything**.
   Note: It may take a few minutes to stop all services.
3. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Manager**.

4. ***If your SQL Server is not listed in the left pane,*** click **Add default server**.
5. ***If you need to add your Orion database because it is not listed in the left pane,*** complete the following steps:
    a. Click **Add SQL Server**.
    b. Using the format **Server/Instance**, select or provide the SQL Server instance you are using as your Orion database.
    c. Select the appropriate login method, providing credentials as required.
    d. Click **Connect to Database Server**.
6. Expand your Orion database in the left pane.
7. Right-click the **Websites** table, and then click **Query Table**.
8. Replace the default query with the following query:

    UPDATE dbo.WebsitesSET SSLEnabled=1WHERE WebsiteID=1
9. Click **Refresh**.
10. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Orion Service Manager**.
11. Click **Start Everything**.
    Note: It may take a few minutes to restart all services.
12. ***If you want to use a designated SSL port, such as the default https port 443, for the web console,*** complete the following procedure to change the web console port:
    a. Click **Start > All Programs > SolarWinds Orion > Configuration and Auto-Discovery > Configuration Wizard**.
    b. Check **Website**, and then click **Next** on the Welcome window.
    c. Enter the designated SSL port number in the **Port** field, and then click **Next**.
    Note: Port 443 is typically reserved for SSL traffic.
    d. Review the configuration summary, and then click **Next**.
    e. Click **Finish** when the Configuration Wizard completes.

Configuring the Web Console to Require SSL

The following procedure configures the web console to require SSL connections.

To configure the web console to require SSL:

1. In a text editor, open the web console configuration file, **web.config**, on your primary SolarWinds server.

   Note: By default, **web.config** is located in **C:\Inetpub\SolarWinds**.

2. In the **<system.web>** section, add the following line:
   <httpCookies requireSSL="true" />
3. Locate the line **<forms loginUrl="~/Orion/Login.aspx"/>**, and then edit it to **<forms loginUrl="~/Orion/Login.aspx" requireSSL=”true” />**.
4. ***If you want to enable the HTTPOnly flag for added security,*** locate the **<httpCookies>** tag, and then edit it to the following:
   <httpCookies httpOnlyCookies="true" requireSSL="true" />
5. Save and close **web.config**.

Enabling FIPS

SolarWinds has developed the FIPS 140-2 Manager to direct you in configuring your SolarWinds software for FIPS 140-2 compliance.

To configure a FIPS-compliant SolarWinds installation:

1. Configure the server on which you have installed your SolarWinds software for FIPS compliance. For more information, see the Microsoft Support knowledge base article, System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing security setting effects in Windows XP and in later versions of Windows.
2. Start the SolarWinds FIPS 140-2 Manager (`SolarWinds.FipsManager.exe`)
   Note: By default, `SolarWinds.FipsManager.exe` is located in *`Install_Volume:`*`\Program Files (x86)\`.
3. Review the welcome text, and then click **Next**.
4. ***If you have configured your SolarWinds server to use FIPS-compliant algorithms for encryption, hashing and signing***, the SolarWinds FIPS 140-2 Manager will attempt to confirm that the current configuration of your SolarWinds products is FIPS-compliant.
5. ***If any currently installed SolarWinds products are not FIPS compliant,*** the FIPS Manager will notify you of which SolarWinds modules are not FIPS-compliant. Click **Close**, and then remove any non-compliant SolarWinds modules from your FIPS-compliant server before running the FIPS 140-2 Manager again.
   Note: SolarWinds recommends that you install all FIPS-compliant SolarWinds software on specifically FIPS-compliant servers and separately maintain all non-compliant software on specifically non-compliant servers.
6. ***If FIPS 140-2 is currently is disabled,*** check **Enable FIPS 140-2**, and then click **Next**.
7. The FIPS Manager may provide a list of objects and saved network discovery definitions that are not FIPS-enabled.
   Note: This list of non-compliant objects does not auto-refresh. To refresh the list of non-compliant objects after editing required credentials, restart the FIPS 140-2 Manager.

8. For each listed object that is not FIPS-compliant:
    a. Click the non-compliant object.
    b. ***If the non-compliant object is a monitored node,*** edit its Polling Method properties as follows:
        - Select **SNMPv3** as the **SNMP Version**.
        - Select FIPS-compliant **Authentication** and **Privacy/Encryption** methods, and provide appropriate passwords.
          Note: SHA1 is a FIPS-compliant authentication method. AES128, AES192, and AES256 are FIPS-compliant Privacy/encryption methods.
        - Click **Submit**.
    c. ***If the non-compliant object is a network discovery,*** edit SNMP credentials as follows:
        - Confirm that all SNMP credentials are SNMPv3. Either delete or edit any credentials that are not VIPS-compliant SNMPv3.
        - Confirm that all SNMP credentials use FIPS-compliant FIPS-compliant **Authentication** and **Privacy/Encryption** methods, and provide appropriate passwords.
          Note: SHA1 is a FIPS-compliant authentication method. AES128, AES192, and AES256 are FIPS-compliant Privacy/encryption methods.
        - Complete the Network Sonar Wizard using the updated credentials.
9. ***If all monitored objects and network discoveries are FIPS-compliant,*** click **Restart now** to restart all relevant SolarWinds services.

Installing SolarWinds Network Performance Monitor

Any installation or upgrade of SolarWinds NPMrequires completion of both the installer and the Configuration Wizard, as detailed in the following sections:

- Completing a SolarWinds NPM Installation
- Completing the Orion Configuration Wizard

Notes:

- Downgrades of Orion products are not supported.
- If you are upgrading or installing multiple Orion products, confirm that you are installing them in the order given in the Upgrade Instructions located in your SolarWinds Customer Portal.
- If you are upgrading from a previous version of Orion Network Performance Monitor, see Upgrading SolarWinds Network Performance Monitor.

Completing a SolarWinds NPM Installation

Before completing a SolarWinds NPM installation, ensure that the server on which you are installing SolarWinds NPM currently meets or exceeds stated requirements. For more information, see SolarWinds NPM Requirements.

Notes:

- If you are using Internet Explorer, SolarWinds recommends that you add the URL of your Orion website (**http://FullOrionServerName/**), the URL of SolarWinds support (**http://support.solarwinds.com**), and **about:blank** to the list of trusted sites. For more information about adding sites to your trusted sites list, see the Microsoft help online.
- For evaluation purposes only, SolarWinds NPM may be installed on Windows 7, Windows XP, or Windows Vista. SolarWinds does not, however, support or recommend installing SolarWinds NPM on these operating systems in production environments.
- When installing SolarWinds NPM on Windows XP, you must confirm that Shared Memory, Named Pipes, and TCP/IP are enabled on remote databases.

- **SolarWinds does not support or allow** installations of SolarWinds NPM on domain controllers.

To install SolarWinds Network Performance Monitor:

1. Log on to your SolarWinds NPM server as an administrator.
2. Run the SolarWinds NPM executable.
3. If prompted, install requirements:
    a. Click **Install**, and then complete the installation.
    b. If required, reboot the computer.

    Notes:

    - Downloading and installing both Microsoft .NET Framework 3.5 SP1 and Microsoft .NET Framework 4.0.3 may take more than 20 minutes, depending on your existing system configuration.
    - If a reboot is required, you might need to run the executable again.
4. ***If you want to help us improve our products and send anonymous data about your Orion usage to SolarWinds,*** select **Send usage statistics...**.
5. Review the Welcome text, and then click **Next**.
6. Select your preferred language, and then click **Next**.
   Note: This selection cannot be changed later.
7. ***If the Orion Network Performance Monitor Setup Wizard detects that Microsoft Internet Information Services (IIS) is not installed,*** select **Suspend installation to manually install IIS**, click **Finish**, quit setup, and then install IIS.

   Note: The Orion Web Console requires that Microsoft IIS is installed on the NPM Server. If you do not install IIS at this point, you must install IIS later, and then configure a website for the Orion Web Console to use.
8. ***If an IIS installation was required,*** launch the installer again, and then click **Next** on the Welcome window.
   Note: A server reboot may be required after installing IIS.

9. Accept the terms of the license agreement, and then click **Next**.
10. ***If you want to install SolarWinds NPM in a destination folder other than the default given,*** click **Browse**, select an installation folder, and then click **OK**.
11. Click **Next** on the Choose Destination Location window.
12. Specify whether you want to enable quality of experience traffic monitoring now or later:
    - To test monitoring and analyzing application traffic via QoE, select **Enable QoE traffic monitoring now**.
    - For an advanced configuration of QoE, select **Enable QoE later**. For more information about QoE monitoring, see Monitoring Quality of Experience.
13. Review what will be installed and click **Next** to start copying the files.
14. Wait until the installation is complete.
15. Review the summary and click **Finish** to exit the wizard.

You have completed your NPM installation.

Next Steps:

- You might be prompted to activate your license. Continue evaluation or activate your license. For more information about activating your license, see Activating SolarWinds Licenses.
- Complete the Configuration Wizard. For more information, see Completing the Orion Configuration Wizard.

Activating SolarWinds Licenses

After you have installed your Orion product, you may be prompted to provide your licensing information (software license key and customer data) and thus activate your product.

- To postpone the activation, click **Continue Evaluation**. You can activate the license later, via the License Manager. For more information, see Activating Licenses with the License Manager.
- To activate the license immediately, click **Enter Licensing Information** and complete the following procedure:

To activate your SolarWinds license:

1. Click **Enter Licensing Information** to launch the Activation Wizard.
2. Select whether you have access to the Internet or whether you want to activate your license offline.

   ### Activating Licenses with Internet Access

   If you have installed your SolarWinds product on a computer which is connected to the Internet, the license key will be activated via the Internet.

   To activate the license, launch the Activation Wizard, and complete the following steps:

   i. Select **I have Internet access...**

   ii. Find out your activation key in the customer portal, and provide it in the **Activation Key** field.

      a. Browse to https://customerportal.solarwinds.com, and then log in using your Customer ID and password, or your individual user account information.

         Note: If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support at http://www.solarwinds.com/support/ticket/serviceticket.aspx.

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

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

      d. Copy your unregistered activation key for the appropriate SolarWinds product to the clipboard, and then paste it into the **Activation Key** field on the Activate NPM window.

   iii. ***If you are using a proxy server to access the Internet***, select **I access the Internet through a proxy server**, and then type the proxy address and port number.

   iv. Click **Next** and complete the Activation Wizard.

   ### Activating Licenses Offline

   If the computer on which you are installing your Orion product is not

connected to the Internet, you need to provide the unique machine ID in the SolarWinds customer portal, download the license key, and complete the activation on the offline computer.

To activate your SolarWinds license for an offline computer, launch the Activation Wizard and complete the following procedure:

i. On the Activate NPM screen, select **This server does not have Internet access**, and click **Next**.

ii. On the Activate Product window to finalize your registration, click **Copy Unique Machine ID**.

iii. Paste the copied data into a new document in a text editor, and then save the text document.

iv. Transfer the document to a computer with Internet access. For example, transfer the document to a shared location.

v. Log on to the SolarWinds customer portal and find out your activation key:

   a. Browse to https://customerportal.solarwinds.com from a computer with Internet access, and then log in using your Customer ID and password, or your individual user account information.

      Note: If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support at http://www.solarwinds.com/support/ticket/serviceticket.aspx.

   b. Click **License Management**.

   c. Browse to the appropriate SolarWinds product, such as Network Performance Monitor, and then click **Manually Register License**.

   d. Provide the Unique Machine ID you transferred earlier, and then download your license key.

   e. Transfer the license key to a shared location.

vi. Return to the offline computer where you have been running the activation wizard, and browse to the shared License Key File location

from the Activate Product window.

vii. Click **Next** to continue.

3. Provide your customer data, and then complete the Activation Wizard.
    a. Provide your **First Name**, **Last Name**, **Email** address, and **Phone Number** to register your Orion product, and then click **Next**.
    b. Click **Finish** when your license is activated.
    c. Review and record the information provided on the License Status window, and then click **Close**.

Completing the Orion Configuration Wizard

The following procedure using the Orion Configuration Wizard completes and configures your SolarWinds NPM installation.

Notes:

- Confirm that you have designated a SQL Server database instance for SolarWinds NPM. For more information, see SolarWinds NPM Requirements.
- Confirm that the Internet Information Services (IIS) Manager is not open while the Configuration Wizard is running.
- SolarWinds recommends that you close any and all browsing sessions that may be open to the web console before starting the Configuration Wizard.
- During configuration, the Orion polling engine will shut down temporarily with the result that, if you are actively polling, you may lose some polling data.
- SolarWinds recommends that you perform upgrades during off-peak hours of network usage to minimize the impact of this temporary polling stoppage.

To configure your Orion product:

1. ***If the Configuration Wizard has not loaded automatically,*** click **Start > All Programs > SolarWinds Orion > Configuration and Auto-Discovery > Configuration Wizard**.
2. Click **Next** on the Welcome dialog of the Configuration Wizard.

3. ***If you are prompted to stop services,*** click **Yes**.

   Note: To ensure that all updates and changes are installed correctly, it is imperative that you stop all services.

4. Specify the **SQL Server** instance you want to use to store network data and click **Next** to continue.

   a. Select an SQL Server from the list

   b. Select the appropriate authentication method (Windows Authentication or SQL Server Authentication). For SQL Server Authentication, provide credentials to log into the selected instance.

   Notes:

   - In general, SolarWinds recommends using SQL Server Authentication to ensure that the NPM server can always access the SQL Server, even when it is hosted remotely on a separate server.
   - For more information about database authentication, see Database Authentication.

5. Specify the SQL Database:

   Note: SolarWinds recommends against using non-alphanumeric characters in database names.

   - ***If you are using an existing database,*** select **Use an existing database**, type the database name or select it from the list, and then click **Next**.

6. Specify the account for accessing the SQL database:

   - ***If you want to create a new SQL account for the SolarWinds NPM polling engine and web console to use for accessing the database,*** select **Create a new account**, provide an account name and password, confirm the account password, and then click **Next**.
   - ***If you want to use an existing SQL account to provide database access to the SolarWinds NPM polling engine and web console,*** select the existing account, provide the appropriate password, and then click **Next**.

7. Specify settings for the Orion Web Console, and then click **Next**.

    a. ***If you need to specify a particular IP Address for the Orion Web Console,*** provide the **IP address** of the host web server.

    Note: SolarWinds recommends the default **(All Unassigned)** unless your environment requires a specific IP address for your Orion Web Console.

    b. Specify both the **Port** through which you want to access the web console and the **Website Root Directory** into which you want to install web console files.

    Note: If 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 **10.120.0.3** and port **8080**, the URL used to access the web console is `http://10.120.0.3:8080`.

    c. ***If you want to enable automatic login using Windows Authentication,*** select **Yes – Enable automatic login using Windows Authentication**.

    Note: Manual login using Windows Authentication is always available, regardless of whether or not automatic login is enabled.

8. ***If you are prompted to create a new directory,*** click **Yes**.
9. ***If you are prompted to create a new website,*** click **Yes**.

    Note: Choosing to overwrite the existing website will not result in the deletion of any custom SolarWinds NPM website settings you may have previously applied.

10. Confirm that all services you want to install are selected and click **Next** to continue.

    Note: Typically, all listed services should be selected for installation.

11. ***If you are prompted to disable the SNMP Trap Service and enable the SolarWinds Trap Service,*** click **Yes** to disable the (Windows) SNMP Trap Service and enable the SolarWinds Trap Service.
12. Review the final configuration items, and then click **Next**.
13. Click **Next** on the Completing the Orion Configuration Wizard dialog.

14. Click **Finish** when the Orion Configuration Wizard completes.
15. Log in to the Orion Web Console as an administrator.

    Notes:

    - By default, until you change your account, you can log in with User name **Admin** and no password.
    - If you are prompted to install the Toolset integration (**SWToolset.exe**), click **More Options**, select a response, and then click **Install** or **Don't Install**, as appropriate.
16. ***If you need to discover and add network devices to the Orion database,*** the Network Discovery Wizard starts. For more information, see Discovering and Adding Network Devices.

Database Authentication

When you are configuring the SolarWinds Orion database, you are required to select the authentication method used by the SolarWinds NPM user to access the selected SolarWinds Orion database. In general, SolarWinds recommends that you use SQL Server Authentication to ensure that the SolarWinds NPM server can always access the SolarWinds Orion database, even when it is hosted remotely on a separate server.

Notes

- The selected SQL Server instance must support mixed-mode or SQL authentication with strong passwords.
  A strong password must meet at least three of the following four criteria:
  - Contains at least one uppercase letter.
  - Contains at least one lowercase letter.
  - Contains at least one number.
  - Contains at least one non-alphanumeric character, e.g., #, %, or ^.
- ***If you are using SQL Express,*** specify your instance as (`local`) and use a strong password. Due to its inherent limitations, SolarWinds recommends against the use of SQL Express in production environments.

- ***If you are creating a new database,*** the user account must be a member of the `dbcreator` server role. The sysadmin role and the SA user account are always members of `dbcreator`.
- ***If you are using an existing database,*** the user account needs only to be in the `db_owner` database role for the existing database.
- ***If you are creating a new SQL account for use with Orion NPM,*** the user account must be a member of the `securityadmin` server role.

  Note: The sysadmin role and the SA user account are always members of `securityadmin`.
- ***If you are using an existing SQL account,*** the user account needs only to be in the `db_owner` database role for the SolarWinds Orion database.

Upgrading SolarWinds Network Performance Monitor

Complete the following procedure when you are upgrading SolarWinds NPM from a previous version or upgrading the licensed number of elements you can monitor.

Notes:

- SolarWinds does not currently support upgrades from one locale to another. If you want to upgrade your SolarWinds installation to use a new locale, you must complete a clean SolarWinds installation using the new locale.
- SolarWinds recommends that you backup your database before any upgrade. For more information about creating database backups, see Managing the Orion Database.
- While it is being upgraded, your SolarWinds NPM polling engine will shutdown temporarily with the result that you may lose some polling data. SolarWinds recommends that you perform upgrades during off-peak hours of network usage to minimize the impact of this temporary polling stoppage.
- Discovery profiles from older SolarWinds NPM versions are not retained through upgrades. If you want to retain a discovery profile, prior to starting your upgrade, externally record the configuration of the profiles you want to retain.

Upgrade Instructions on the Customer Portal

Specific instructions for completing an upgrade are available in the SolarWinds Customer Portal. If you are upgrading an SolarWinds NPM installation that includes other Orion modules, consult the upgrade information on Customer Portal:

1. Log in to your SolarWinds Customer Portal at https://customerportal.solarwinds.com//.
2. Click **License Management**, and then click **Upgrade Instructions** under the license listing of any Orion product.

To upgrade SolarWinds Network Performance Monitor:

1. ***If you are using more than one polling engine to collect network information,*** shut down all polling engines.
2. Log on to the computer on which you want to upgrade SolarWinds Network Performance Monitor using an account with administrative privileges.
3. Launch the SolarWinds NPM executable.
4. Review the Welcome text, and then click **Next**.
5. SolarWinds Network Performance Monitor automatically detects the previous installation. When prompted to upgrade the current installation, click **Next**.

   Note: All customizations, including web console settings, are preserved.
6. Accept the terms of the license agreement, and then click **Next**.
7. Confirm the current installation settings, and then click **Next** on the Start Copying Files window.
8. Provide required licensing information on the Install Software License Key window.

   Note: You need your customer ID and password to successfully install the key. For more information, see Activating SolarWinds Licenses.
9. Click **Continue**, and then click **Continue** again when the license is installed.
10. Review the Upgrade Reminder, and then click **Next**.
11. Click **Finish** on the InstallShield Wizard Complete window.
12. Complete the Configuration Wizard. For more information, see Completing the Orion Configuration Wizard.

Upgrading an Evaluation License

Upgrading an evaluation license requires that you purchase the appropriate license and activate it.

The standard SolarWinds NPM evaluation period is 30 days. At the end of this period you will be prompted to either buy a license to SolarWinds NPM or enter information corresponding to an SolarWinds NPM license you have already purchased. You can upgrade your evaluation license at any point in your evaluation period, if you have purchased an SolarWinds NPM license.

To upgrade a SolarWinds NPM evaluation license:

1. Click **Start > All Programs > SolarWinds Orion > Network Performance Monitor > Network Performance Monitor Licensing**.
2. Click **Enter Licensing Information**.
3. Activate your license. For more information, see Activating SolarWinds Licenses.

Uninstalling SolarWinds NPM

The following procedure fully uninstalls SolarWinds NPM and deletes the SolarWinds Orion database.

Notes:

- This is a general uninstall procedure, and it may differ slightly from version to version.
- This is the recommended procedure when installing daily builds for testing.

To fully uninstall SolarWinds NPM and remove the SolarWinds Orion database:

1. Click **Start > Control Panel > Add or Remove Programs**.
2. One-by-one, select the following items, click **Remove** for each of them, and complete the uninstall wizard:
   - **SolarWinds Network Performance Monitor...**
   - **SolarWinds Job Engine**
   - **SolarWinds Orion Information Service**
3. Start the Registry Editor and delete SolarWinds-specific folders.
   a. Click **Start > Run**...
   b. Type **regedit**, and then click **OK**.
   c. Expand **HKEY_LOCAL_MACHINE > Software**.
   d. Delete both the SolarWinds and the SolarWinds.net folders.

   If you are uninstalling SolarWinds NPM from a 64-bit computer, expand HKEY_LOCAL_MACHINE > Software > Wow6432Node, and then delete both the SolarWinds and the SolarWinds.net folders.

4. Delete the SolarWinds-specific folders in the following locations:
    - Delete the **Program Files** folder on your main volume. Typically, the Program Files folder is located at **C:\Program Files**.
    - Delete the **Program Files\Common Files** folder on your main volume. Typically, the Common Files folder is located at **C:\Program Files\Common Files**.
    - Delete the **All Users\Application Data\ directory**. Typically, this SolarWinds folder is located in **C:\Documents and Settings\All Users\Application Data**.
    - Delete the SolarWinds website directory. Typically, the SolarWinds website directory is located in **C:\Inetpub**.
5. Using your SQL Server tools, delete your SolarWinds Orion database and your Orion database user.
    - The SolarWinds Orion database is typically named **SolarWindsOrion**, and it can be found in the Databases folder of your SQL Server management application.
    - The default SolarWinds Orion database user is **SolarWindsNPM**. To find the user, expand **Security > Logins** in your SQL Server management application.

Chapter 3: Discovering and Adding Network Devices

Orion products use either Network Sonar discovery and import or Node Management in the Orion Web Console to discover objects for monitoring. The method recommended largely depends on the number of devices to be added.

- To discover and add a larger number of devices across your enterprise, the Network Sonar and Network Sonar Results Wizards are available. For more information, see Network Discovery Using the Network Sonar Wizard.
- The web console provides an easy-to-use Web Node Management to discover and add individual objects for monitoring. For more information, see Adding Devices for Monitoring in the Web Console.

There are two ways—Web Node Management and Network Sonar discovery—to add nodes to the Orion database. To discover and add a larger number of devices across your enterprise, the Network Sonar and Network Sonar Results Wizards are available. This chapter provides instructions for quickly populating your NPM database with the network objects you want to monitor and manage with NPM. The Orion Web Console also provides an easy-to-use Web Node Management wizard suited to discovering and adding individual network objects. For more information, see Monitoring Devices in the Web Console.

Network Discovery Using the Network Sonar Wizard

Orion platform products employ the easy-to-use Network Sonar Wizard to discover devices on your network.

Before using the Network Sonar Wizard, consider the following points about network discovery:

- The Network Sonar Wizard recognizes network devices that are already in your SolarWinds Orion database and prevents you from importing duplicate devices.
- CPU and Memory Utilization charts are automatically enabled for your Windows, Cisco Systems, VMware, and Foundry Networks devices.
- The community strings you provide in the Network Sonar Wizard are only used for SNMP **GET** requests, so read-only strings are sufficient.

When you add credentials in the Network Sonar Wizard, Orion automatically adds those credentials to the Credential Manager so that you can reuse them later on without having to enter them every time.

To discover devices on your network:

1. Log on to the Orion Web Console and navigate to **Settings > Network Sonar Discovery**.
2. Click **Add New Discovery** to create a new discovery. Select a discovery, and use one of the following choices if you already have a discovery.
    - Click **Discover Now** to use an existing discovery to rediscover your network, select the discovery you want to use, and then complete the Network Sonar Results Wizard after discovery completes.
    - Click **Edit** to modify an existing discovery before using it.
    - Click **Import All Results** to import some or all devices found in a defined discovery that you may not have already imported for monitoring.
    - Click **Import New Results** to import any newly enabled devices matching a defined discovery profile.

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

3. To add the custom SNMP credentials or SNMPv3 credentials, complete the following steps.

   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 order them in the list.
   - If you intend to use SNMPv3 for monitoring VLAN interfaces on Cisco devices, confirm that all relevant VLAN contexts are added to all VLAN groups defined for your monitored Cisco devices.

   a. Click **Add New Credential**, and then select the **SNMP Version** of your new credential.
   b. ***If you are using a credential you have already provided,*** select this credential in the **Choose Credential** field.
   c. ***If you are adding an SNMPv1 or SNMPv2c credential,*** provide the new **SNMP Community String**.
   d. ***If you are adding an SNMPv3 credential,*** provide the following information for the new credential:
      - **User Name**, **Context**, and **Authentication Method**
      - **Authentication Password/Key**, **Privacy/Encryption Method** and **Password/Key**, if required.
   e. Click **Add**.

4. Click **Next** on the SNMP Credentials view.
5. To check nodes polled by agents for updates, select **Check all existing nodes polling with agents for node changes and updates**. For more information, see Using the Network Sonar Wizard to Check Agent Polled Nodes.
6. Click **Next** on the Check All Nodes Currently Polling with Agents for Updates view.

7. To discover any VMware VCenter or ESX Servers on your network, confirm that **Poll for VMware** is checked, and then complete the following steps to add or edit required VMware credentials.

   Note: Repeat the following procedure for each new credential. To speed up discovery, use the arrows to move the most commonly used credentials on your network to the top of the list.

   a. Click **Add vCenter or ESX Credential**.
   b. ***If you are using an existing VMware credential,*** select the appropriate credential from the **Choose Credential** dropdown menu.
   c. ***If you are adding a new VMware credential,*** select **<New Credential>** in the **Choose Credential** dropdown menu, and then provide a new credential name in the **Credential Name** field.

      Note: SolarWinds recommends against using non-alphanumeric characters in VMware credential names.

   d. Add or edit the credential **User Name** and **Password**, as necessary.

      Note: The default ESX user name is **root**.

   e. Confirm the password, and then click **Add**.
8. Click **Next** on the Local vCenter or ESX Credentials for VMware view.
9. To discover any WMI- or RPC-enabled Windows devices on your network, complete the following steps to add or edit credentials.

   a. Click **Add New Credential**.
   b. ***If you are using an existing Windows credential,*** select the appropriate credential from the **Choose Credential** drop down menu.
   c. ***If you are adding a new Windows credential,*** select **<New Credential>** in the **Choose Credential** drop down menu, and then provide a new credential name in the **Credential Name** field.

      Note: SolarWinds recommends against using non-alphanumeric characters in Windows credential names.

   d. Add or edit the credential **User Name** and **Password**, as necessary.
   e. Confirm the password, and then click **Add**.

Notes:

- SolarWinds does not poll interfaces on WMI- or RPC-enabled nodes.
- Repeat the following procedure for each new credential. To speed up discovery, use the arrows to move the most commonly used credentials on your network to the top of the list.

10. Click **Next** on the Windows Credentials view.
11. 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**.

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

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

    c. ***If you want to delete one of multiple ranges,*** click **X** next to the IP range you want to delete.

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

12. 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. 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**.

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

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

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

13. To add IPv6 devices or devices that you already know their IP addresses or hostnames, complete the following procedure:

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

    b. Type the IPv4 or IPv6 addresses or hostnames of the devices you want to discover for monitoring into the provided field.

    Note: Type only one hostname, IPv4 address, or IPv6 address per line.

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

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

14. Configure the options on the Discovery Settings view, as detailed in the following steps.

    a. 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.

b. 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.

c. 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.

d. 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.

e. Position the slider to type a value to set the number of WMI Retries.

Note: This value is the number of times Network Sonar Discovery will retry a failed WMI credential.

f. Position the slider or type a value to set how long Network Sonar Discovery waits before trying the WMI credentials again in WMI Retry Interval.

g. 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.

h. 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. To discover devices that respond to SNMP or WMI, check **Ignore nodes that only respond to ICMP (ping). Nodes must respond to SNMP, WMI**.

    Note: By default, Network Sonar uses ICMP **ping** requests to locate devices. Most information about monitored network objects is obtained using SNMP queries, but Network Sonar can also use WMI to monitor devices.

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. Configure a schedule for your discovery.

    To run the discovery only once, perform the following steps.

    a. Select **Once** from the **Frequency** list, and then specify whether you want to run the discovery immediately or not by selecting the appropriate option.

    To run on a regular schedule, perform either of the following steps.

    a. To set up a discovery in an hourly frequency, select **Hourly** from the **Frequency** list, and then provide the number of hours to pass between two discoveries.
    b. To set up a discovery to run once daily, select **Daily** from the **Frequency** list, and then provide the time at which you want your discovery to run every day, using the format **HH:MM AM/PM**.
    c. To set up a discovery to run at another specific frequency, select **Advanced** from the **Frequency** list, and then click **Add Frequency**. Provide a name for the frequency, and then select the appropriate frequency from the list. Depending on your selection, specify the dates and times, select whether you want to start the discovery right now, or at a specific date, and optionally specify the end date for the scheduled discovery. After specifying your settings, click **Add Frequency**.

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.

    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. For more information about managing scheduled discovery results, see Managing Scheduled Discovery Results.
    - 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.

Using the Network Sonar Results Wizard

The Network Sonar Results Wizard directs you through the selection of devices for monitoring.

It opens when the Network Sonar Wizard completes or when you click either **Import All Results** or **Import New Results** for a selected discovery. For more information, see Network Discovery Using the Network Sonar Wizard.

To select the results of a network discovery for monitoring:

1. On the Device Types to Import page, check the device types you want to monitor, and then click **Next**.
   Note: If you are not sure you want to monitor a specific device type, check the device type in question. If you do not want to monitor a selected device later, delete the device using Web Node Management.
2. Select the interfaces you want to monitor or filter the results to specific interfaces, and then click **Next**.
   Note: If you are not sure you want to monitor a specific interface type, check the interface type in question. If you do not want to monitor a selected interface later, delete it using Web Node Management.
   a. In the Selection Criteria area, check the appropriate **Status**, **Port Mode**, and **Hardware** properties of the interfaces you want to monitor.
   b. To select discovered interfaces using keywords, phrases or regular expressions, click **+** to expand **Advanced selection options**, select from the available advanced options, as desired, and then click **Reselect Interfaces**.
   c. In the List of Interfaces area, check the Interface Types you want to monitor, and then click **Next**.
3. On the Volume Types to Import page, check the volume types you want to monitor, and then click **Next**.
   Note: If you are not sure you want to monitor a specific volume type, check the volume type in question. If you do not want to monitor any volume of the selected type later, delete the volume using Web Node Management.
4. To import nodes, even when they are already known to be polled by another polling engine, check the option in the **Allow Duplicate Nodes** section. For more information about working with multiple polling engines, see Managing Orion Polling Engines.

5. ***If there are any devices on the Import Preview that you do not ever want to import,*** check the device to ignore, and then click **Ignore**. Selected nodes are added to the Discovery Ignore List. For more information, see Using the Discovery Ignore List.
6. Confirm that the network objects you want to monitor are checked on the Import Preview page, and then click **Import**.
7. After the import completes, click **Finish**.
   Note: Imported devices display in the All Nodes resource.

Adding Devices for Monitoring in the Web Console

The following procedure shows how to add a device for monitoring in the Web Console.

Note: This procedure does not cover the addition of objects specifically monitored by individual Orion platform products. For more information, see the Administrator Guide for each specific Orion product.

To add a device for monitoring in the Orion Web Console:

1. Log in to the Web Console as an administrator.
2. Click **Settings** in the top right of the web console.
3. Click **Manage Nodes** in the Node & Group 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 the IP address of the node you are adding is dynamically assigned,*** check **Dynamic IP Address**.
7. Select the Polling Method to be used to monitor this node:
    a. ***Select* External Node: No Status *if you do not want to collect data from the node***. Use this if you want to monitor a hosted application or other element attached to the node but not the node itself.
    b. ***Select Status Only: ICMP if the node does not support SNMP or WMI***. This will collected only status, response time and packet loss.
    c. ***Select Most Devices: SNMP and ICMP to use the standard polling method***. This is the default method for devices such as switches and routers, and Linux and UNIX servers. You will need to complete the following:
        i. Select the version of SNMP to use. The default is **SNMPv2c**. However, **SNMPv1** is supported for older devices, and **SNMPv3** for device supporting enhanced security.

ii. ***If you have installed multiple polling engines***, select the **Polling Engine** you want to use to collect statistics from the added node.

Note: This option is not displayed if you are only using one polling engine.

iii. ***If the SNMP port on the added node is not the Orion default of 161,*** enter the actual port number in the **SNMP Port** field.

iv. ***If the added node supports 64-bit counters and you want to use them,*** check **Allow 64-bit counters**.
Note: Orion supports 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.

v. **For SNMPv1 or SNMPv2c**, enter the **Community String** and, if required, the **Read/Write Community String**.

Note: Community Strings are passwords used to authenticate data sent between the management station and the device. See the documentation provided for your network device for further information. (The default for **Community String** is usually "public".) Click **Test** to validate the string or strings entered here.

vi. **For SNMPv3**, further credentials are required. See the documentation provided for your network device for further information.

vii. Click **Test** to validate.

d. ***Select Window Servers: WMI and ICMP, to use agentless polling for Windows servers***. You will need to complete the following:

i. Select the credential to be used. You can either select an existing credential from the dropdown list, or select **<New Credential>**.

ii. ***If you are creating a new credential,*** provide a **Credential name**, enter an appropriate **User name** and **Password**, and enter the password again in the **Confirm password** field.

iii. Click **Test** to validate.

e. ***Select Windows Servers: Agent, to use agent software to monitor Windows hosts*** in remote or distributed environments, such as the cloud. The agent software is downloaded and installed when you complete this page.

i. Select the credential to be used. You can either select an existing credential from the dropdown list, or select **<New Credential>**.

Note: Administrator credentials are needed only for installing the agent.

ii. ***If you are creating a new credential,*** provide a **Credential name**, enter an appropriate **User name** and **Password**, and enter the password again in the **Confirm password** field.

iii. Click **Test** to validate.

8. ***If the node hosts a UCS manager***, check ***UCS manager credentials***, and supply the following information:

a. Enter the **Port** on which the UCS manager listens.

b. Check **Use HTTPS**, if required.

c. Enter the **Username** and **Password** for the device.

d. Click **Test** to validate this data.

9. ***To monitor Active Directory users that log on to your network***, check **Active Directory Domain Controller**, and supply the following information.

a. Select the credential to be used. You can either select existing credential from the dropdown list, or select **<New Credential>**.

Note: Administrator credentials are needed only for installing the agent.

b. ***If you are creating a new credential,*** provide a **Credential name**, enter an appropriate **User name** and **Password**, and enter the password again in the **Confirm password** field.

c. Click **Test** to validate.

d. Enter the **Domain Controller Polling Interval** to be used. The default is 30 minutes.

10. ***If you are adding a VMware device,*** check **Poll for VMware** to ensure that SolarWinds NPM acquires any data the VMware device provides to SNMP polling requests, and then complete the following steps to provide required vCenter or ESX Server credentials. For more information, see Requirements for Virtual Machines and Servers.

    a. Select the credential to be used. You can either select existing credential from the dropdown list, or select **<New Credential>**. **Note**: Administrator credentials are needed only for installing the agent.

    b. ***If you are creating a new credential,*** provide a **Credential name**, enter an appropriate **User name** and **Password**, and enter the password again in the **Confirm password** field.

    c. Click **Test** to validate.

11. Click **Next**.

12. ***If the Choose Resources page is displayed***, check the resources and statistics you want to manage for this node. The following options are available in the selection toolbar:

    - Click **All** to select all listed resources and statistics for monitoring.
    - Click **None** to clear any selections.
    - Click **All Volumes** to select all listed volumes for monitoring.
    - Click **All Interfaces** to select all listed interfaces for monitoring.
    - Click **All Active Interfaces** to select all active interface for monitoring.
    - Click **No Interface Statistics** to remove any interface statistics.
    - After you have selected objects for monitoring, click **Next**.

13. ***If the Add Application Monitors tab is displayed***, select any applications you want to monitor on the selected node. You can filter the applications displayed using the **Show only** dropdown list.

    a. Select the credential to be used. You can either select existing credential from the dropdown list, or select **<New Credential>**.

    b. ***If you are creating a new credential,*** provide a **Credential name**, enter an appropriate **User name** and **Password**, and enter the password again in the **Confirm password** field.

    c. Click **Test** to validate, and then click **Next** to continue.

    d. Click **Next**.

14. ***If the Add Pollers page is displayed***, select the universal device pollers to add to your selected node, and click **Next**.

15. ***If the Add UDT Port page is displayed***, you can check the **Scan device for ports** box to display a list of UDT ports on the node. By default all are selected. Select those to be monitored, and then click **Next**.

16. The Change Properties page is displayed for all polling methods. Here you can:

    - Change the name of the Node. **Note:** the Polling IP Address and Polling Method cannot be changed.
    - Change the SNMP version and Community Strings or Credential settings, if the Polling Method is **Most Devices: SNMP and ICMP**.
    - Change the default **Node Status Polling**, **Collect Statistics Every** and **Poll for Topology Data Every** values, as appropriate.

17. ***If any Custom Properties have been set up***, you can edit these on the Change Properties page.

18. ***To override the CPU Load, Memory Usage, Response Time, Percent Packet Loss Alerting Thresholds***, check the corresponding boxes, and amend the default values. For more information, see Orion General Threshold Types.

19. ***If you have Network Configuration Manager installed***, there will be an option to manage the node using NCM. For more information, see the Network Configuration Administrator Guide.

20. Click **OK, Add Node** to add the node with these settings.

Importing a List of Nodes Using a Seed File

In versions of Orion platform products following the release of Orion NPM version 10.0, the Specific Nodes option in the Network Discovery Wizard may be used to import devices from a seed file. The following procedure details how the Specific Nodes option is used with a seed file to import devices into the SolarWinds Orion database.

Note: A Seed File discovery option is available in SolarWinds NPM prior to version 10.

To import devices from a seed file:

1. Open your seed file.
2. Logon to the Orion Web Console and navigate to **Settings > Network Sonar Discovery**.
3. Click **Add New Discovery** to create a new discovery. Select a discovery, and use one of the following choices if you already have a discovery.
    - Click **Discover Now** to use an existing discovery to rediscover your network, select the discovery you want to use, and then complete the Network Sonar Results Wizard after discovery completes. For more information about network discovery results, see Using the Network Sonar Results Wizard.
    - Click **Edit** to modify an existing discovery before using it.
    - Click **Import All Results** to import some or all devices found in a defined discovery that you may not have already imported for monitoring. For more information about network discovery results, see Using the Network Sonar Results Wizard.
    - Click **Import New Results** to import any newly enabled devices matching a defined discovery profile. For more information about network discovery results, see Using the Network Sonar Results Wizard.
4. ***If the devices on your network do not require community strings other than the default strings public and private provided by Orion,*** click **Next** on the SNMP Credentials view.

5. ***If you need to supply new SNMP credentials to discover the devices in your seed file,*** click **Add New Credential**, provide the required information, and then click **Add**. For more information, see Network Discovery Using the Network Sonar Wizard.
6. Click **Next** on the SNMP Credentials view.
7. To check nodes polled by agents for updates, select **Check all existing nodes polling with agents for node changes and updates**. For more information, see Using the Network Sonar Wizard to Check Agent Polled Nodes.
8. ***If you intend to import known VMware vCenter or ESX servers and you need to supply new VMware credentials to discover these servers in your seed file,*** complete the following steps on the Local vCenter or ESX Credentials for VMware view:

    a. Check **Poll for VMware**, and then click **Add vCenter or ESX Credential**.

    b. Provide the required information, and then click **Add**.

    Note: For more information, see Network Discovery Using the Network Sonar Wizard.

9. Click **Next** on the Local vCenter or ESX Credentials for VMware view.
10. To discover any WMI- or RPC-enabled Windows devices on your network, click **Add New Credential**, provide the required information, and then click **Add**.
11. Click **Next** on the Windows Credentials view.
12. Click **Specific Nodes** in the Selection Method menu.
13. Copy and then paste the IP addresses or hostnames of the devices you want to discover from your seed file into the provided field.

    Note: Confirm that there are no more than one IPv4 address or hostname per line.

14. Click **Validate** to confirm that the provided IP addresses and hostnames are assigned to SNMP-enabled devices.
15. ***If you have provided all the IP addresses and hostnames you want to discover,*** click **Next**.

16. Complete the Network Discovery and Network Discovery Results Wizards. For more information, see Network Discovery Using the Network Sonar Wizard.

Choosing Your Polling Method

SolarWinds provides five different polling methods to help you monitor your nodes in the way that best suits your environment.

External Node (No Status)

The node is not polled and no data is collected from this node. However, the node is included in your environment and is used to monitor an application or another element on the node. This also allows you to build a more complete map of your network environment within your SolarWinds NPM platform product.

Status Only: ICMP

Limited information is gathered using Internet Control Message Protocol (ICMP) or ping. This polling method only provides information such as status, response time, and packet loss. When a node is queried, it only returns a response time and a record of any dropped packets. This information is used to monitor status and measure average response time and packet loss percentage for managed devices.

Use this method when you only need limited information or if you want to monitor devices that do not support SNMP or WMI.

Note: This requires that you enable ICMP on your nodes. You may also want to consider adjusting any network intrusion detection systems or your firewalls to allow for the ICMP traffic.

Most Devices SNMP & ICMP

This method allows you to query Management Information Base (MIB) and performance indicators that are tied to specific Object Identifiers (OIDs) in addition to polling the device status, average response time, and packet loss percentage. This method is suitable for SNMP-enabled devices such as routers, switches, and computers. You must provide the appropriate SNMP community strings for SNMP v1 or v2c, or SNMP v3 credentials.

Your devices must have ICMP and SNMP enabled to use this polling method. If you want to poll with a specific version of SNMP, you must disable all other versions on the device.

Note: You may also want to consider adjusting any network intrusion detection systems or your firewalls to allow for the ICMP traffic.

Windows Servers: WMI and ICMP

This polling method can only be used for Windows computers. Windows Management Instrumentation (WMI) is a proprietary technology used to poll performance and management information from Windows-based network devices, applications, and components. When used as an alternative to SNMP, WMI can provide much of the same monitoring and management data currently available with SNMP-based polling with the addition of Windows specific communications and security features.

Your devices must have WMI and SNMP enabled to use this polling method. You can use WBEMTest.exe, which is included on every computer that has WMI installed, to test the connectivity between your SolarWinds Orion server and your Windows computer.

Note: Due to specific characteristics of WMI polling requests, polling a single WMI enabled object uses approximately five times the resources required to poll the same or similar object with SNMP on the same polling frequency.

Windows Servers: Agent

An agent is software that provides a communication channel between the SolarWinds Orion server and a Windows computer. Agents are used to communicate the information that SolarWinds plug-ins collect to the SolarWinds Orion server.

Information collected by plug-ins depend on the type of plug-in installed on the agent. For example, the Quality of Experience plug-in collects packet traffic, while a SAM plug-in collects application data that are used to monitor the applications. Agents automatically download the plug-ins for all installed products.

This polling method is most useful in the following situations:

- When host and applications are behind firewall NAT or proxies
- Polling node and applications across multiple discrete networks that have overlapping IP address space
- Allows for secure encrypted polling over a single port

- Support for low bandwidth, high latency connections
- Polling nodes across domains where no domain trusts have been established
- Full end to end encryption between the monitored host and the poller

Managing Scheduled Discovery Results

The Scheduled Discovery Results tab of Network Discovery provides a list of all recently discovered, changed, or imported devices on your monitored network. Results are compared between discoveries, and results are listed on this tab. The following procedure provides guidelines for managing discovery results.

To manage scheduled discovery results:

1. Logon to the Orion Web Console and navigate to **Settings > Network Sonar Discovery**.
2. Click **Scheduled Discovery Results**.
3. Select the type of devices you want to view from the Status menu in the left pane. The following options are available:
    - Select **Found and Changed** to view a combined list of all devices found or changed as described above.
    - Select **All except Ignored** to view all discovered, changed or imported devices you have not already designated as Ignored, as detailed above.
    - Select **Found** to view all devices discovered by a scheduled discovery.
    - Select **Changed** to view all devices that have changed between recent scheduled discoveries. Changes include the addition of interfaces and device configuration changes.
    - Select **Imported** to view all devices you have recently imported into your Orion database. For more information about importing devices, see Using the Network Sonar Results Wizard.
    - Select **Ignored** to view all devices you have added to your Discovery Ignore List. For more information about the Discovery Ignore List, see Using the Discovery Ignore List.
4. To apply a grouping criterion to organize your listed results, select an appropriate criterion from the **Group by:** menu in the left pane.
5. To update your SolarWinds Orion database to include changed or discovered nodes in the results list, check all nodes to update or to add, and then click **Import Nodes**.

6. To ignore devices in future discoveries, regardless of discovered updates or changes, select all nodes to ignore, and then click **Add to Ignore List**.

Using the Discovery Ignore List

Often, devices are found during a network discovery that you never intend to monitor. The Discovery Ignore List is a record of all such devices on your network. By placing a device on the Discovery Ignore List you can minimize the SNMP processing load associated with discovering devices that you do not intend to monitor.

To manage devices on the Discovery Ignore List:

1. Logon to the Orion Web Console and navigate to **Settings > Network Sonar Discovery**.
2. Click **Discovery Ignore List**.
3. To add devices to the Discovery Ignore List, complete the following procedure:
    a. Click **Scheduled Discovery Results**.
    b. Check devices you want to ignore, and then click **Add to Ignore List**.
4. To remove devices from the Discovery Ignore List, complete the following procedure:
    a. Click **Scheduled Discovery Results**, and then check the devices you want to remove from the list.
    b. Click **Remove from Ignore List**.
    c. Confirm that you want to stop ignoring selected items by clicking **OK**.

Downloading the SolarWinds MIB Database

SolarWinds maintains a MIB database that serves as a repository for the OIDs used to monitor a wide variety of network devices. This MIB database is updated regularly, and, due to its size, it is not included in the initial NPM installation package. If you are either updating your existing MIB database or using the Universal Device Poller for the first time, you will need to download the SolarWinds MIB database as detailed in the following procedure.
Note: You may need to restart the Universal Device Poller after installing the new MIB database.

To download and install the SolarWinds MIB database:

1. ***If you are responding to a prompt to download and install the SolarWinds MIB database,*** click **Yes**.

   Note: This prompt is typically only encountered by first-time users.

2. ***If you are downloading an update to your existing SolarWinds MIB database,*** complete the following procedure:

   a. Use your SolarWinds Customer ID and Password, to log in to the Customer Portal (http://www.solarwinds.com/customerportal/).

   b. On the left, under Helpful Links, click **Orion MIB Database**.

3. ***If you are using Internet Explorer and it prompts you to add the SolarWinds downloads site http://solarwinds.s3.amazonaws.com,*** complete the following steps to start the MIB database download:

   a. Click **Add** on the warning window.

   b. Click **Add** on the Trusted Sites window.

   c. Click **Close**, and then refresh your browser.

4. Click **Save** on the File Download window.
5. Navigate to an appropriate file location, and then click **Save**.
6. After the download completes, extract `MIBs.zip` to a temporary location.

7. Open the folder to which you extracted `MIBs.zip`, and then copy `MIBs.cfg` to the SolarWinds folder in either of the following locations on your default install volume, depending on your NPM server operating system:
    - `\Documents and Settings\All Users\Application Data\` on Windows Server 2003 and XP.
    - `\Users\All Users\Solarwinds\` on Windows Server 2008 and Vista.

Discovery Central

Discovery Central provides a centralized overview of the types and number of network objects you are monitoring with your currently installed SolarWinds products. The Discovery Central view is subdivided into sections corresponding to the SolarWinds products you have installed. The Network Discovery section displays for all node-based products. For more information about Network Discovery, see Network Discovery. For more information about specific sections, see the Administrator Guide for the corresponding SolarWinds product.

Clicking **Go to Orion Home** opens the Summary Home view for your entire monitored network.

Network Discovery

The Network Discovery resource provides the number of nodes and volumes that are currently monitored. This information is both available and applicable to all installed Orion products.

Click **Discover my Network** to start a Network Sonar Discovery. For more information, see Network Discovery Using the Network Sonar Wizard.

Click **Add a Single Node** to open the Add Node – Define Node view of the Orion Node Management utility. For more information, see Adding Devices for Monitoring in the Web Console.

Interface Discovery

The Interface Discovery resource provides the number of interfaces on which you can monitor network traffic. To discover interfaces on your network, simply discover or add the parent node and SolarWinds will automatically discover any and all interfaces on the designated parent node. This information is available and applicable to SolarWinds Network Performance Monitor (NPM) and all installed SolarWinds NPM modules.

Click **Discover My Network** to start a Network Sonar Discovery. For more information, see Network Discovery Using the Network Sonar Wizard.

Virtualization Discovery

The Virtualization Discovery section provides the number of virtual devices, including VMware vCenters, Datacenters, clusters, ESX Servers, and virtual machines that are currently monitored. This information is both available and applicable to all installed Orion products.

Click **Discover My Network** to start a Network Sonar Discovery. For more information, see "Network Discovery Using the Network Sonar Wizard" in the SolarWinds Orion Common Components Administrator Guide.

Click **Add a Single Node** to open the Add Node – Define Node view of the Orion Node Management utility. For more information, see "Managing Devices in the Web Console" in the SolarWinds Orion Common Components Administrator Guide.

Agent Deployment

Agents provide an additional method to poll devices that are part of a separate network or have intermittent connectivity to the network with your SolarWinds Orion server.

To deploy agents to devices that can be accessed from the SolarWinds Orion server, click **Deploy Agent on my Network**. For more information, see Deploying Agent Software via Orion Server Push.

To deploy agents manually to devices, click **Download Agent Installation Files**. This option is often used when deploying agents to devices that are not on the same network as the SolarWinds Orion server. For more information, see Deploying the Agent Manually.

Additional Discovery Central Resources

As they are released following the release of Orion NPM 10.1.2, each SolarWinds Orion module will provide its own Discovery Central resource. These additional Discovery Central resources provide the number of module-related network objects that are currently monitored. For more information about any of these additional Discovery Central resources, see the corresponding Orion module Administrator Guide.

Chapter 4: Managing the Orion Web Console

The Orion Web Console is an integral part of the Orion family of products that can be configured for viewing from virtually any computer connected to the Internet. You can also customize the web console for multiple users and store individually customized views as user profiles. Administrator functions are accessed by clicking **Settings** in the top right of all Orion Web Console views.

Logging in for the First Time as an Administrator

When you launch the Orion Web Console, you are presented with a login view requiring both a **User Name** and a **Password**.

To log in to the Orion Web Console:

1. Launch the Orion Web Console using either of the following methods:
   - Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
   - Or launch a browser and enter `http://ip_address` or `http://hostname`, where *ip_address* is the IP address of your SolarWinds Orion server, or where *hostname* is the domain name of your SolarWinds Orion server.
2. Enter **Admin** as your **User Name**, and then click **Login**.
   Notes: Until you set a password, you can log in as **Admin** with no Password. After your first login, you may want to change the Admin password.

Windows Authentication with Active Directory

As of Orion Platform version 2010.2, the Orion Web Console can authenticate Active Directory users and users who are members of Active Directory security groups.

SolarWinds offers a free analyzer tool for Active Directory that provides instantaneous visibility into effective permissions and access rights. The tool provides a complete hierarchical view of the effective permissions access rights for a specific file folder (NTSF) or share drive. Download it for free from here: http://www.solarwinds.com/products/freetools/permissions_analyzer_for_active_directory/.

To enable Active Directory Windows authentication to the web console:

1. Install and configure Active Directory on your local network.

   Notes:

   - For more information about installing Active Directory on Windows Server 2003, see the Microsoft Support article, "How To Create an Active Directory Server in Windows Server 2003".
   - For more information about Active Directory on Windows Server 2008, see the Microsoft TechNet article, "Active Directory Services".
   - For information about Active Directory on Windows Server 2012, see the Microsoft TechNet article, "What's New in Active Directory in Windows Services".

2. If you want to enable automatic login for web console accounts using Windows Authentication, configure the Orion Web Console as shown in the following steps:

   a. Click **Start > All Programs > SolarWinds Orion > Configuration and Auto-Discovery > Configuration Wizard**.

   b. Check **Website**, and then click **Next**.

c. After providing the appropriate **IP Address**, **Port**, and **Website Root Directory**, select **Yes – Enable automatic login using Windows Authentication**.

d. Click **Next**, and then complete the Configuration Wizard.

3. Log in to the web console using the appropriate domain and user, providing **Domain\User name** or **Username@Domain** as the web console **User name**.

Supported Active Directory Scenarios

The following Active Directory login scenarios are supported for SolarWinds products using the latest version of the Orion Platform.

Scenario	Web Console Login Supported?	Local Login Required?	Network Atlas and Unmanage Utility Login Supported?
Login with "Orion Server" domain AD account	Yes	No LogonFallback must be enabled.	Yes
Login with "Orion Server" domain Group AD account			
Login with trusted domain AD user			No
Login with trusted domain AD Group User			
Login with "Orion Server" domain Group AD account (group user belongs to trusted domain)[1]			

Scenario	Web Console Login Supported?	Local Login Required?	Network Atlas and Unmanage Utility Login Supported?
Login with trusted domain Group AD account (group user belongs to "Orion Server" domain)[2]	No	N/A	
Login with AD user or Group user from a foreign AD forest	No, without an Additional Website[3]		

Notes:

1. Use a group account from the domain where the Orion server is located. This group contains a user from the trusted domain. Log-in with this user.
2. Use a group account from the domain where the Orion server is located. This domain is trusted by the domain in which the Orion server is located. This group contains a user from the domain of the Orion server. Log-in with this user.
3. Active Directory authentication is performed by the web service. If you need to authenticate users from an AD forest other the one to which your primary SolarWinds server belongs, you must have an Additional Web Server in the AD forest wherein the users to be authenticated exist.

Enabling LogonFallback

LogonFallback must be enabled when the Active Directory user of the Orion Web Console does not have local logon rights to the web server machine. The following procedure enables LogonFallback on the server hosting your Orion Web Console.

To enable LogonFallback:

1. Locate the file `web.config` on the server hosting your Orion Web Console.
   Note: The default location is `c:\inetpub\SolarWinds\`.
2. Create a backup of `web.config`.
3. Locate row `<add key="LogonFallback" value="false" />`.
4. Set `value="true"`.
5. Save `web.config`.
6. Restart your SolarWinds website in Internet Information Services Manager.

Using the Web Console Notification Bar

Below the web console menu bar, the Orion notification bar provides informational messages related to the following NPM features:

- If you have configured the Orion Web Console to check for product updates, an announcement displays in the notification bar when an update, including any upgrade, service pack, or hotfix, to NPM or any other Orion modules you currently have installed becomes available.
- If you have configured the Orion Web Console to store blog posts, new and unread posts to the Orion Product Team Blog are announced in the notification bar.
- If you have currently configured a scheduled discovery, results display in the notification bar when the discovery completes. For more information about Scheduled Discovery, see Discovering and Adding Network Devices in the Orion Common Components web help.
- If you are currently using NPM to monitor any VMware ESX or ESXi Servers, the notification bar can display messages communicating the number of ESX nodes found during any discovery, and, if any discovered ESX nodes require credentials, the notification bar tells you. For more information about managing ESX Servers, see Monitoring Your Virtual Infrastructure.

For more information about any displayed notification bar message, click **More Details** and a web console view relevant to the displayed message opens.

To delete a posted message, either click **Dismiss Message** next to the displayed message, or properly address the situation mentioned in the posted notification.

To remove the notification bar from your web console, click Close (**X**) at the right end of the notification bar.

Navigating the Orion Web Console

The Orion Web Console offers two primary methods of navigation: top-level web console tabs and view-level breadcrumbs.

Using Web Console Tabs

Depending on the modules installed, the Solarwinds Orion Web Console displays the following tabs:

Home

The **Home** tab provides a menu bar of links to views aiding you in general network management and monitoring. Information, like events and Top 10 lists, and technologies, like alerts, used to generate the views linked from the Home menu are generally available to all Orion modules. By default, the **Orion Summary Home** view displays when you click **Home** from any view in the web console.

Network (NPM)

The **Network** tab opens a menu bar of links to views and technologies, like EnergyWise, wireless network, and interface monitoring, which are specific to the features provided by NPM. If NPM is installed, the **NPM Summary Home** view displays by default when you click **Home** from any web console view.

Applications (SAM)

If you are viewing the Orion Web Console on a server on which SolarWinds Server & Application Monitor (SAM) is also installed, the **Applications** tab opens a menu of default views for some of the many different types of applications SAM can monitor. If SAM is installed without NPM, the **SAM Summary Home** view displays by default when you click **Home** from any web console view.

Configs (NPM and NCM)

If the Orion NCM Integration for Orion NPM is installed, the **Configs** tab provides links to default device configuration management views. If NPM is installed, clicking **Home** from any web console view displays the **NPM Summary Home** view by default.

Virtualization

The Virtualization tab provides access to specific views and resources that are tailored for monitoring virtual devices. For more information about virtualization monitoring in Orion, see Monitoring Your Virtual Infrastructure.

The web console provides an additional module-specific tab for each installed Orion module. These tabs offer access to views and tools specific to the Orion module added. For more information about additional Orion modules, see www.solarwinds.com. For more information about customizing menu bars, see Customizing Web Console Menu Bars.

Using and Disabling Web Console Breadcrumbs

As you navigate web console views, your location is recorded as a series of links, or breadcrumbs, to the views you have opened.

Each breadcrumb offers the following navigation options:

- Clicking a breadcrumb opens the corresponding view directly.
- Clicking **>** next to a breadcrumb opens a clickable list of all other views at the same navigation level in the web console. For example, if you are on a Node Details view, clicking **>** displays a list of other monitored nodes.

Note: Only the first 50 monitored nodes, listed in alphanumeric order by IP address, are displayed.

Customizing Web Console Breadcrumbs

Dropdown breadcrumb lists are customizable, as shown in the following steps.

To customize the items in a breadcrumb dropdown:

1. Click **>** at an appropriate level in a breadcrumb to open the dropdown.
2. Click **Customize this list**.
3. Select a criterion from the menu, and then click **Submit**.
   Note: All items in the customized list will be identical for the selected criterion.

Disabling Web Console Breadcrumbs

To ensure access is appropriately restricted for account limited users, you may want to disable breadcrumbs, as indicated in the following procedure.

To disable web console breadcrumb navigation:

1. Log on to your Orion server using an account with administrative access.
2. Open **web.config** (default location **C:\Inetpub\SolarWinds**) for editing.
3. In the **<appsettings>** section, locate the following setting:

   <add key="DisableBreadCrumbs" value="false"/>

4. Change **"false"** to **"true"**, as follows:

   <add key="DisableBreadCrumbs" value="true"/>

5. Save **web.config**.
   Note: If you run the Configuration Wizard after editing this setting, your changes may be overwritten.

Administrative Functions of the Orion Web Console

The following sections describe the primary administrative functions performed by an Orion Web Console administrator.

Changing an Account Password

Orion Web Console administrators may change user account passwords at any time, as shown in the following procedure.

Note: In environments where security is a priority, SolarWinds recommends against providing a view where users may change their own web console account passwords.

To change an account password:

1. Log in to the web console as an administrator.
2. Click **Settings** in the top right corner of the web console.
3. Click **Manage Accounts** in the User Accounts grouping of the Main Settings and Administration page.
4. Select the user account with the password you want to change, and then click **Change Password**.
5. Complete the **New Password** and **Confirm Password** fields, and then click **Change Password**.

Web Console Administration

If you are logged in to the web console as an administrator, clicking **Settings** in the top right corner of the web console displays the Main Settings and Administration page, presenting a variety of tools to control the appearance and delivery of information to Orion Web Console users.

Note: As more Orion modules are added, additional options will be displayed.

Getting Started with Orion

Before you can start monitoring your network you must designate the network objects you want your SolarWinds NPM installation to monitor. The Getting Started with Orion grouping provides direct links to the following discovery-related views so you can quickly and easily start monitoring your network:

- **Discovery Central** provides a centralized overview of the types and number of network objects you are monitoring with your Orion installation. For more information, see Discovery Central in the Orion Common Components web help.
- Clicking **Network Sonar Discovery** opens the Network Sonar Discovery Wizard. Network Discovery enables you to quickly discover devices across your entire network for monitoring. For more information, see Network Discovery Using the Network Sonar Wizard.
- Clicking **Add a Node** opens the Add Node Wizard directly. For more information about adding nodes individually, see Adding Devices for Monitoring in the Web Console.

Node & Group Management

The Node & Group Management grouping of the Settings page gives you access to the following web console views for managing nodes and groups:

- Clicking **Manage Nodes** displays the Node Management page, where an Orion Web Console administrator can immediately add, view, and manage all network objects currently managed or monitored by your Orion installation. For more information, see Monitoring Devices in the Web Console.
- Clicking **Manage Virtual Devices** opens the Virtualization Polling Settings view where you can view both a list of currently monitored Hyper-V or VMware ESX Servers and a library of the VMware credentials used to monitor your ESX Servers. For more information, see Monitoring Your Virtual Infrastructure.
- Clicking **Manage Dependencies** opens the Manage Dependencies view. Dependencies allow you to formalize dependent relationships between monitored objects based on network topology or priority to eliminate the potential for duplicated or redundant polling and alerting.

- Clicking **Manage Agents** allows you to create and manage your alerts. For more information, see Managing Agents.
- Clicking **Manage Groups** opens the Manage Groups view. To a greater degree than previously available with custom properties, groups enable you to logically organize your monitored network objects. For more information, see Managing Groups.
- Clicking **Manage Custom Properties** allows you to create and manager custom properties that you can use within your Orion platform products. For more information, see Creating Custom Properties.
- Clicking **Manage World Map** allows you to manage the nodes you want to display in the Worldwide Map resource.
- Clicking **Manage Pollers** allows you to create new pollers or edit existing pollers to fit the needs of your unique devices. You can also import pollers created by your peers from thwack.
- Clicking **Manage Hardware Sensors** allows you to enable or disable monitoring hardware health sensors in the Orion Web Console. For more information, see Monitoring Hardware Health.

Alerts & Reports

The Alerts & Reports grouping allows an administrator to access the following pages:

- **Manage Alerts** - create and manage web-based alerts. For more information, see Creating and Managing Alerts.
- **Manage Reports** - create and manage web-based reports. For more information, see Creating Reports in the Web Console.
- **Manage SMTP Servers** - add and manage SMTP servers used to send email notifications.
- **Configure Default Send Email Action** - configure the default SMTP server and email information used with the Send Email alert action.

Product Specific Settings

The Settings grouping of the Settings page gives an Orion Web Console administrator access to the following settings configuration pages:

- **Virtualization Settings** allow an Orion Web Console administrator to setup Virtualization Manager integration, configure virtualization, and view your License Summary.
- **Web Console Settings** allow an Orion Web Console administrator to customize the function and appearance of both the Orion Web Console and the charts that are displayed as resources in Orion Web Console views. For more information about configuring Orion Web Console and Chart Settings, see Orion Web Console and Chart Settings.
- **Agent Settings** allow an Orion Web Console administrator to configure settings relevant for your agents. For more information, see Agent Settings.

Thresholds & Polling

The Thresholds & Polling grouping of the Settings page allows an administrator to modify poller settings and thresholds for specific statistics.

- **Polling Settings** define the configuration of polling intervals, timeouts, statistics calculations, and database retention settings for your Orion polling engine. For more information about configuring Orion Polling Settings, see Configuring Polling Engine Settings.
- **Virtualization Thresholds** allows you to set warning and critical thresholds specific for the Virtualization module.
- **Custom Poller Thresholds** allow you to set warning and critical threshold levels for your custom pollers.
- **NPM Thresholds** allow you to set warning and critical thresholds specific for the Network Performance Monitor.
- **Orion Thresholds** allow you to configure warning and critical thresholds for nodes and volumes. These thresholds are used in all Orion modules.

For more information about custom poller, NPM, or Orion thresholds, see Orion Thresholds.

Windows Credentials

Use the **Manage Windows Credentials** page to create and manage credentials you use to connect to Windows computers on your network.

User Accounts

The User Accounts grouping of the Settings page gives a web console administrator access to the following web console configuration pages:

- Click **Manage Accounts** to access the view where you can manage individual Orion accounts and groups.
- Click **Accounts List** to view a table of existing accounts and appropriate details, such as assigned rights or last login.

Views

The Views grouping of the Main Settings and Administration page gives an Orion Web Console administrator access to the following view configuration pages:

- The **Manage Views** page enables a web console administrator to add, edit, copy, or remove individual web console views. For more information about managing Orion Web Console views, see Customizing Views.
- The **Add New View** page enable you to define new web console views.
- The **Created NOC Views** link opens the NOC Views page, which displays the list of current Network Operations Center page and enables you to add new NOC views.

  For more information, see Using and Configuring NOC Views.
- The **Views by Device Type** page gives an Orion Web Console administrator the ability to designate default views for network devices. For more information, see Views by Device Type.

Details

The Details grouping of the Settings page provides links to the following pages containing information about your SolarWinds NPM installation:

Database Details

This is an information-only page that displays details about the SQL Server database currently used by your SolarWinds NPM installation. In addition to current version information and configuration settings for both your SolarWinds Orion server and your database server, this page displays the total number of monitored objects in the SolarWinds Orion database.

Polling Engines

SolarWinds NPM supports the implementation of multiple distributed polling engines. Each engine can monitor and collect data from different parts of your network. This page shows the status and selected configuration information for each currently operational polling engine.

Orion Platform Details

This is an information-only page that displays details about your installation of the common components and resources that all Orion platform products share, including information about your SolarWinds Orion server, monitored object counts, and the version numbers of the executables and DLLs required by any and all installed Orion platform products.

License Details

This is an information-only page that displays details about all Orion products that you currently have installed. This page also shows the version numbers of the Orion products you are running and the versions of associated DLLs. For more, see Maintaining Licenses with License Manager in the Orion Common Components web help.

Customize Navigation & Look

The Customize grouping of Settings page offers options to customize the navigation and appearance of your Orion Web Console on the following pages:

- The **Customize Menu Bars** page allows an Orion Web Console administrator to configure the menu bars seen by individual users. For more information, see Customizing Web Console Menu Bars.

- The **Color Scheme** page gives a web console administrator the ability to select a default color scheme for resource title bars. The color scheme selection takes effect immediately throughout the web console. For more information, see Changing the Web Console Color Scheme.
- The **External Websites** page enables an Orion Web Console administrator to designate any external website as an Orion Web Console view, appearing in the Views toolbar. For more information, see Creating and Editing External Website Views.

Viewing Secure Data on the Web

In the interest of security, sensitive network information, such as community strings, logins, and passwords, is not viewable in the web console. However, if you have secured your network, you may check **Allow Secure Data On Web (advanced)** in the Calculations & Thresholds area of the Orion Polling Settings page to allow the passage of community strings through the web console.

Note: This setting does not affect the display of custom reports that you export to the web. For more information, see Creating Reports in the Web Console

Handling Counter Rollovers

The Counter Rollover setting configures NPM to properly handle counter rollovers. NPM is capable of handling either 32-bit or 64-bit counters, but, by default, NPM assumes counters are 32-bit. 32-bit counters have a maximum value of 2^{32}, or 4,294,967,296, and 64-bit counters, if they are supported by your network devices, have a maximum value of 2^{64}, or 18,446,744,073,709,551,616.

Note: The 32-bit counters option is designated as Method 1 in the Counter Rollover field on the Orion Polling Settings page.

To designate the type of counter-handling used by NPM:

1. Log in to the web console as an administrator.
2. Click **Settings** in the top right of the web console.
3. Click **Polling Settings** in the Thresholds & Polling grouping of the Orion Website Administration page.
4. ***If you are using 64bit counters,*** select **Method 2** in the Counter Rollover field in the Calculations & Thresholds area.

Notes:

- If Method 2 is selected, NPM will intentionally skip a poll if a polled value is less than the previous polled value to permit counting to 2^{64}.
- Orion fully supports the use of 64-bit counters; however, these 64-bit counters can exhibit erratic behavior in some implementations. If you notice peculiar results when using these counters, disable the use of 64-bit counters for the problem device and contact the device manufacturer.

5. ***If you are using of 32bit counters,*** select **Method 1** in the Counter Rollover field in the Calculations & Thresholds area.
   Note: If Method 1 is selected, when a rollover is detected, the time between polls is calculated as (2^{32} – Last Polled Value) + Current Polled Value.

Orion Thresholds

Many of the resources available in the Orion Web Console are capable of displaying error and warning conditions for the devices on your network. Orion uses the values provided on the threshold settings pages to determine when and how to display errors and warnings in the Orion Web Console.

The following sections provide more information about threshold types and configuration:

- Orion General Threshold Types
- Setting Orion General Thresholds

The following sections provide information about threshold types and configuration specific for SolarWinds NPM:

- Network Performance Monitor Threshold Types
- Setting Network Performance Monitor Thresholds

Orion General Threshold Types

The following device conditions may be configured as Orion General Thresholds:

Avg CPU Load

Monitored network devices experiencing CPU loads higher than the value set for the **Critical Level** display in High CPU Load reports and resources. Gauges for these devices also display as bold red.

Monitored network devices experiencing a CPU load higher than the value set for the **Warning Level**, but lower than the value set for the **Critical Level**, display as red in High CPU Load reports and resources. Gauges for these devices also display as red.

Disk Usage

Monitored network devices experiencing a disk usage higher than the value set for the **Critical Level** display as bold red in High Disk Usage reports and resources.

Monitored network devices experiencing a disk usage higher than the value set for the **Warning Level**, but lower than the value set for the **Critical Level**, display as red in High Disk Usage reports and resources.

Percent Memory Used

Monitored network devices experiencing a percent memory usage higher than the value set for the **Critical Level** display in High Percent Utilization reports and resources. Gauges for these devices also display as bold red.

Monitored network devices experiencing a percent memory usage higher than the value set for the **Warning Level**, but lower than the value set for the **Critical Level**, display in High Percent Utilization reports and resources. Gauges for these devices also display as red.

For each of the above, you can specify whether you want to calculate exhaustion using average daily values or peak daily values.

Percent Packet Loss

Monitored network devices experiencing a percent packet loss higher than the value set for the **Critical Level** display in High Percent Loss reports and resources. Gauges for these devices also display as bold red.

Monitored network devices experiencing a percent packet loss higher than the value set for the **Warning Level**, but lower than the value set for the **Critical Level**, display in High Percent Loss reports and resources. Gauges for these devices also display as red.

Orion calculates percent packet loss using ICMP ping requests made on the Default Poll Interval. Orion pings monitored devices and records the results of the ten most recent ping attempts. Percent packet loss is expressed as the number of failed ping requests, X, divided by the number of ping requests, 10. For more information about the Default Poll Interval, see Configuring Polling Engine Settings.

For example, if, at a given point in time, the last ten ping requests made of a selected device resulted in 2 failures and 8 successes, the percent packet loss for the selected device at the given time is reported as 2/10, or 20%.

Response Time

Monitored devices experiencing response times longer than the value set for the **Critical Level** display in High Response Time reports and resources. Gauges for these devices also display as bold red.

Devices experiencing response times longer than the value set for the **Warning Level**, but shorter than the value set for the **Critical Level**, also display in High Response Time reports and resources. Gauges for these devices also display as red.

Orion calculates response time using ICMP ping requests made on the Default Node Poll Interval. Orion pings monitored devices and records the results of the ten most recent ping attempts. Average Response Time is expressed as the average response time of these last 10 ping requests. If Orion does not receive a ping response within the Default Poll Interval, Orion will attempt to ping the non-responsive device once every 10 seconds for the period designated as the Warning Interval. For more information, see Configuring Polling Engine Settings.

Setting Orion General Thresholds

Orion general thresholds are used for nodes and volumes in all Orion modules.

To set Orion General Thresholds:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console.
3. Click **Orion Thresholds** in the Thresholds & Polling group of the Main Settings & Administration page.

   Note: For more information about Orion General Thresholds, see Orion General Threshold Types.

4. Provide appropriate values for **Critical Level** or **Warning Level** for selected thresholds.

   Note: For **Avg CPU Load**, **Disk Usage** and **Percent Memory Used**, you can specify whether you want to calculate exhaustion using average or peak daily values.

5. Click **Submit**.

Network Performance Monitor Threshold Types

Thresholds allow you to specify when you want to be notified that a certain metric on a device has reached a certain level.

- When a metric reaches the specified **Critical Level** threshold on a node or interface, the node or interface will be displayed as bold red in resources and reports.

- When a metric reaches the specified **Warning Level** thresholds on a node, the node or interface will be highlighted in red in appropriate resources and reports.

  Note: Flapping Routes use different colors when the thresholds are exceeded: red for the error threshold and yellow for the warning threshold.

The following device condition thresholds are available for configuration as Network Performance Monitor thresholds:

Cisco Buffer Misses

Many Cisco devices can report buffer misses. Monitored network devices with more buffer misses than the value set for the **Critical Level** display as bold red in Cisco Buffer resources. Monitored network devices with more buffer misses than the value set for the **Warning Level**, but fewer than the value set for the **Critical Level**, display as red in Cisco Buffer resources.

Interface Errors and Discards

Monitored interfaces experiencing more errors and discards than the value set for the **Critical Level** display as bold red in High Errors and Discards reports and resources. Monitored interfaces experiencing more errors and discards than the value set for the **Warning Level**, but fewer than the value set for the **Critical Level**, display as red in High Errors and Discards reports and resources.

Interface Percent Utilization

Monitored interfaces experiencing current percent utilization higher than the value set for the **Critical Level** display in High Percent Utilization reports and resources. Gauges for these devices also display as bold red. Monitored interfaces experiencing current percent utilization higher than the value set for the **Warning Level**, but lower than the value set for the **Critical Level**, display in High Percent Utilization reports and resources. Gauges for these devices also display as red.

Specify whether you want to calculate exhaustion using average daily values or peak daily values by selecting the appropriate option in **Capacity Planning**.

Flapping Routes

Specify thresholds for highlighting flapping routes in the Top Flapping Routes resource.

- If a route flaps more frequently than specified in **Routing flaps error threshold**, the current flaps number will be highlighted in red.
- If a route flaps more frequently than specified in **Routing flaps warning threshold**, the current flaps number will be highlighted in yellow.

Setting Network Performance Monitor Thresholds

Network Performance Monitor Thresholds are node and interfaces thresholds used only by the Network Performance Monitor.

For more information about NPM threshold types, see Network Performance Monitor Threshold Types.

To set NPM thresholds:

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 **NPM Thresholds** in the Thresholds & Polling grouping.

   Note: For more information about Network Performance Monitor thresholds, see Network Performance Monitor Threshold Types.
3. Provide appropriate values for **Critical Level** and **Warning Level** for selected thresholds.
4. For the **Interface Percent Utilization** metric, specify whether you want to use average or peak daily values in calculations for capacity forecasting.
5. Click **Submit**.

Customizing Views

Orion Web Console views are configurable presentations of network information that can include maps, charts, summary lists, reports, events, and links to other resources. Customized Views can then be assigned to menu bars. With NOC View Mode enabled, views may be optimized for display in Network Operations Centers.

Creating New Views

You can customize the Orion Web Console for individual users by logging in as an administrator and creating new views as shown in the following procedure. **Note:** In environments where security is a priority, SolarWinds recommends against providing a view where users may change their own web console account passwords.

To create a new view:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Views** in the Views group
3. Click **Add**.
4. Enter the **Name of New View**, and then select the **Type of View**.

   Note: The **Type of View** selection affects how the view is made accessible to users, and your choice may not be changed later. For more information, Views by Device Type.
5. Click **Submit.**

After you have created a new view, the Customize page opens. For more information, see Editing Views.

Creating a Custom Summary View

The Orion Custom Summary View enables you to create a fully customized object-based view composed solely of resources you have selected. The following procedure creates a custom summary view in the web console.

To create or edit a custom summary view in the web console:

1. Click **Home > Custom Summary**.
2. Click **Edit** in any Custom Object Resource.

3. Provide a **Title** and **Subtitle** for the selected Custom Object Resource.
4. Choose an object type from the **Choose Object Type** dropdown.
5. Click **Select Object**.
6. On the Select Objects window, use the **Group by** selection field, as appropriate, to filter the list of monitored objects.
7. Select one or more object types on which to base the selected Custom Object resource, and then click the green right arrow to move all objects of the selected type into the Selected Objects window.
8. Select one or more objects on which to base the selected Custom Object resource, and then click **Submit**.
9. The fields displayed and information required depend upon the object type selected. Complete these fields as appropriate and click **Submit**.

Note: For more information about customizing available resource types, click **Help** in the header of any resource on the Custom Summary view, and then click the corresponding resource type.

Creating and Editing External Website Views

With the external website view feature, any administrator can select any external website and designate it as an Orion Web Console view, as shown in the following procedure.

To create or edit an external website view in the web console:

1. Click **Settings** in the top right of the web console.
2. Click **External Websites** in the Customize Navigation & Look grouping of the Orion Website Administration page.
3. ***If you want to delete an existing external website,*** click **Delete** next to the website you want to delete, and then click **OK** to confirm the deletion.
4. ***If you want to add a new external website,*** click **Add**.
5. ***If you want to edit an existing external website,*** click **Edit** next to the name of the website you want to edit.
6. Provide a **Menu Title** for the external website to display in the Views toolbar.

7. ***If you want to include a heading within the view,*** provide an optional **Page Title** to display within the view.
8. Provide the **URL** of the external website, in `http://domain_name` format.
9. Select the **Menu Bar** to which you want to add the new external website link.
   Note: For more information about customizing menu bars, see Customizing Web Console Menu Bars.
10. Click **OK**.
11. Click **Preview** to view the external website as the web console will display it.

Editing Views

The Orion Web Console allows administrators to configure views for individual users.

To make views and graphs larger for larger screens, resize the columns dynamically (drag the division bars) and use your browser zoom controls, such as <Ctrl>+<+> in Chrome.

The following steps are required to configure an existing view.

To edit an existing view:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Views** in the Views group.
3. Select the view you want to customize from the list, and then click **Edit**.
4. ***To add a subview that can be accessed from tabs on the left***:
   a. Check the **Enable left navigation** box.
   b. Click the **Add tab** on the left.
   c. Enter a name for the tab in the **Tab Name** field.
   d. Click **Browse** next to the tab Icon, and select an appropriate icon for this tab.

e. Click **Update**.

f. You can now add further tabs, or proceed as below.

5. ***To change the width of a column,*** enter the width in pixels in the **Width** field beneath the column.
6. ***To add a column***, click **Add New Column**.
7. ***To add a resource,*** repeat the following steps for each resource:

   a. Click **+** next to the column in which you want to add a resource.

   b. Check all resources you want to add, and click **Add Selected Resources**.

   Notes:

   - Use the **Group by:** field on the left to limit the resource list or use the **Search** field at the top to locate specific resources.
   - Resources already in your view will not be checked on this page listing all web console resources. It is, therefore, possible to pick duplicates of resources you are already viewing.
   - Some resources may require additional configuration. For more information, see Resource Configuration Examples.
   - Several options on the Add Resources page are added to the list of resources for a page, but the actual configuration of a given map, link, or code is not added until the page is previewed.

8. ***To delete a resource from a column,*** select the resource, and then click **X** next to the resource column to delete the selected resource.
9. ***To copy a resource in a column,*** select the resource, and then click  next to the resource column to delete the selected resource.
10. ***To move a resource to another column***, use the back and forward arrow icons next to the resource column to transfer the resource to the previous or next column.
11. ***If you are using subviews and want to move a resource to another tab***, click on ***Move to a different tab*** to open a window enabling you to move to a selected tab and column.

12. ***To rearrange the order in which resources appear in a column,*** select resources, and then use the up and down arrow icons to rearrange them.
13. ***If you have finished configuring your view,*** click **Preview**.

    Note: A preview of your custom web console displays in a new window. A message may display in the place of some resources if information for the resource has not been polled yet. For more information, see Resource Configuration Examples.
14. Close the preview window.
15. ***If you are satisfied with the configuration of your view,*** click **Done**.

Note: For more information about adding a customized view to menu bars as a custom item, see Customizing Web Console Menu Bars. For more information about assigning your customized view as the default view for a user, see Editing User Accounts.

Using and Configuring NOC Views

A Network Operations Center (NOC) view provides a single page view of critical statistics that can fit on a TV screen or a mobile device. If you define multiple subviews, they rotate automatically on the screen, each subview available as a separate slide.

Headers and footers are compressed in NOC views, increasing the available space to display NPM resources.

Enabling NOC Views

You can configure any Orion Web Console view to appear in the NOC view form.

To enable the NOC view for a view:

1. Log in to the Orion Web Console using an account with view customization privileges.
2. Open the appropriate view, and click **Customize View** in the top right corner of the view.
3. Select the **Enable NOC view** option.
4. ***If the view contains several subviews***, define the rotation interval for the subview. Select the appropriate time interval in the **Rotate tabs** drop-down lists.

Note: You can also get a direct link your NOC view and display the view in a web browser.
To get the link, go to the Enable NOC view area, right-click the NOC view name in Link to NOC View, and select **Copy Shortcut**.

5. Apply your changes:
   - Click **Done** to return to the normal view.
   - Click **Done & Go to NOC View** to return to the NOC view.

   You have created a NOC version of your view with a compressed header and footer, and without the left navigation area.

Customizing NOC Views

To add resources, remove resources, or add subviews on a NOC view, click the NOC Settings icon and select **Customize Page**.

For more information, see Customizing Views.

Exiting NOC Views

To exit a NOC view, click the NOC Settings icon and select **Exit NOC mode**.

You will return to the default view with the full header, footer and left navigation.

Managing NOC Views

You can display a list of all NOC views defined in your Orion to get a better understanding of your NOC views. From the NOC views list, you can easily add, edit or manage your NOC views.

To manage your NOC views:

1. Click **Customize Page** in the right corner of any view.
2. Click **List of created NOC views** in the NOC view section.

   Note: You can also access the list via **Settings > Views > Created NOC Views**.

3. Manage the NOC views:
   - To add a new view, click **Add New View**.
   - To edit an existing NOC view, select the appropriate view and click **Edit**. For more information, see Customizing Views.

- To disable the NOC feature for a view and maintain the default view, select the appropriate view and click **Disable NOC**.

Displaying Subviews

If more subviews have been defined for the view, you can see white circles in the top right corner. The currently active tab is displayed in orange.

To display another subview, click the appropriate circle.

Dragging and Dropping Resources in NOC Views

If you want to reposition resources within a NOC view, you need to turn on the drag&drop mode.

To drag and drop resources in a NOC view:

1. Click the **Settings** icon in the top right corner of the NOC view, and select **Enable Drag&Drop / Pause**.
2. Drag and drop resources within the selected pane.
3. When you have finished repositioning the resources, click the **Settings** icon again and select **Disable Drag&Drop / Resume** to turn the mode off.

Changing the NOC View Logo

You can hide the default SolarWinds logo on the NOC view, or use a customized image in the top left corner of your NOC views.

Logo requirements:

- Supported image formats: .png, .jpg
- Maximum resolution: 900x200 px

To use a customized logo on your NOC views:

1. If you already are in a NOC view, click the NOC Settings icon and select **Customize NOC View Logo**.

   Note: You can also access the Web Console Settings from normal views, via **Settings > Web Console Settings**.

2. To hide the logo, clear the **NOC View Logo** option.
3. To change the logo:
   a. Make sure that **NOC View Logo** is selected.
   b. Click the **Browse** button for NOC View Logo and navigate to the appropriate logo image.

      Note: By default, the SolarWinds logo is used on NOC views. It is available as **SW_NOClogo.png** in **/NetPerfMon/images** on your Orion server.

4. Click **Submit** to apply your changes in the view.

Configuring View Limitations

As a security feature, the web console gives administrators the ability to apply device-based view limitations.

The following limitations are defined by default:

Orion Web Console View Limitations		
Single Network Node	Group of Nodes	System Location Pattern
Node Name Pattern	System Name Pattern	Single Interface (SolarWinds NPM)
Machine Type Pattern	Group of Machine Types	Interface Status (SolarWinds NPM)
Hardware Manufacturer	Single Hardware Manufacturer	Interface Alias Pattern (SolarWinds NPM)
System Location	System Contact Pattern	Group of Interfaces (SolarWinds NPM)
System Contact	IP Address Pattern	Interface Name Pattern (SolarWinds NPM)
Group of Volumes	Device Status	Interface Type (SolarWinds NPM)
Single Machine Type	Single Group	Group of Groups
Group Name Pattern		

The following procedure configures a view limitation.

To enable a view limitation:

1. Click **Settings** in the top right of the web console, and then click **Manage Views** in the Views group of the Orion Website Administration page.
2. Select the view to which you want to add a limitation, and then click **Edit**.

3. In the View Limitation area of the Customize View page, click **Edit**.
4. Select the type of view limitation you want to apply, and then click **Continue**.
5. Provide or check appropriate strings or options to define the device types to include or exclude from the selected view, and then click **Submit**.

   Note: The asterisk (*) is a valid wildcard. Pattern limitations restrict views to devices for which the corresponding fields include the provided string.

Copying Views

When you want to create multiple views based on the same device type, copying views allows you to create one view, and then use that view as a template to create other new views. The following steps copy an existing view.

To copy a view:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Views** in the Views group.
3. Select the view you want to copy, and then click **Copy**.
4. ***To edit a copied view,*** follow the procedure in Editing Views.

Deleting Views

Deleting views is a straightforward process, as shown in the following procedure.

To delete a view:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Views** in the Views group.
3. Select the view you want to delete, and then click **Delete**.

Views by Device Type

There are vast differences among network objects and the statistics they report, but the Orion Web Console can make it easier to view network data by displaying object details by device type, giving you the ability to have a different view for each unique type of device you have on your network, including routers, firewalls, and servers. The following steps assign a view by any available device type.

To assign a view by device type:

1. Click **Settings** in the top right of the web console, and then click **Views by Device Type** in the Views group of the Orion Website Administration page.
2. Select available Web Views for the different types of devices that Orion is currently monitoring or managing on your network.
3. Click **Submit**.

Resource Configuration Examples

Several resources that may be selected from the Add Resources page require additional configuration. Included in this section are examples of these resources and the steps that are required for their proper configuration.

Selecting a Network Map

Network maps created with Orion Network Atlas can give a quick overview of your network, right from the main web console view. For more information, see the SolarWinds Orion Network Atlas Administrator Guide.

Note: Clicking the resource title in the title bar menu displays the resource by itself in a browser window.

The following procedure adds a network map to the Orion Web Console.

To add a network map to the web console:

1. Navigate to the view to which you want to add the map, and then click **Customize Page**.
2. Click the plus sign in the appropriate column to open the Add Resource dialog.
3. Enter "`map`" in the **Search** box, and then click **Search**.
4. Select the box before **Map**, and then select **Add Selected Resources**.
5. Use the arrow icons by the right-hand side of the column to position the map, and then click **Preview** to display the map in a separate browser tab.
6. Click **Edit** in the Map resource title bar.
7. ***If you do not want to use the default title provided,*** enter a new **Title** for the title bar of the added map.
8. enter a new **Subtitle** for the added map.
   If you want a subtitle,
9. Select from the list of available maps.
10. Select the **Zoom** percentage at which you want to display the map.
    Note: If you leave the **Zoom** field blank, the map displays at full scale, based on the size of the column in which the map displays.
11. Click **Submit**.

Displaying a List of Objects on a Network Map

When your web console view includes a network map, it can be helpful to maintain a list of network objects that appear on the map. The following procedure enables a resource listing network map objects.
Note: Click the resource title to display the resource in a new browser window.

To display a list of network map objects:

1. Navigate to the view to which you want to add the map, and then click **Customize Page**.
2. Click the plus sign in the appropriate column to open the Add Resource dialog.
3. Enter "`map`" in the **Search** box, and then click **Search**.

4. Check the box before **List of Objects on Network Map**, and then select **Add Selected Resources**.
5. Use the arrow icons by the left side of the column to position the resource and click **Preview** to display the map in a separate browser tab.
6. Click **Edit** in the title bar of the List of Objects on Network Map resource.
7. ***If you do not want to use the default title provided,*** enter a new **Title** for the header of the objects list.
8. ***If you want a subtitle,*** enter a new **Subtitle** for the added objects list.
9. Select the required network map from the list of available maps, and click **Submit**.

Displaying a Custom List of Maps

The web console allows you to populate a custom view with a list of available network maps. Each map in your custom list, when clicked, opens in a new window. The following procedure enables a custom network maps list resource.

Note: Click the resource title to display the resource in its own browser window.

To display a custom list of maps:

1. Navigate to the view to which you want to add the list of maps, and then click **Customize Page**.
2. Click the plus sign in the appropriate column to open the Add Resource dialog.
3. Enter "`map`" in the **Search** box, and then click **Search**.
4. Select the box before **Custom List of All Maps**, and then select **Add Selected Resources**.
5. Use the arrow icons by the left side of the column to position the resource, and then click **Preview** to display the map in a separate browser tab.
6. Click **Edit** in the title bar of the Custom List of Maps resource.
7. ***If you do not want to use the default title provided,*** enter a new **Title** for the header of the maps list.
8. ***If you want a subtitle,*** enter a new **Subtitle** for the custom list of maps.

9. Make sure the maps you want to include in your maps list are checked.
10. Click **Submit**.

Displaying the Worldwide Map

The worldwide map provides a quick geographical overview of your network at any level from global down to street. For more information, see Managing the Worldwide Map of Orion Nodes Resource.

Note: Click the resource title in the title bar menu to display the resource in its own browser window.

The following procedure adds the worldwide map to the Orion Web Console.

To display the worldwide map:

1. Navigate to the view to which you want to add the map, and then click **Customize Page**.
2. Click the plus sign in the appropriate column to open the Add Resource dialog.
3. Enter "`map`" in the **Search** box, and then click **Search**.
4. Select the box before **Worldwide Map**, and then select **Add Selected Resources**.
5. Use the arrow icons by the column to position the map, and then click **Preview** to display the map in a separate browser tab.
6. If the map looks correct, click **Done**.
7. To customize the way the world map is displayed, click **Edit** in the Worldwide Map resource title bar.
8. ***If you do not want to use the default title provided,*** enter a new **Title** for the title bar of the added map.
9. ***If you want a subtitle,*** enter a new **Subtitle** for the added map.
   Note: Titles and subtitles can be entered as either text or HTML.
10. Enter the required **Height**. (The default is 400px.)
11. Click **Set location and zoom level** if you want to change the default location (the center of the map) and zoom magnitude of the map. You can also set this manually by clicking **Advanced**, and entering the latitude and longitude of the default location and the zoom level.

12. To filter the groups and nodes displayed, click **Group** and/or **Nodes**, and then enter the SWQL for the filters to be used. Click **Examples** to see a few simple samples.
13. Click **Submit**.

Displaying an Event Summary - Custom Period of Time

You may want your web console view to display an event summary for a specified period of time. The following procedure details the steps to include an event summary in your web console.
Note: Click the resource title in the title bar menu to display the resource by itself in a browser window.

To display an event summary:

1. Navigate to the view to which you want to add the events summary, and then click **Customize Page**.
2. Click the plus sign in the appropriate column to open the Add Resource dialog.
3. Enter "`event`" in the **Search** box, and then click **Search**.
4. Select the box before **Event Summary**, and then select **Add Selected Resources**.
5. Use the arrow icons by the column to position the resource, and then click **Preview** to display the resource in a separate browser tab.
6. Click **Edit** in the title bar of the Event Summary resource.
7. ***If you do not want to use the default title provided,*** enter a new **Title** for the header of the event summary.
8. ***If you want a subtitle,*** enter a new **Subtitle** for the links list.
9. Select the time period for displaying events the **Time Period** drop-down list.
10. Click **Submit**.

Specifying User-Defined Links

The User-Defined Links option can be used to create quick access to external websites or customized views. URLs of your customized views can be copied from their preview pages and pasted in a User-Defined Links field. The following steps enable user-defined links from within your web console.
Note: Click the resource title in the title bar menu to display the resource by itself in a browser window.

To enable a user-defined links resource:

1. Navigate to the view to which you want to add the links resource, and then click **Customize Page**.
2. Click the plus sign in the appropriate column to open the Add Resource dialog.
3. Enter "`links`" in the **Search** box, and then click **Search**.
4. Select the box before **User Links**, and then select **Add Selected Resources**.
5. Use the arrow icons by the column to position the resource, and then click **Preview** to display the resource in a separate browser tab.
6. Click **Edit** in the title bar of the User Links resource.
7. ***If you do not want to use the default title provided,*** enter a new **Title** for the links list.
8. ***If you want a subtitle,*** enter a new **Subtitle** for the links list.
9. Enter the following information for each link you want to define:
    a. A link **Name** and the **URL** of your link.
    b. ***If you want your links to open in a new browser window,*** check **Open in New Window.**
10. Click **Submit**.

Specifying Custom HTML

In situations where you have static information that you want to provide in the web console, use the **Custom HTML** option. This can also be used to create quick access to your customized views. The following procedure creates a static content area within your web console for displaying HTML content.
Note: Click the resource title to display the resource in a new browser window.

To specify custom HTML:

1. Navigate to the view to which you want to add the resource, and then click **Customize Page**.
2. Click the plus sign in the appropriate column to open the Add Resource dialog.
3. Enter "`html`" in the **Search** box, and then click **Search**.
4. Select the box before **Custom HTML**, and then select **Add Selected Resources**.
5. Use the arrow icons by the column to position the resource, and then click **Preview** to display the resource in a separate browser tab.
6. Click **Edit** in the title bar of the Custom HTML resource.
7. ***If you do not want to use the default title provided,*** enter a new **Title** for the specified content area.
8. ***If you want a subtitle,*** enter a new **Subtitle** for the specified content area.
9. Enter HTML formatted content as required.
10. Click **Submit**.

Specifying an Orion Report

The web console is able to incorporate reports that you have created in Orion Report Writer into any view. The following procedure takes a report that you have created with Report Writer and includes it within a web console view.
Note: Click the resource title in the title bar menu to display the resource by itself in a browser window.

To include an Orion report:

1. Navigate to the view to which you want to add the report resource, and then click **Customize Page**.

2. Click the plus sign in the appropriate column to open the Add Resource dialog.
3. Enter "`report`" in the Search box, and then click **Search**.
4. Select the box before **Report from Orion Report Writer**, and then select **Add Selected Resources**.
5. Use the arrow icons by the column to position the resource, and then click **Preview** to display the resource in a separate browser tab.
6. Click **Edit** in the title bar of the Report from Orion Report Writer resource.
7. ***If you do not want to use the default title provided,*** enter a new **Title** for the included report.
8. ***If you want a subtitle,*** enter a new **Subtitle** for the included report.
9. **Select a Report** to include from the drop-down.
10. ***To filter the nodes used to create the included report,*** enter an appropriate query in the **Filter Nodes** field.
    Note: Filter Nodes is an optional, advanced, web console feature that requires some knowledge of SQL queries. Click **+** next to **Show Filter Examples** to view a few example filters.
11. Click **Submit**.

Displaying a Custom List of Reports

The web console allows you to populate a custom view with a custom reports list. When clicked from the list, each report opens in a new window. The following procedure details the steps required to enable a custom list of network reports.
Note: Click the resource title to display the resource in a new browser window.

To display a custom list of reports:

1. Navigate to the view to which you want to add the custom list of reports, and then click **Customize Page**.
2. Click the plus sign in the appropriate column to open the Add Resource dialog.
3. Enter "`report`" in the **Search** box, and then click **Search**.
4. Select the box before **Report from Orion Report Writer**, and then select **Add Selected Resources**.

5. Use the arrow icons by the column to position the resource, and then click **Preview** to display the resource in a separate browser tab.
6. Click **Edit** in the title bar of the Report from Orion Report Writer resource.
7. ***If you do not want to use the default title provided,*** enter a new **Title** for the header of the reports list.
8. ***If you want a subtitle,*** enter a new **Subtitle** for the custom list of reports.
9. Check the reports that you want to include in your custom list of reports. **Note:** To allow a user to view a report included in the custom list, you must set the report access for the account. For more information, see Configuring an Account Report Folder.
10. Click **Submit**.

Filtering Nodes

Your Orion Web Console can maintain a customizable node list for your network. Node lists can be configured for specific views using SQL query filters. The following steps set up node filtering for node lists included in web console views. **Note:** Click the resource title to display the resource in a new browser window.

To enable filtering on a node list:

1. Navigate to the view to which you want to add the node list, and then click **Customize Page**.
2. Click the plus sign in the appropriate column to open the Add Resource dialog.
3. Enter "`nodes`" in the **Search** box, and then click **Search**.
4. Select the box before **All Nodes - Table**, and then select **Add Selected Resources**.
5. Use the arrow icons by the column to position the table, and then click **Preview** to display the resource in a separate browser tab.
6. Click **Edit** in the title bar of the All Nodes – Table resource.
7. ***If you do not want to use the default title provided,*** enter a new **Title** for the node list.
8. ***If you want a subtitle,*** enter a new **Subtitle** for the node list.

9. ***To filter your node list by text or IP address range,*** provide the text or IP address range by which you want to filter your node list in the Filter Text field, as shown in the following examples:
    - Type **Home** in the Filter Text field to list all nodes with "Home" in the node name or as a location.
    - Type **192.168.1.*** in the Filter Text field to list all nodes in the 192.168.1.0-255 IP address range.
10. Select the property that is appropriate to the filter text provided above, as shown in the following examples:
    - ***If you typed*** **Home in the Filter Text area,** select **Node Name** or **Location** to list nodes with "Home" in the node name or as a location.
    - ***If you typed*** **192.168.1.*** ***in the Filter Text area,*** select **IP Address** to list only nodes in the 192.168.1.0-255 IP address range.
11. ***To apply a SQL filter to the node list,*** enter an appropriate query in the **Filter Nodes (SQL)** field.

    Notes:

    - **Filter Nodes (SQL)** is an optional, advanced, web console feature that requires some knowledge of SQL queries. Click **+** next to **Show Filter Examples** to view a few example filters.
    - By default, node list resources are designed to sort nodes alphabetically by node caption. This configuration cannot be overwritten using a SQL filter, so **order by clauses included in SQL filters are redundant and will result in Custom SQL filter formatting errors.**
12. Click **Submit**.

Grouping Nodes

Your Orion Web Console can maintain a customizable node list for your network. Node lists can be configured for specific views with node grouping. The following steps set up node grouping for node lists included in web console views.
Note: Click the resource title in the title bar menu to display the resource by itself in a browser window.

To enable grouping on a node list:

1. Navigate to the view to which you want to add the resource, and then click **Customize Page**.
2. Click the plus sign in the appropriate column to open the Add Resource dialog.
3. Enter "`nodes`" in the **Search** box, and then click **Search**.
4. Check the box before **All Nodes - Tree**, and then select **Add Selected Resources**.
5. Use the arrow icons by the column to position the tree resource, and then click **Preview** to display the resource in a separate browser tab.
6. Click **Edit** in the title bar of the All Nodes – Tree resource.
7. ***If you do not want to use the default title provided,*** enter a new **Title** for the node list.
8. ***If you want a subtitle,*** enter a new **Subtitle** for the node list.
9. Select up to three criteria, in specified levels, for **Grouping Nodes** within your web console view.
10. Select whether you want to put nodes with null values **In the [Unknown] group** or ungrouped, **At the bottom of the list**.
11. ***If you want to apply a SQL filter to the node list,*** enter an appropriate query in the **Filter Nodes** field.

    Notes:

    - **Filter Nodes (SQL)** is an optional, advanced, web console feature that requires some knowledge of SQL queries. Click **+** next to **Show Filter Examples** to view a few example filters.
    - By default, node list resources are designed to sort nodes alphabetically by node caption. This configuration cannot be overwritten using a SQL filter, so **order by** clauses included in SQL filters are redundant and will result in Custom SQL filter formatting errors.
12. Click **Submit**.

Adding a Service Level Agreement Line to Charts (Orion NPM)

The Orion Web Console can display a service level agreement (SLA) line on any Min/Max/Average bps chart. When you add a customer property named "SLA" and populate the field with your device SLA values, the Orion Web Console displays the appropriate line on your charts.

Notes:

- Interface data is only available in SolarWinds NPM.
- The SLA line may not appear immediately. It may take several minutes for the change to be detected by the Orion web engine.

To add a Service Level Agreement line to Min/Max/Average bps charts:

1. Click **Settings**.
2. In the Node & Group Management section, click **Manage Custom Properties**.
3. Click **Add Custom Property**.
4. Select **Interfaces** as the custom property object type, and then click **Next**.
5. Click **SLA** in the list of predefined **Property Templates**, make any required changes to the fields displayed, and then click **Next**.
6. Click **Select Interfaces**.
7. Select and add all interfaces to which you want to apply the same service level, and then click **Select Interfaces**.
8. Enter the SLA value (in bps) in the **SLA** column for each interface you want to label with SLA values. For example, type **1544000** for a T1 interface (1.544 Mbps) or **225000** for a serial connection running at 225 Kbps.
9. ***To enter a different SLA value for a different set of interfaces,*** click **Add More**, and then repeat interface selection and value population as indicated previously.
10. Click **Submit**.
11. Browse to the Interface Details view of one of the interfaces you edited. The SLA line displays on any chart showing Min/Max/Average bps.

Exporting Views to PDF

Many views in the Orion Web Console may be exported directly to portable document format (.pdf). Views that may be exported display **Export to PDF** in the top right corner of the exportable view.

Note: The Export to PDF feature requires IIS Anonymous Access. Confirm that the IUSR_SERVERNAME user is in the local Users group on your Orion server.

To export a view to PDF:

1. Open the web console view to export, and then click **Export to PDF** in the top right corner of the view.
2. ***If you are prompted to save the .pdf file,*** click **Save**.
3. Navigate to an appropriate location, provide an appropriate file name, and then click **Save**.

Using the Orion Web Console Message Center

The Message Center provides a single, customizable view in the web console where, in a single table, you can review all events, alerts, traps, and Syslog messages on your network.

To view and configure the Message Center:

1. Click **Home > Message Center**.
2. ***To display messages for specific devices,*** select appropriate device properties in the Filter Devices area.
3. In the Filter Messages area, select the **Time period** for the messages you want to review, and then provide the number of messages you want to show.
4. ***To show all messages, including messages that have been acknowledged,*** check **Show acknowledged** in the Filter Messages area.
5. ***To display only certain types of messages,*** filter messages as shown in the following steps:
    a. ***To view alerts,*** confirm that **Show active alerts** is checked, and then select the type of alerts to display.
    b. ***To view event messages,*** confirm that **Show event messages** is checked, and then select the type of events to display.
    c. ***To view Syslog messages,*** confirm that **Show syslog messages** is checked, and then select the **Severity** and **Facility** of the Syslog messages you want to display.
    Note: For more information about Syslog severities and facilities, see Syslog Message Priorities.
    d. ***To view received traps,*** confirm that **Show received traps** is checked, and then select the **Trap type** and **Community String** of the traps you want to display.
    e. ***To view audit events,*** confirm that **Show Audit Events** is checked, and then select the **Action type** and **User** corresponding to the audit events you want to display.
6. Click **Apply** to update the list of displayed messages.

Customizing the Orion Web Console

The following sections provide details for customizing your Orion Web Console:

- Customizing Web Console Menu Bars
- Changing the Web Console Color Scheme
- Changing the Web Console Site Logo

Customizing Web Console Menu Bars

The menu bars displayed at the top of every page may be configured to display various menu items. You can also define menu items and add them to custom menu bars. For more information about customizing menu bars for individual accounts, see Editing User Accounts.

To customize web console menu bars:

1. Click **Settings** in the top right of the web console.
2. Click **Customize Menu Bars** in the Customize Navigation & Look grouping of the Orion Website Administration page.
3. ***If you want to modify an existing menu,*** click **Edit** on the menu bar you want to modify, and then click and drag items between the Available items list on the left and the Selected items list on the right until the Selected items list includes all the items you want to include in your edited menu.
   Note: Hover over any view title to read a description. Selected items display from left to right in the edited menu bar as they are listed from top to bottom.
4. ***If you want to create a new menu bar,*** complete the following steps:
   a. Click **New Menu Bar** at the bottom of the page, and provide a **Name for the New Menu Bar**.
   b. Click and drag the items you want to include in your new menu bar from the Available items list on the left to their correct relative locations in the Selected items list on the right.
   Note: Hover over any view title for a description. Selected items display from left to right in the new menu bar as listed from top to bottom.

5. ***If you want to add a custom menu item,*** complete the following steps:
    a. Click **Edit** under the menu bar to which you are adding the custom item.
    b. Click **Add** at the bottom of the page, and provide the **Name**, **URL**, and **Description** of your custom menu item.
    c. ***If you want the menu option to open in a new window,*** check **Open in a New Window**.
    d. Click **OK**.
6. ***If you want to delete a menu item,*** click and drag the item to delete from the Selected items list on the right to the Available items list on the left. **Warning:** Do not delete the **Admin** option from the Admin menu bar.
7. ***If you want to change the location of an item in your menu,*** click and drag items to move them up and down in the Selected items list.
8. ***If you have finished editing your menu bar,*** click **Submit**.

Changing the Web Console Color Scheme

The overall color scheme of the Orion Web Console may be changed to any of several color schemes that are viewable by all users, as shown in the following procedure.

To change the web console color scheme:

1. Click **Settings** in the top right of the web console.
2. Click **Color Scheme** in the Customize grouping.
3. Select the desired color scheme, and then click **Submit**.

Changing the Web Console Site Logo

The Orion Web Console can be configured to display your logo instead of the default SolarWinds banner across the top of every web console page. The following steps change the default SolarWinds web console banner.

To change the web console banner:

1. Create an appropriately sized graphic to replace the SolarWinds logo.

    Notes: The SolarWinds banner file is 271x48 pixels at 200 pixels/inch.

The SolarWinds.com **End User License Agreement** prohibits the modification, elimination, or replacement of the SolarWinds.com logo, the link on the menu bar, or the SolarWinds copyright line at the bottom of the page.

2. Place your graphic in the **images** directory.

   Note: By default, it is in **C:\Inetpub\SolarWinds\NetPerfMon**.

3. Log in to the web console as an administrator, and then click **Settings** in the top right of the web console.
4. Click **Web Console Settings** in the Settings grouping of the Orion Website Administration page.
5. Ensure the **Site Logo** box is checked, and click **Browse** to navigate to the replace image.

Orion Web Console and Chart Settings

The Orion Website Settings page allows an Orion Web Console administrator to set a number of options that apply to the web console user environment.

The following settings are configured on this page:

- Web Console Settings
- Auditing Settings
- Chart Settings
- Discovery Settings

To configure Orion Website and Chart Settings:

1. Click **Settings** in the top right of the web console, and then click **Web Console Settings** in the Product Specific Settings group.
2. When you finish configuring web console and chart settings, click **Submit**.

Web Console Settings

The following options are configured on the Orion Web Console Settings page:

- **Session Timeout** is the amount of time (in minutes) the Orion Web Console waits through user inactivity before the user is logged out.
- **Windows Account Login** allows you to select whether or not you want to enable automatic login with Windows Active Directory credentials. With this feature enabled, in the future, the current user can log in automatically.
- **Page Refresh** specifies the amount of time that passes before a web console page, or view, reloads automatically.
- **Site Logo URL** is the local path to the banner graphic that appears at the top of every web console page. For more information about changing the banner to display your logo, see Changing the Web Console Site Logo.
- **NOC View Logo** is the local path to the banner graphic that appears at the top of every NOC view web console page.
- **Site Login Text** is optional text displayed on the Orion Web Console login page. The text entered here is seen by all web console users when they log in. HTML tags are allowed.
- **Help Server** is the URL of the server where online help for Orion products is stored. The default location is http://www.solarwinds.com. If you are in an Internet-restricted network environment but require access to online help, download the entire online help, copy it to a web server, and then change the Help Server URL to that of the web server.
- **Status Rollup Mode** establishes the way the availability status of a collection of nodes on the node tree or on a map is displayed in the web console.

  There are the following options for when there are nodes of differing statuses in a selected group:

  - **Mixed Status shows Warning**, the default status, ensures the status of a node group displays the worst warning-type state in the group. If none of the group members have a warning-typed state but the group contains both up and down nodes, a Mixed Availability warning state is displayed for the whole group. For example, **Critical** + **Down** = **Critical**, **Critical** + **Warning** = **Critical**, and **Up** + **Down** = **Mixed Availability**.

    - **Show Worst Status** ensures the worst state in a node group is displayed for the whole group. For example, **Up** + **Down** = **Down** and **Unreachable** + **Shutdown** = **Shutdown**.
- **Child Status Rollup Mode** indicates how the status of any single node on the node tree or on a map is displayed. You can show the status of the node and its children, node status and interfaces, if you have Orion NPM installed, or just node ICMP status.
    - Select **Show Worst Status** to ensure that the worst status of the node group is displayed for the whole group (e.g. red if any of the nodes are down).
    - Select **Show Worst Status (Interfaces only)** to ensure that the worst status of any of the interfaces on a selected node is displayed.
    - Select **Show Worst Status (Applications only)** to ensure that the worst status of any of the applications on a selected node is displayed.
    - Select **Show only ICMP Status** to only display up/down status for monitored interfaces.
- **Child Status Display Mode** designates how the status of the children of any single node on the node tree or on a map is displayed. You can show the status of the node and any of its children with either a static of a blinking icon. By default, Orion uses a static icon to display the status of child objects.
- **Integration Tips** enables you to show or hide the list of products in the How SolarWinds Products Work Together section of the Settings page.
- **Drag and Drop Views** enables you to turn on or off the ability to drag resources around on views.

Auditing Settings

The **Enable audit trails** option enables you to keep a record of all actions taken by web console users. Depending on the number of technicians or the activity level of your installation, this may increase the storage needs of your database.

Chart Settings

The following chart settings may be configured in the Chart Settings section of the Web Console Settings page:

- **Chart Aspect Ratio** is the height/width ratio for web console charts. This ratio should be set between **0.25** and **3.0** to avoid erratic display problems, though the performance of individual systems may differ.
- **Thumbnail Aspect Ratio** is the height/width ratio for chart thumbnails.
- **95th Percentile Calculations** is a setting that adds annotation lines to charts at the entered percentile. This value is normally set to 95. For more information, see 95th Percentile Calculations.
- The **Maximum number of data series displayed on chart** setting determines the maximum number of data series that will display on a chart at the same time. The default value for this setting is **10**.
- The actual data points that are used to create a chart may be shown by checking **Show data points on lines**.
- **Font Size** sets the default relative size, **Small**, **Medium**, or **Large**, of the text that is displayed within charts in the Orion Web Console. This setting is independent of your browser settings. The font settings in your browser will affect resource headers and some resource contents.

Other Settings

The Discovery, Worldwide Map and Active Alert Settings sections provide the following settings:

- **Notify about new removable volumes** allows you to indicate whether or not you want to be notified when removable volumes are added to your network and discovered during network discovery.
  You should configure the default send email action to receive notifications. For more information about network discovery in Orion, see Discovering and Adding Network Devices in the Orion Common Components web help.
- **Automatic Geolocation** enables automatic geolocation on worldwide maps when checked.
- **Active alerts** refresh enables you to specify how often the active alerts grid page is refreshed.

Active Alerts Settings

Select how frequently you want the active alerts resource to refresh. Any alerts that trigger within the refresh interval appear when the grid refreshes.

Using Node Filters

When you are managing or monitoring large numbers of network devices, node list resources can easily become very large and difficult to navigate. Filters are optional SQL queries that are used to limit node list displays for easier resource navigation. SQL queries can be made on any predefined or custom properties. For more information about defining custom properties, see Creating a Custom Property.

Note: If you have upgraded to SolarWinds Network Performance Monitor version 2015.1.2, your custom SQL or SWQL query or filter may no longer work correctly. For a list of database changes from SolarWinds Network Performance Monitor version 2014.2 to version 2015.1.2, including new tables, column changes, or data constraint or data type changes, see the Database Changes spreadsheet.

To apply a node filter:

1. Click **Edit** in any node list resource.
2. Provide an appropriate SQL query in the **Filter Nodes (SQL)** field, and then click **Submit**.

The following are a few example filters with associated SQL queries.

Note: By default, node list resources are designed to sort nodes alphabetically by node caption. This configuration cannot be overwritten using a SQL filter, so **order by** clauses included in SQL filters are redundant and will result in Custom SQL filter formatting errors.

- Filter the results to only show nodes that are not **Up**:

  Status<>1

  The following are valid status levels:

  - **0 = Unknown** (current up/down status of the node is unknown)
  - **1 = Up** (The node is responding to PINGs)
  - **2 = Down** (The node is not responding)
  - **3 = Warning** (The node may be responding, but the connection from the server to the Node is dropping packets)

- Only show Cisco devices: **Vendor = 'Cisco'**
- Only show devices in Atlanta. (using a custom property named City):

  City = 'Atlanta'
- Only show devices beginning with "AX3-": **Caption Like 'AX3-*'**
- Only show Nortel devices that are Down:

  Vendor Like 'Nortel*' AND Status=2
- Only show devices ending in '-TX':

  Vendor Like '*-TX'

Customizing Charts in the Orion Web Console

The Orion Web Console provides many charts for all monitored objects, which may be customize to your own requirements, as covered in the following sections.

- Some charts have an **Edit** button that enables you to edit titles, time periods and other details. For more information, see Customizing Charts.
- Other charts have a dropdown menu, enabling you to change the date range, edit the chart or display raw data. For more information, see Customizing Custom Charts.

In some cases, the same chart is available in both versions.

Customizing Charts

If the chart you want to customize has an **Edit** button, clicking it will open the Edit Resource page. Here you can customize the following fields:

Title

Enter or edit a title for this resource.

Subtitle

Enter or edit an optional subtitle for the resource.

Depending on the type of chart, some of the following will be available:

Calculated series: Show a trend line

Check this box to display a trend line on the graph. This shows potential future results as extrapolated from collected historical data. **Note:** Due to the broad array of factors that can affect the performance of devices on your network, are intended as approximate predictions of future data only.

Calculated series: Show the sum of all data series

Check this box if you want to display the sum of all data series in the form of stacked bars or lines.

Calculated Series: Show the 95th percentile line

Check this box to show the 95th percentile line. This is a well-known statistical standard used to discard maximum spikes, based on 5 minute data samples. The calculation gathers these values every 5 minutes for however long you select, throwing away the top 5% so as to yield the 95th percentile value. For more information, see 95th Percentile Calculations

Or:

Maximum Number of Items to Display:

Enter the highest number of items you want to display in this chart.

Time periods: Default zoom range

Select the default range of data to be displayed from the dropdown list.

Time periods: Amount of historical data to load

Select the amount of historical data to load from the dropdown list.

Time periods: Sample interval

Select the sample interval to be used from the dropdown list. Each sample interval is represented on a chart by a single point or bar. Data within a selected sample interval is summarized automatically.

Advanced: Chart title

Enter a title to appear above the chart.

Advanced: Chart Subtitle

Enter an optional subtitle to appear beneath the chart title. The default is `${ZoomRange]`, which shows the selected zoom range.

Customizing Custom Charts

If the chart you want to customize has a dropdown menu in its top line, the following information applies.

Custom Chart Dropdown Menu Options

The dropdown menu of the custom chart resource provides the following options for viewing and configuring chart data:

- View chart data over the **Last 7 Days** or over the **Last 30 Days**
- Select **Edit Chart** or click on the chart to open the chart resort in a new tab.
- **View Chart Data** as an HTML format document
- **View Chart Data in Excel** to see chart data in an Excel™-compatible format

Editing the Chart

If you click **Edit Chart** from the dropdown menu or click on the chart, the chart resource is opened in a new tab and you can edit the following:

Chart Titles: Title

Enter a title to be displayed above the chart.

Chart Titles: Subtitle

Enter an optional subtitle to be displayed beneath the title.

Chart Titles: Subtitle #2

Enter a second optional subtitle to be displayed beneath the title.

Time Period: Select a Time Period

Select the time period that you want the chart to cover.

Alternatively, you can enter a specific time period for the chart.

Time Period: Beginning Date/Time

Enter the start date and time for the chart in one of the formats shown. If you do not enter a time, this will default to 12:00:00 AM.

Time Period: Ending Date/Time

Enter the end date and time for the chart in one of the formats shown. If you do not enter a time, this will default to 12:00:00 AM.

Sample Interval

Check this box to display a trend line on the graph. This shows potential future results as extrapolated from collected historical data.
Note: Due to the broad array of factors that can affect the performance of devices on your network, are intended as approximate predictions of future data only.

Chart Size: Width

Enter a custom width, in pixels, for this chart. The default is 640.

Chart Size: Height

Enter a custom height, in pixels, for this chart. Enter 0 to maintain the original width/height ratio.

Font Size

Select the font size for the chart from the dropdown list.

Trend Line: Show Trend

Check this box to display a trend line on the graph. This shows potential future results as extrapolated from collected historical data.
Note: Due to the broad array of factors that can affect the performance of devices on your network, are intended as approximate predictions of future data only.

Display Chart Data: Raw Data

Click to display or save the data being used in this report as an xls file.

Display Chart Data: Chart Data

Click to display the data in this report as a HTML table in the web browser.

Custom Node Charts

The following node-related charts, grouped by type, are available as resources within the Orion Web Console. You can display them on Node Details views, by adding the Custom Node Chart resource.

For more information about adding resources to Orion Web Console views, see Customizing Views. For more information about Chart settings, see Orion Web Console and Chart Settings.

Availability

The following charts display node availability information over custom time periods for nodes monitored by Orion.

- Availability
- Availability – Autoscale
- Availability and Response Time

CPU Load

The following charts display CPU loading information over specified periods of time for nodes monitored by Orion.

- Average CPU Load
- Min/Max/Average CPU Load

Memory Usage

The following charts present memory usage information over custom time periods for nodes monitored by Orion.

- Average Memory Usage
- Memory/Buffer Failures
- Min/Max/Average Memory Usage
- Percent Memory Used

Packet Loss and Response Time

The following charts are available to display historical statistics about packet loss and response time for nodes monitored by Orion.

- Availability and Response Time
- Average Response Time
- Average Response Time and Packet Loss

- Min/Max/Average Response Time
- Min/Max/Average Response Time and Packet Loss
- Percent Loss – Bar Chart
- Percent Loss – Line Chart

Custom SolarWinds NPM Interface Charts

In addition to the default charts provided with any Orion installation, SolarWinds NPM provides the following interface-related charts, grouped by type, as resources within the Orion Web Console that you can customize for your own use.

Note: To add any interface chart to a web console view dealing with monitored interfaces, add the Custom Interface Chart resource. For more information about adding resources to views, see Editing Views. For more information about customizable chart types available in the web console, see Customizing Charts in the Orion Web Console.

Discards and Errors Charts

The following charts are available to display information about discards and errors on interfaces monitored by SolarWinds NPM.

- In/Out Discards – Step Chart
- In/Out Errors – Step Chart
- In/Out Errors and Discards – Step Chart

Percent Utilization Charts

The following charts are available to display percent utilization information for monitored interfaces in SolarWinds NPM.

- Min/Max/Average Percent Utilization
- Min/Max/Average Transmitted + Received Traffic Percent Utilization
- Percent Utilization – Line Chart
- Percent Utilization – Step Chart

Traffic Charts

The following charts are available to display information about interface traffic, including multicast traffic, on devices monitored by SolarWinds NPM.

- Average bps – Line Chart
- Average bps – Step Chart
- Average Packets per Second
- Min/Max/Average bps In/Out
- Min/Max/Average bps Received
- Min/Max/Average bps Transmitted
- Min/Max/Average bps Transmit+Receive
- Min/Max/Average bps Transmit+Receive Percent Utilization
- Min/Max/Average Packets In/Out
- Multicast Traffic
- Total Bytes Transferred
- Total Packets Transmitted/Received

Other Charts

The following charts are also available to display information about monitored interfaces.

- Custom Interface Chart enables you to create your own custom interface chart.
- Multiple Object Chart enables you to create your own custom charts that compare data for multiple monitored objects.

Custom Volume Charts

The following volume-related charts, grouped by type, are available as resources within the Orion Web Console. To add any of these charts to a web console view dealing with monitored volumes, add the Custom Volume Chart resource to the Volume Details view. For more information about adding resources to Orion Web Console views, see Customizing Views. For more information about customizing the following charts, see Orion Web Console and Chart Settings.

Allocation Failures

Shows the number of disk allocation failures that have occurred on the selected volume.

Min/Max/Average Disk Usage

Shows both the total disk space available and the average amount of disk space used on the selected volume. Bars are also included to show minimum and maximum levels of disk usage.

Percent Disk Usage

Shows the total available disk space and the average amount of disk space used, as a percentage of the total available, on the selected volume.

Volume Size

Shows the total disk space available on the selected volume.

Custom Object Resources in the Orion Web Console

The Orion Web Console provides a Custom Object resource that enables you to configure any of a wide array of resources to display performance data for any specific monitored objects.

The following sections provide more information about editing a Custom Object resource, selecting monitored objects, and configuring the data displayed in a Custom Object resource:

- Editing a Custom Object Resource
- Selecting Custom Objects and Resources
- Available Custom Resources

Editing a Custom Object Resource

The following procedure edits a Custom Object resource.

To edit a Custom Object resource:

1. Click **Edit** in the header of a Custom Object resource.
2. Edit the resource **Title** and **Subtitle** as appropriate.
3. Select an appropriate object type from the **Choose Object Type** selection box.
4. Click **Select Object** to select appropriate monitored objects. For more information, see Selecting Custom Objects and Resources.
5. **Select a Chart** to include in your custom object resource.
6. ***If you want to automatically display nodes related to the current view,*** check the corresponding **Select object** option.
7. ***If you want to limit the number of data series that are displayed in your resource,*** check the **Limit Series** option, and then select the number of series to allow.
8. Select whether or not you want to **Show Sum in Data Series**.
9. Select the **Time Period** and **Sample Interval**.
10. If you want to automatically hide the resource when there is no data for it to

report, select **Yes** for the **Auto-Hide Resource** option.

11. ***If you have completed your edits,*** click **Submit**.

Selecting Custom Objects and Resources

The following procedure selects a network object for a selected Custom Object resource.

Note: The following procedure assumes both that you are editing a custom object resource and that you are already viewing the Select Orion Nodes view in the web console.

To select a custom monitored object for a Custom Object resource:

1. In the **Group by:** field, select an appropriate object grouping criterion.

   Note: Defined custom properties are listed for all grouping types.

2. Either check a listed group of objects or expand listed groups to check included objects, and then click the green arrow (➡) to move selected objects into the selected objects pane on the right.
3. Check the objects to monitor in selected objects pane on the right.
4. Click **Submit**.
5. Select the desired resource type in the **Select object resource** field, and then configure options as required. For more information about available resources, see Available Custom Resources.

Available Custom Resources

A Custom Object resource may be configured to provide the same data as any of a number of Orion Web Console resources for a selected network object:

Notes:

- Resource availability is dependent on the Orion products installed.
- For more information about any available custom resource, click **Help** in the resource title to view the corresponding help topic.

Accessing Nodes Using HTTP, SSH, and Telnet

The Orion Web Console supports the use of HTTP, SSH, and Telnet protocols for remote device access if associated applications like PuTTy and FiSSH on your Orion server are properly registered. For more information, see the MSDN online help.

Launch remote access applications from any Details view as follows:

- To browse directly to the viewed device using a web browser, click  .
- To open a secure shell (SSH) to a monitored device, click  .
- To open a Telnet session with a monitored device, click  .

Chapter 5: Monitoring Devices in the Web Console

Like all products in the Orion family, Orion Network Performance Monitor offers immediate insight into the performance of your network.

The following sections describe the various features and functions that enable you to monitor and manage all your network devices from the Orion Web Console.

Notes:

- For more information about network device monitoring and management features specific for individual device types and technologies, see Monitored Device Types and Technologies.
- For more information about adding devices to the Orion Web Console, see Discovering and Adding Network Devices.

Network Overview

By default in all NPM installations, the Orion Web Console offers a Network Overview that provides, at a glance, a wide array of information about all the nodes and interfaces on your network that NPM is currently monitoring. The Network Overview lists a node property status icon to the left of each monitored node on your network. To the right of each node is a row of status icons, where each icon represents the status of a selected interface property on the listed node. A legend at the bottom of the Network Overview provides translations between icon colors and measured values for each network device property. For more information, see Status Icons and Identifiers.

The following table lists the types of information for monitored nodes and interfaces that may be communicated on the Network Overview.

Node Property	Interface Property
Response Time	Percent Utilization
Average Response Time	Type
Maximum Response Time	Errors and Discards Today
CPU Load	Errors and Discards This Hour
Percent of Memory Used	Status
Percent Packet Loss	Traffic
Machine Type	
Node Status	

Hovering over any icon, IP address, or node name opens a tooltip providing current status information about the associated node or interface.

To view the Network Overview:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Log in to the Orion Web Console, and then click **Network > Overview**.

3. Select the node property you want to view in the **Nodes** field, and then select the interface property you want to view in the **Interfaces** field.
4. Click **Refresh** to show the updated overview.

Viewing Node Resources

The List Resources feature of the Orion Web Console Node Management utility allows you to immediately see all monitored interfaces, volumes, and interface charts on a selected node, as shown in the following procedure.

To view a list of all resources present on a node:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Nodes** in the Node & Group Management grouping of the Orion Website Administration page.
3. Locate the node to view using either of the following methods:
    - Use the search tool above the node list to search your Orion database for the node you want to view.
    - Select an appropriate **Group by:** criterion, and then click the appropriate group including the node to view.
4. Check the node to view from the list, and click **List Resources** on the Node Management toolbar. The interfaces and volumes for this nodes are displayed, showing which are being currently monitored.

Monitoring Interface Status

Monitoring node and interface availability is important for immediate troubleshooting. However, in some areas, an interface being down does not directly impact Internet or intranet connectivity.

SolarWinds NPM provides you with the Interface Downtime resource which displays more information about interface availability, specifying when and how long the interface was down. To display downtime for all monitored interfaces on a node, add the Interface Downtime resource on the appropriate node view.

Note: The downtime information might be useful for example for SLA providers who want to prove specific times of interface/port unavailability.

To display more details about an interface downtime:

1. Log into the Orion Web Console.
2. Navigate to the appropriate interface or node view and consult the Interface Downtime resource.

By default, the resource shows the interface status in the last 24 hours, each hour represented as a block in the appropriate color.

To take a more detailed look at a problematic section, position the mouse over the appropriate spot on the graph.

Changing the Time for Displayed Interface Status

By default, the resource displays downtime data for the last 24 hours, one block representing 1 hour. You can display any time frame within the stored history.

To change the displayed period

1. Go to the Interface Downtime resource and click **Edit**.
2. Select **Custom** in the **Downtime period** list and specify **Beginning** and **End** dates and times.
3. When displaying longer time periods, you might need to change the time frame represented by one block. Select **Custom** in **Display settings** and provide an appropriate value.
4. Click **Submit** to apply your changes.

Editing the Title and Subtitle

To edit the resource labels, click **Edit**, enter appropriate labels, and click **Submit**.

Changing How Long the Interface Status History Is Retained

By default, interface status history is stored in the database for 7 days.

To change the interface status history retention:

1. Log on to the Orion Web Console as an administrator.
2. Click **Settings**, and then click **Polling Settings** in the Thresholds and Polling grouping.
3. Scroll down to **Database Settings**, and provide how long you want to keep interface status history in the database in the **Downtime History Retention** field. Enter a value in days, from 7 to 60 days.

Disabling Interface Downtime Monitoring

Monitoring interface downtime can affect performance of SolarWinds NPM. To decrease the load, you can disable interface downtime monitoring. For periods where interface downtime was not monitored, the Interface Downtime resource shows grey blocks.

To disable interface monitoring:

1. Log on to the Orion Web Console as an administrator.
2. Navigate to Polling Settings via **Settings > Polling Settings** in the Thresholds & Polling grouping.
3. Clear the **Interface Downtime Monitoring** box in the Network grouping.
4. Click **Submit** to apply your changes.

Interface downtime will not be monitored any more. Starting from now, the Downtime Monitoring resource will display "Downtime monitoring is disabled. To enable it, go to Polling Settings."

Detecting Possible Duplex Mismatches

One of the most common causes of performance issues on 10/100 or 100/1000 Mbit Ethernet links occurs when one port on the link operates at half-duplex while the other port operates at full-duplex.

NPM helps you detect configuration errors, and supports you in predicting possible duplex mismatches.

To detect duplex mismatches:

1. Log into the Orion Web Console.
2. Go to the appropriate node details view.
3. Consult the Possible Duplex Mismatches resource.

   The resource lists all duplex interfaces on the node, percentage of transmit and receive errors, neighboring node and interface. If the neighboring interface or node is not monitored in NPM, the appropriate columns are empty.
   The last column displays the duplex mode issue - Mismatch, or Unknown.

   Duplex Mismatch

   To be able to detect duplex mismatches, your nodes need to meet the following requirements:

   - Both nodes must be monitored by NPM
   - Both nodes must be connected.
   - Both nodes must be in the up state during the discovery
   - Duplex of both devices must be identified as Full or Half.

   The resource shows all duplex mismatches, not only 100% duplex mismatches. These are reported on by the **Duplex Mismatch** alert.

   Possible Duplex Mismatch

   If at least one of the link interfaces has the duplex mode defined as half or full, the resource helps you identify possible mismatch.

Possible duplex mismatches are visible in the duplex mode column as the **Unknown** duplex mode. They are identified in the following cases:

- If the switch port reports more than 0.5% receive or transmit errors.
- If the switch port reports CRC errors.
- If the switch port reports Late Collision errors.

How do I resolve mismatches?

To resolve a duplex mismatch, make sure your hardware is working, and unify the duplex mode configuration on neighboring interfaces.

Troubleshooting

The Possible Duplex Mismatches does not display on Node Details view

If the resource does not appear on the node details view, there might be a performance issue due to the amount of interfaces and topology connections. Check the following logs for the occurrence of mismatch information:

C:\ProgramData\SolarWinds\Logs\Orion\OrionWeb.log

C:\ProgramData\SolarWinds\InformationService\v3.0\Orion.InformationService.log

The Possible Duplex Mismatches resource does not display percentage of errors

Possible causes:

- No statistical data for these interfaces.
- A performance issue connected with getting statistic information for the resource.

Viewing Node Data in Tooltips

Node tooltips provide immediate status overviews of monitored nodes. To view a quick overview of any monitored node in the web console, hover over the device name. The information in the following tables displays immediately.

Note: You can also view interface data in tooltips.

Node Data	
Node Status	Current status of the node. (Up, Down, Warning, Unmanaged, or Unreachable)
Polling IP Address	The IP address currently assigned to the selected node
Machine Type	The vendor icon and vendor description of the selected node
Average Response Time	The measured average response time of the selected node as of the last node poll
Packet Loss	The percent of all transmitted packets that are lost by the selected node as of the last node poll
CPU Load	The percent of available processing capacity on the selected node that is currently used as of the last node poll
Memory Used	The percent of available memory on the selected node that is currently used as of the last node poll

Viewing Interface Data in NPM Tooltips

In addition to the tooltips available by default for nodes monitored in the Orion Web Console, interface tooltips provided by NPM display immediate status overviews of monitored interfaces. To view a quick overview of any monitored interface in the web console, hover over the interface name. The following interface information is then displayed immediately.

Note: For more information about tooltips, including information about node tooltips provided by default in the Orion Web Console, see Viewing Node Data in Tooltips.

Interface Tooltip Data	
Interface Name	The name of the interface as discovered from its parent node
Operational Status	Operational status of the interface
Administrative Status	Administrative status of the interface (enabled or disabled)
Interface Type	Numerical type of the interface, as determined by NPM when the parent node is discovered.
Transmitted Current Traffic	The amount of traffic the interface was transmitting as of the last interface poll
Transmitted Percent Utilization	The percent of available bandwidth used for traffic transmitted from the interface as of the last interface poll
Received Current Traffic	The amount of traffic the interface was receiving as of the last interface poll
Received Percent Utilization	The percent of available bandwidth used for traffic received by the interface as of the last interface poll

Customizing the Manage Nodes View

The Manage Nodes view is the primary user interface for device management in the web console, and it is composed of both the node tree, a hierarchical directory of monitored elements, in the left pane and a more detailed listing of all monitored devices in the main pane. Devices in the main pane are grouped according to the **Group by:** criterion selected in the left pane. The following sections provide steps for customizing the Manage Nodes view.

Customizing the Manage Nodes View Node Tree

The node tree in the left pane of the Manage Nodes view provides a hierarchical directory of the devices that are currently monitored. Devices are grouped using any of the following criteria available in the **Group by:** selection field above the node tree.

Note: Currently defined custom properties are also available as columns.

Available Grouping Criteria for the Manage Nodes View Node Tree			
[No Grouping]	EnergyWise	Vendor	Machine Type
Polling Engine	Polling Method	SNMP Version	Status
Location	Contact	Community	RWCommunity
IP Version	City	Comments	Department

Customizing the Manage Nodes View Node List

The node list in the main pane of the Manage Nodes view provides a detailed table listing the devices that are currently monitored. Devices in the main pane are grouped according to the **Group by:** criterion selected to sort the node tree in the left pane.

Click **>>** in the table header to configure any of the following types of information as table columns.

Note: Currently defined custom properties are also available as columns.

Available Manage Nodes View Columns		
IP Address	IP Version	Status

Available Manage Nodes View Columns		
Contact	Location	Polling Method
Polling Engine	City	Comments
Department		

Editing Node Properties

The following procedure provides the steps required to edit monitored node properties using the Node Management utility of the Orion Web Console.

Note: Editing multiple objects in multiple browser tabs in the same session may result in lost data or database errors. Limit object management activities to a single browser tab to prevent database errors and data losses.

To edit node properties in the Orion Web Console:

1. Click **Settings** in the top right of the web console, and then click **Manage Nodes** in the Node & Group Management grouping.
2. Select **Nodes** from the **Show** drop-down list, and locate the node to edit using either of the following methods:
   - Use the search tool above the node list to search your Orion database for either the object you want to edit or the parent node of the volume you want to edit.
   - Select an appropriate **Group by:** criterion, and then click the appropriate group including either the node to edit or the parent of the object to edit.
3. Check the node to edit and click **Edit Properties**:
4. ***To rename the node,*** type the new name in the **Name** field.

   Note: Changing the node name only affects the way the node is identified on charts and graphs within System Manager and in the Orion Web Console. It does not impact the node as it is referenced on the network.

5. ***To change the Polling IP address*** type the new address in the **Polling IP Address** field, or click **Select IP Address**, select from the list displayed and click **Select IP Address**.

Warning Unlike changing the name of a node, changing the IP address does affect data collection. Do not change the IP address, unless it has changed on your network, in which case this allows you to continue accumulating statistics without having to reconfigure the node.

6. ***To dynamically assign the IP address of the selected node,*** check **Dynamic IP Address (DHCP or BOOTP)**, and then provide the **DNS Hostname** and select the appropriate **IP Address Resolution** format (**IPv4** or **IPv6**) for the selected node.

   Note: The IP address will be determined automatically. If the selected device is dual-stack, IPv4 resolution will be used, by default.

7. ***To change the view type for displaying details about this node,*** click on the **View Type** field and select the required type from the drop-down list.
8. ***If you are using SNMP to poll the selected node***, you can:

   a. Edit the **SNMP Version** and **SNMP Port** fields.

   b. ***If you have high-speed interfaces and you are experiencing frequent counter rollovers,*** you may wish to enable 64-bit counters. Confirm that the monitored device supports 64-bit counters and check the **Allow 64-bit Counters** checkbox in the **Node Details** window.

      Note: Some vendor implementations of 64-bit counters produce faulty data. If you are experiencing erratic or incorrect data, you may wish to disable 64-bit counters by unchecking **Allow 64-bit Counters**.

   c. Edit the **Community Strings** (for SNMPv1 and SNMPv2c) or **Credentials**, **Privacy** and **Authentication** settings (for SNMPv3), as required.

Warning: Unlike changing the name of a node, changing the IP address, community string, or SNMP port does affect data collection. Do not change the IP address, community string, or SNMP port in this window unless they have changed on your network. Changing these values in this window allows you to continue to accumulate statistics for a node without having to reconfigure the node if its IP address, community string, or SNMP port changes. Changing the SNMP port applies to statistics polls, Universal Device Pollers, and SNMP trap collection. For more information about custom MIBs, see “Monitoring MIBs with Universal Device Pollers” in the SolarWinds Orion Network Performance Monitor Administrator Guide. For more information on SNMP traps, see “Monitoring SNMP Traps” in the SolarWinds Orion Network Performance Monitor Administrator Guide.

d. Click **Test** to test your provided SNMP settings.

9. ***To change the existing polling intervals,*** provide new intervals in the **Node Status Polling**, **Collect Statistics** and **Poll for Topology Data** fields.
10. ***If there are multiple polling engines in your environment and you want to change the polling engine to which the selected node is assigned,*** click **Change Polling Engine**, and then select a new polling engine.
11. ***To add, edit, or delete an existing dependency that includes the selected node,*** click **Manage Dependencies**, and then add, edit, or delete dependencies, as appropriate. For more information, see Managing Dependencies.
12. ***If you have defined custom properties for nodes,*** you can enter or change those here, or click **Manage Custom Properties** to create or manage custom properties. For more information, see Creating Custom Properties.
13. ***If the selected node is a UCS Manager and you want to poll for UCS data,*** check **Poll for UCS**, and then provide the following:
    Note: After providing credentials, click **Test** to confirm that they are valid for the selected UCS Manager.
    - The **Port** on which the UCS Manager listens to managed UCS objects
    - A valid **User name** and **Password**

14. If the node has UDT ports attached, you can poll Layer 3 data by checking **Poll Layer 3 data from device** and enter the polling interval in the **Layer 3 Polling Interval** field.

    Note: Check **Disable VRF context polling**, if required.

15. Edit the **Web Browse Template**, if required. The default is `http://{{HrefIPAddress}}`.
16. ***To monitor Active Directory users that log on to your network***, check **Active Directory Domain Controller**, and supply the following information.

    a. Select the credential to be used. You can either select existing credential from the dropdown list, or select **<New Credential>**. Note: Administrator credentials are needed only for installing the agent.

    b. ***If you are creating a new credential,*** provide a **Credential name**, enter an appropriate **User name** and **Password**, and enter the password again in the **Confirm password** field.

    c. Click **Test** to validate.

    d. Enter the **Domain Controller Polling Interval** to be used. The default is 30 minutes.

17. ***To poll for VMware,*** check **Poll for VMware** to ensure that Orion acquires any data the VMware device provides to SNMP polling requests, and then complete the following steps to provide required vCenter or ESX Server credentials. For more information, see Requirements for Virtual Machines and Servers.

    a. Select the credential to be used. You can either select existing credential from the dropdown list, or select **<New Credential>**. **Note:** Administrator credentials are needed only for installing the agent.

    b. ***If you are creating a new credential,*** provide a **Credential name**, enter an appropriate **User name** and **Password**, and enter the password again in the **Confirm password** field.

    c. Click **Test** to validate.

18. ***To override the CPU Load, Memory Usage, Response Time, Percent Packet Loss Alerting Thresholds***, check the corresponding boxes, and amend the default values. For more information, see Orion General Threshold Types.

19. ***If you have Network Configuration Manager installed***, there will be an option to manage the node using NCM. For more information, see the Network Configuration Administrator Guide.
20. Click **Submit**.

Editing Interface Properties

The following interface properties are configured on the Edit Interface view of the web console:

- Interface name
- Unplugged status
- Custom bandwidth
- Polling intervals
- Custom properties
- Alerting Thresholds

For more information about interface dependencies, see Managing Dependencies.

Interface properties are configured as shown in the following procedure.

To configure interface properties:

1. Log in to the Orion Web Console as an administrator.
2. Open the appropriate Edit Interface page:
    a. Click **Settings** in the top right of the web console.
    b. Click **Manage Nodes** in the Node & Group Management grouping.
    c. Locate the parent node of the interface you want to manage, using either of the following methods:
        - Use the search tool above the node list to search your Orion database for the parent node of the interface you want to manage.
        - Select an appropriate **Group by:** criterion, and then click the appropriate group including the parent node of the interface you want to manage.
    d. Click **+** to expand the parent node, and then check the interface you want to manage.
    e. Click the **Edit Properties** button.

3. Make your changes:

Edit Interface Name

Edit the existing name in the appropriate field.

To display the interface as unplugged rather than down, select the **Display interface as unplugged...** box.

Notes:

- In interface names, aliases, or descriptions, use only the following recommended characters:

  a-z A-Z 0-9 space , . - _ ( ) /

- Do not use **\ | : * ? ' "**, or angle brackets (**<** or **>**). Angle brackets and any strings contained within angle brackets will be removed during polling, as bracketed text may be incorrectly parsed as web markup tags.

Designate Bandwidth for the Interface

To designate a custom bandwidth for the selected interface, check **Custom Bandwidth**, and then provide appropriate values for **Transmit** and **Receive Bandwidth**, in Mb/s.

Change Polling Interval

To change the current interface polling intervals, edit the existing values for **Interface Status Polling**, in seconds, and **Collect Statistics Every**, in minutes, as desired.

Notes:

- Interface status is determined using an SNMP request on the parent node that is queued on the interval designated in the Interface Status Polling field. The default interface status polling interval is 120 seconds.
- Interface statistics are also determined using SNMP polls of the parent node. The default statistics collection interval is 9 minutes.

Customize Alerting Thresholds for the Interface

You can customize thresholds whose reaching triggers alerts for individual interfaces. You can change alerting thresholds for the following metrics on the appropriate interface:

- Received /Transmit Interface Errors and Discards
- Receive/Transmit Interface Utilization

To customize a threshold, select **Override Orion General Thresholds** next to the appropriate metric, and provide new values for **Warning** and **Critical** Thresholds.

4. ***If you have finished editing interface properties,*** click **Submit**.

Deleting Devices from Monitoring

The following procedure deletes devices from the list of monitored nodes.

Warning: Deleting nodes from monitoring automatically stops monitoring of all applications, interfaces, and volumes on the deleted nodes. An individual event may be recorded for each deleted network object.

Note: You can select multiple devices to delete at the same time. Additionally, using the search tool above the node list, you can select multiple interfaces on different nodes for simultaneous deletion.

To delete devices from monitoring in 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.
3. Click **Manage Nodes** in the Node & Group Management grouping of the Orion Website Administration page.
4. ***To delete a node and all its applications, interfaces, and volumes from monitoring,*** complete the following steps.
    a. Locate the node to delete using either of the following methods:
        - Use the search tool above the node list to search your Orion database for the node you want to delete.
        - Select an appropriate **Group by:** criterion, and then click the appropriate group including the node to delete.
    b. Check the node to delete in the list, and then click **Delete** on the toolbar.
5. ***To delete a monitored application, interface, or volume,*** use the following steps.
    a. Locate the element to delete using either of the following methods:
        - Use the search above the node list to search your Orion database either for the object to delete or for its parent object to delete.
        - Select a **Group by:** criteria, and then click the appropriate group including the parent node of the object to delete.

b. Click **+** to expand the parent node of the object you want to delete.

c. Check the object to delete, and then click **Delete** on the toolbar.

6. Click **OK** to confirm deletion.

Promoting a Node from ICMP to SNMP Monitoring

After adding a node to the Orion database as an ICMP only node, you may need to promote the node to SNMP to start collecting additional statistics. The Node Management utility of the Orion Web Console can easily promote your node to SNMP without any loss of historical data.

To promote an ICMP only node to SNMP:

1. Click **Settings** in the top right of the web console, and then click **Manage Nodes** in the Node & Group Management grouping.
2. Select **Nodes** from the **Show** drop-down list, and locate the node to edit using either of the following methods:
   - Use the search tool above the node list to search your Orion database for either the object you want to edit or the parent node of the volume you want to edit.
   - Select an appropriate **Group by:** criterion, and then click the appropriate group including either the node to edit or the parent of the object to edit.
3. Check the node to edit and click **Edit Properties**:
4. Select **Most Devices: SNMP and ICMP** in the Polling Method section.
5. Select the version of SNMP to use. The default is **SNMPv2c**. However, **SNMPv1** is supported for older devices, and **SNMPv3** for device supporting enhanced security.
6. ***If you have installed multiple polling engines,*** select the **Polling Engine** you want to use to collect statistics from the added node.

   Note: This option is not displayed if you are only using one polling engine.

7. ***If the SNMP port on the added node is not the Orion default of 161,*** enter the actual port number in the **SNMPPort** field.

8. ***If the added node supports 64bit counters and you want to use them,*** check **Allow 64bit counters**.
   Note: Orion supports 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. **For SNMPv1 or SNMPv2c**, enter the **Community String** and, if required, the **Read/Write Community String**. Note: The Community String is a password to authenticate data sent between the management station and the device. The default is usually "public", otherwise use the strings provided with the device. Click **Test** to validate the string or strings entered here.
10. **For SNMPv3**, further credentials are required. See the documentation provided for your network device for further information.
11. Click **Test** to validate.
12. Click **Submit**.

Promoting a Node from ICMP to WMI Monitoring

After adding a node to the Orion database as an ICMP only node, you may need to promote the node to WMI to start collecting additional statistics. The Node Management utility of the Orion Web Console can easily promote your node to WMI without any loss of historical data.

Note: Once you promote a node from ICMP to WMI, you cannot go back to polling via ICMP.

To promote an ICMP only node to WMI:

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 Nodes** in the Node & Group Management grouping of the Orion Website Administration page.
3. Locate the device to promote using either of the following methods:
   - Use the search tool above the node list to search your Orion database for the node you want to promote.
   - Select an appropriate **Group by** criteria, and then click the appropriate group including the node to promote.
4. Click **Edit Properties**, and then select Windows Servers: WMI and ICMP.
5. Provide existing WMI credentials, or create new credentials.
6. ***If you want to verify your credentials,*** click **Test**.
7. ***If you want to change the default polling settings for your promoted node,*** edit the **Node Status Polling** or **Collect Statistics Every** values in the Polling area, as appropriate.

   Note: The **Node Status Polling** value refers to the period of time, in seconds, between the node status checks Orion performs on the promoted node. The **Collect Statistics Every** value refers to the period of time between updates Orion makes to displayed statistics for the promoted node.
8. ***If you have defined any custom properties for monitored nodes,*** provide appropriate values for the promoted node in the appropriate Custom Properties fields.
9. Click **Submit** when you have completed properties configuration for your

promoted node.

10. ***If you have successfully added the node,*** click **OK**.

Setting Device Management States

Monitored devices are regularly polled for operational status. Collected statistics are displayed in the Orion Web Console. Using the Node Management feature of the Orion Web Console, the management status of monitored nodes is easily set or changed, allowing you to either temporarily suspend data collection or resume polling and statistics collection, as necessary. The following procedure sets or changes management states for monitored nodes in the Orion Web Console.
Note: Setting a node to an unmanaged state automatically suspends the management of all interfaces and volumes on the selected node for the period entered.

To set or change the management state of a node:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Nodes** in the Node & Group Management grouping of the Orion Website Administration page.
3. Locate the node to manage using either of the following methods:
    - Use the search tool above the node list to search your Orion database for the device you want to manage.
    - Select an appropriate **Group by:** criteria, and then click the appropriate group including the node to manage.
4. Check the node to change, and then click **Unmanage** or **Remanage**, as appropriate, for the selected node.
5. ***If you have selected Unmanage,*** provide start and end times and dates for your management suspension, and click **OK**.

Setting Interface Management States

Monitored interfaces are regularly polled for operational status, and collected statistics are displayed in the Orion Web Console. Using the Node Management feature of the Orion Web Console, the management status of monitored interfaces is easily set or changed, allowing you to either designate an interface as "Unpluggable", temporarily suspend data collection, or resume polling and statistics collection, as necessary. The following procedure sets or changes management states for monitored interfaces in the Orion Web Console.

To set or change the management state of an interface:

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 & Group Management grouping of the Orion Website Administration page.
4. Locate the parent node of the interface to manage using either of the following methods:
    a. Use the search tool above the node list to search your Orion database for the interface you want to manage.
    b. Select an appropriate **Group by:** criterion, and then click the appropriate group including the parent node of the interface to manage.
5. Click **+** to expand the parent node of the interface you want to edit.
6. Check the interface you want to edit.
7. ***If you want to set the interface as Unmanaged,*** complete the following steps:
    a. Click **Unmanage**.
    b. Provide a date and time to start the device unmangement period.
    c. Provide a date and time to end the device unmangement period.
    d. Click **OK**.
8. ***If you want restart management of an interface that has been set to Unmanaged,*** click **Remanage**.

9. ***If you want to set the interface as Unpluggable ,*** complete the following steps:
    a. Click **Edit Properties**.
    b. Check **Display interface as unplugged rather than down**.
    c. Click **Submit**.

Remotely Managing Monitored Interfaces

Using the Node Management utility, you have the ability to shut down or enable interfaces, and override configured EnergyWise power settings remotely, as shown in the following procedure.

To remotely manage an interface:

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 Nodes** in the Node & Group Management grouping.
3. Locate the parent node of the interface you want to manage, using either of the following methods:
   - Use the search tool above the node list to search your Orion database for the parent node of the interface you want to manage.
   - Select an appropriate **Group by:** criterion, and then click the appropriate group including the parent node of the interface you want to manage.
4. Click **+** to expand the parent node, and then check the interface to manage.
5. ***If you want to shut down the selected interface,*** click **More Actions > Shut Down**, and then click **OK** to confirm.
6. ***If you want to enable the selected shutdown interface,*** click **More Actions > Enable**.
7. ***If the selected interface is EnergyWise-enabled and you want to override the current power level setting,*** click **More Actions > Override Power Level**, set the power level, as desired, and then click **OK**.

   Note: Remote overrides are temporary and will be reset in accordance with your configured EnergyWise policy for the selected interface. For more information about monitoring EnergyWise-enabled devices, see Monitoring EnergyWise Devices.

Unscheduled Device Polling and Rediscovery

Devices are polled for statistics and status regularly, according to the settings maintained in the Polling Settings view in the Orion Web Console. For more information, see Orion Polling Settings. Sometimes, however, it may be necessary to conduct an unscheduled poll or rediscovery of a monitored device, as shown in the following procedure.

To perform an unscheduled poll or rediscovery:

1. Log in to the Orion Web Console as an administrator, and then click **Settings** in the top right of the web console.
2. Click **Manage Nodes** in the Node & Group Management grouping.
3. Select Nodes or Interfaces from the **Show** drop-down list.
4. Locate and check the node or interface you want to poll or locate and check the node to rediscover, using either of the following methods:
   - Use the search tool above the node list to search your Orion database.
   - Select an appropriate **Group by:** criteria, and then click the appropriate group including either the node or interface you want to poll or the node you want to rediscover.
5. ***If you want to poll the selected node or interface,*** click **More Actions > Poll Now**.
6. ***If you want to rediscover the selected node,*** click **More Actions > Rediscover**.

Monitoring Windows Server Memory

When SolarWinds NPM polls a Windows server for CPU load and memory utilization, it pulls the amount of physical memory to define the 100% level, and then it totals the amount of memory in use by each allocation to compute what percentage of the physical memory is in use. This can result in memory utilization readings over 100%, as many applications pre-allocate memory and swap before it is actually needed.

To work around this, you can also add physical memory as a volume for these servers within SolarWinds NPM. When monitored as a volume, the values will be more in line with your expectations.

Changing the Polling Method for a Node

The following procedure details the steps required to change the polling method used to monitor a node in the Orion Web Console.

To change the polling method used to monitor a 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 & Group Management grouping of the Orion Website Administration page.
4. Check the node for which you want to change the polling method, and then click **Edit Properties**.
5. Select the appropriate **Polling Method**, as follows:
    - ***If you have added this node only to monitor an object on the node and not the node itself,*** select **No Status: External Node**.

      Note: No data is collected for external nodes.
    - ***If you only want to use ICMP to monitor the selected node,*** select **Status Only: ICMP**.

      Note: Select this option for limited data collection for nodes that support neither WMI nor SNMP. Only status, response time, and packet loss data are collected for ICMP-only nodes.
    - ***If the selected node is a Windows Server, and you only want to use WMI and ICMP for monitoring,*** select **Windows Servers: WMI and ICMP**, and then provide appropriate WMI credentials for the Windows Server you are adding.

      Note: Using WMI to monitor your added node may not provide as much data as you may be able to obtain using SNMP.

      If you are adding a node for typical monitoring, select Most Devices: SNMP and ICMP, and then provide the **SNMP Version** and **SNMP Port** fields, as appropriate.

      Note: If the SNMP port on the added node is not the Orion default of 161, provide the actual port number in the **SNMP Port** field.

6. ***If you are using SNMP to poll the selected node and you want to provide additional community strings,*** provide them in the **Community String** field.

   Notes:

   - For most SNMPv2c devices, the community string **public** gives Orion NPM sufficient access. If you are providing multiple community strings, separate them with spaces, as shown in the following example:

     Cstring1 Cstring2 Cstring3

   - Orion uses **SNMPv2c** by default. If the device you are adding supports or requires the enhanced security features of SNMPv3, select **SNMPv3**. If SNMPv2c is enabled on a device you want NPM to monitor, by default, NPM will attempt to use SNMPv2c to poll for performance information. If you only want NPM to poll using SNMPv1, you must disable SNMPv2c on the device to be polled.

7. ***If you have selected SNMPv3 as the SNMP version for the selected node and you want to provide additional read/write community strings,*** provide them in the **Read/Write Community String** field, as shown in the following example:

   RWCstring1 RWCstring2 RWCstring3

8. ***If you want to save the provided credentials as a credential set,*** provide a **Name**, and then click **Save**.
9. Click **Submit**.

Assigning Pollers to Monitored Devices

SolarWinds NPM provides both a selection of predefined pollers and the Universal Device Poller utility for defining your own pollers to monitor specific aspects of your network devices. In the Orion Web Console, the assignment of pollers to monitored devices is a straightforward process, as shown in the following steps.

Notes:

- If you do not see a poller that meets your specific monitoring needs, use the Universal Device Poller to create your own poller. For more information, see Monitoring MIBs with Universal Device Pollers.
- To manage pollers directly from the Manage Nodes page, click **Manage Pollers** in the top right of the page.

To assign a poller to a monitored device:

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 Nodes** in the Node & Group Management group.
3. Locate the node to poll, the interface to poll, or the parent node of the interface or volume to poll using either of the following methods:
    - Use the search tool above the node list to search your Orion database.
    - Select an appropriate **Group by:** criterion, and then click the appropriate group including either the node to poll or the parent node of the interface or volume to poll.
4. ***If you want to assign a poller to a node,*** complete the following steps:
    a. Check the monitored node to which you want to assign the poller, and then click **Assign Pollers** in the Node Management toolbar.
    b. Click **+** to expand the appropriate poller group.
    c. Check the pollers you want to assign, and then click **Submit**.
    d. Click **OK** to confirm the assignment.
5. ***If you want to assign a poller to an interface or volume,*** complete the following steps:

a. Click **+** next to the parent node of the interface or volume to which you want to assign the poller.
b. Check the interface or volume to which you want to assign the poller.
c. Click **Assign Pollers** in the Node Management toolbar.
d. Click **+** to expand the appropriate poller group, check the pollers you want to assign, and then click **Submit**.
e. Click **OK** to confirm the assignment.

Changing Polling Engine Assignments

If there are multiple Orion polling engines in your environment, node assignments may be changed directly from the Manage Nodes view. For more information, see Changing Polling Engine Node Assignments.

Scheduling a Node Maintenance Mode Time Period

When you need to perform maintenance on a node or its components, such as upgrading firmware, installing new software, or updating security, you may want to discontinue polling while the device is down for maintenance. Disabling polling, or setting a node status as Unmanaged, while performing node maintenance, maintains the accuracy of your data and prevents unnecessary alert messages.

Chapter 6: Monitored Device Types and Technologies

NPM provides interface-level performance data and additional insight into different device types and technologies.

This section provides more details about monitoring the following device types and technologies:

- Cisco EnergyWise-enabled devices. For more information related specifically to monitoring EnergyWise-enabled devices, see Monitoring EnergyWise Devices.
- Microsoft Hyper-V and VMware virtual servers and managers. For more specific information about monitoring virtual devices, see Monitoring Your Virtual Infrastructure.
- Fibre Channel (FC)
- Virtual Storage Area Networks (VSAN)
  For more information on monitoring FCs and VSANs, see Monitoring Fibre Channel Devices and VSANs.
- Cisco Unified Computing Systems (UCS)
- Wireless devices, including wireless clients, rogue access points, and wireless controllers. For more information related specifically to monitoring wireless devices, see Monitoring Wireless Networks.
- F5 BIG-IP Devices. For more information, see Monitoring F5 BIG-IP Devices.

Note: For more information about network device monitoring and management features available in SolarWinds NPM, see Monitoring Devices in the Web Console.

Monitoring F5 BIG-IP Devices

NPM now specifically supports performance monitoring for F5 BIG-IP devices and interfaces. NPM monitoring for F5 devices and interfaces includes device status and availability, CPU and memory performance statistics, interface performance details, and related graphs and charts.

Notes:

- F5 node, interface and status reporting is supported for F5 firmware versions 11.2 and higher.
- NPM uses existing interface resources to provide F5 interface statistics.

The following resources are available in SolarWinds NPM installations:

- F5 Connections
- F5 CPU
- F5 Device Details
- F5 List of Virtual Servers
- F5 List of Nodes
- F5 List of Pools
- F5 Memory
- F5 Throughputs

F5 Connections

The following table summarizes the data available in the F5 Connections resource:

Note: All data is polled from F5-BIGIP-SYSTEM-MIB

Data Type	Object Name OID
Connections Current	sysGlobalStat:sysStatClientCurConns 1.3.6.1.4.1.3375.2.1.1.2.1.8

Data Type	Object Name OID
Connections SSL	sysGlobalClientSslStat:sysClientsslStatCurNativeConns
	1.3.6.1.4.1.3375.2.1.1.2.9.4
Connections SSL Current	sysGlobalClientSslStat:sysClientsslStatCurCompatConns
	1.3.6.1.4.1.3375.2.1.1.2.9.7
Connections Total	sysGlobalStat:sysStatClientTotConns
	1.3.6.1.4.1.3375.2.1.1.2.1.7

F5 CPU

The following table summarizes the data available in the F5 CPU resource:

Note: All data is polled from F5-BIGIP-SYSTEM-MIB

Data Type	Object Name OID
Idle Cycles	sysStatTmIdleCycles
	1.3.6.1.4.1.3375.2.1.1.2.1.42.0
Sleep Cycles	sysStatTmSleepCycles
	1.3.6.1.4.1.3375.2.1.1.2.1.43.0
Total Cycles	sysStatTmTotalCycles
	1.3.6.1.4.1.3375.2.1.1.2.1.41.0

F5 Device Details

The following table summarizes the data available in the F5 Device Details resource:

Note: All data is polled from F5-BIGIP-SYSTEM-MIB

Data Type	Object Name OID
Product Name	sysProductName 1.3.6.1.4.1.3375.2.1.4.1
Product Version	sysProductVersion 1.3.6.1.4.1.3375.2.1.4.2
Product Build	sysProductBuild 1.3.6.1.4.1.3375.2.1.4.3
Product Edition	sysProductEdition 1.3.6.1.4.1.3375.2.1.4.4
Product Serial Number	sysGeneralChassisSerialNum 1.3.6.1.4.1.3375.2.1.3.3.3
Sync Status	sysCmSyncStatusId 1.3.6.1.4.1.3375.2.1.14.1.1
Failover Status	sysCmFailoverStatusId 1.3.6.1.4.1.3375.2.1.14.3.1

F5 List of Virtual Servers

The following table summarizes the data available in the F5 List of Virtual Servers resource:

Note: All data is polled from F5-BIGIP-LOCAL-MIB

Data Type	Object Name OID
Name	ltmVirtualServTable:ltmVirtualServName
	1.3.6.1.4.1.3375.2.2.10.1.2.1.1
Address Type	ltmVirtualServTable:ltmVirtualServAddrType
	1.3.6.1.4.1.3375.2.2.10.1.2.1.2
IP Address	ltmVirtualServTable:ltmVirtualServAddr
	1.3.6.1.4.1.3375.2.2.10.1.2.1.3
Port	ltmVirtualServTable:ltmVirtualServPort
	1.3.6.1.4.1.3375.2.2.10.1.2.1.6
Enabled State	ltmVsStatusTable:ltmVsStatusEnabledState
	1.3.6.1.4.1.3375.2.2.10.13.2.1.3
Availability State	ltmVsStatusTable:ltmVsStatusAvailState
	1.3.6.1.4.1.3375.2.2.10.13.2.1.2

F5 List of Nodes

The following table summarizes the data available in the F5 List of Nodes resource:

Note: All data is polled from F5-BIGIP-LOCAL-MIB

Data Type	Object Name OID
Name	ltmNodeAddrTable:ltmNodeAddrName (for BIG-IP SW Ver 11.2+)
	1.3.6.1.4.1.3375.2.2.4.1.2.1.17

Data Type	Object Name OID
Address Type	ltmNodeAddrTable:ltmNodeAddrAddrType 1.3.6.1.4.1.3375.2.2.4.1.2.1.1
IP Address	ltmNodeAddrTable:ltmNodeAddrAddr 1.3.6.1.4.1.3375.2.2.4.1.2.1.2
Enabled State	ltmNodeAddrStatusTable:ltmNodeAddrStatusEnabledState 1.3.6.1.4.1.3375.2.2.4.3.2.1.4
Availability State	ltmNodeAddrStatusTable:ltmNodeAddrStatusAvailState 1.3.6.1.4.1.3375.2.2.4.3.2.1.3

F5 List of Pools

The following table summarizes the data available in the F5 List of Pools resource:

Note: All data is polled from F5-BIGIP-LOCAL-MIB

Data Type	Object Name OID
Name	ltmPoolTable:ltmPoolName 1.3.6.1.4.1.3375.2.2.5.1.2.1.1
Mode	ltmPoolLbMode 1.3.6.1.4.1.3375.2.2.5.1.2.1.2
Enabled State	ltmPoolStatusTable:ltmPoolStatusEnabledState 1.3.6.1.4.1.3375.2.2.5.5.2.1.3

Data Type	Object Name OID
Availability State	ltmPoolStatusTable:ltmPoolStatusAvailState 1.3.6.1.4.1.3375.2.2.5.5.2.1.2

F5 Memory

The following table summarizes the data available in the F5 Memory resource:

Note: All data is polled from F5-BIGIP-SYSTEM-MIB.

Data Type	Object Name OID
Total Memory	sysStatMemoryTotal 1.3.6.1.4.1.3375.2.1.1.2.1.44.0
Used Memory	sysStatMemoryUsed 1.3.6.1.4.1.3375.2.1.1.2.1.45.0

F5 Throughputs

The following table summarizes the data available in the F5 List of Pools resource:

Note: All data is polled from F5-BIGIP-SYSTEM-MIB.

Data Type	Object Name OID
Client Bytes In	sysGlobalStat:sysStatClientBytesIn 1.3.6.1.4.1.3375.2.1.1.2.1.3

Data Type	Object Name OID
Client Bytes Out	sysGlobalStat:sysStatClientBytesOut
	1.3.6.1.4.1.3375.2.1.1.2.1.5
Server Bytes In	sysGlobalStat:sysStatServerBytesIn
	1.3.6.1.4.1.3375.2.1.1.2.1.10
Server Bytes Out	sysGlobalStat:sysStatServerBytesOut
	1.3.6.1.4.1.3375.2.1.1.2.1.12

Monitoring Fibre Channel Devices and VSANs

NPM specifically recognizes VSANs and Fibre Channel devices on your network when they are added to the Orion database as network objects for monitoring.

In addition to the Fibre Channel Units and Ports report that is predefined in all NPM installations, NPM offers the following VSAN- and Fibre Channel-related web console views and resources:

VSAN Views

NPM offers the following VSAN-related views in the Orion Web Console:
Note: For more information about web console views, see Customizing Views.

VSAN Details

Each VSAN is monitored as its own network object, with its own VSAN Details view. The VSAN Details view is preconfigured with the following resources:

VSAN Details Resources	
All VSAN Members	Provides an overview of all monitored devices in a selected VSAN, including interface port assignments and status.
VSAN Details	Provides information about the selected VSAN, itself, including status, name, ID media type, and load balancing type.
Event Summary	A summary of recent defined Orion events on the selected VSAN. Events are listed by VSAN member.
Total Bytes Transferred	A chart presenting total bytes both transferred and received on the selected VSAN over a customizable time period.
In/Out Errors and Discards	A chart presenting all receive and transmit errors and discards on the selected VSAN over a customizable time period.
VSAN Traffic	A chart reporting average traffic on the selected VSAN over a customizable time period.

VSAN Summary

The VSAN Summary view is preconfigured with the following resources:

VSAN Details Resources	
All VSAN Nodes	Provides a list of all VSANs currently monitored by NPM, where each monitored VSAN is treated as a single node.
Fibre Channel Reports	A customizable resource providing a link to the predefined Fibre Channel Units and Ports report. Additional reports may be added to the list as they are defined.
Last 25 Events	A list of the last 25 Orion events related to monitored VSANs.
VSAN Traffic	A chart reporting average traffic on all monitored VSANs over a customizable time period

Monitoring EnergyWise Devices

SolarWinds has partnered with Cisco to present EnergyWise to optimize energy usage on your network. EnergyWise technology enables you to configure energy usage policies for EnergyWise-enabled and power-over-Ethernet (PoE) devices.

What is EnergyWise?

EnergyWise is a Cisco technology developed to help you cut enterprise energy costs, address environmental concerns, and adhere to government directives around green technologies. By deploying EnergyWise capable devices and by enabling their energy-saving features, you can run business-critical systems in a fully powered state while allowing less critical devices on Power over Ethernet (PoE) ports to power down or drop into standby during off-peak hours.

EnergyWise Terminology

The following terms and concepts are provided in the EnergyWise MIB and used within EnergyWise resources in the Orion Web Console.

Domain

The EnergyWise MIB includes a field for labeling groups of EnergyWise capable devices, or entities, as members of a designated domain. With respect to NPM, a single domain consists of all monitored EnergyWise entities defined as neighbors

Entity

Any network device, including switches, IP phones, and other components connected to Power over Ethernet (PoE) ports on EnergyWise capable devices, that either draws power from another network device or supplies power to another network device.

Importance Level

The Importance Level, or, simply, the Importance, is a priority value ranging from 1 to 100 that is assigned to both EnergyWise entities and EnergyWise policies. The higher the value, the more important the device and the less likely it is to be changed by energy policy modifications. When a policy application is attempted, the importance levels of the policy and the selected entity are compared to determine whether or not the policy is actually applied to the selected entity. If the policy importance level is greater than or equal to the entity importance level, the policy is applied to the entity and the entity power level is changed. Likewise, as long as the importance level of an entity to which policy applications are attempted is greater than the importance levels of the policies applied, the entity power level will remain unchanged.

For example, an IP phone assigned an importance level of 80 is operating at a power level of 8. Policy A5, to change entity power levels to 5, has an importance of 50, and Policy B10, to change entity power levels to 10, has an importance of 95. If Policy A5 is applied to the phone, the phone will continue to operate at power level 8. However, if Policy B10 is applied to the phone, the phone power level changes to 10 in keeping with applied Policy B.

The importance value may be used to exempt specific entities from policy changes. For example, if all your emergency phones are on a single switch, the switch should never go into standby mode. To ensure that the switch hosting your emergency phones never goes into standby mode, set the switch importance to 100 so all policies with an importance of 99 and lower will have no effect on the emergency phone switch.

Keywords

The EnergyWise MIB provides for the identification of individual entities with unique labels. When an entity is initially configured, keywords may be added in series, as a string of words separated by commas without spaces, as shown in the following example:

Keyword1,Keyword2,Keyword3

Name

A user-friendly identifier for an EnergyWise entity or domain that may be assigned in the EnergyWise MIB when the entity or domain is configured. The default name for a switch is the hostname, and the default name for a Power over Ethernet (PoE) port is a shortened version of the port name. EnergyWise name values cannot include spaces. Modifying the EnergyWise name does not change the hostname of the device or the port name on the device. Omit spaces and refrain from using asterisks (*) in your name designations. Valid characters include alphanumeric characters and symbols, including **#**, **(**, **%**, **!**, or **&**.

Neighbor

Any two EnergyWise entities defined within the same domain are neighbors. Neighbors are capable of communicating EnergyWise events including the issuance of energy management directives.

Policy Level

The Policy Level is the power level of the policy that is currently applied to the selected entity.

Power Level

The Power Level is a designation of the amount of power an EnergyWise entity is allowed to draw, based on the policies currently acting upon it. The following table details available levels with category labels and icon colors.

Notes:

- In some web console resources, the Power Level may be designated as either the EnergyWise Level or the EW Level.
- A known issue exists in some Cisco IOS versions where power levels are reported as **1-11** and not as **0-10**. Beginning with SolarWinds NPM version 10.1.2, power levels are automatically corrected within SolarWinds NPM. SolarWinds NPM also properly handles this issue in the event that the IOS on a monitored device is not affected by this known issue.

Level	Label	Category	Color	Color Code
10	Full	Operational (1)	Red	FF0000
9	High			
8	Reduced		Yellow	FFFF00
7	Medium			
6	Frugal		Green	00FF00
5	Low			
4	Ready	Standby (0)	Blue	0000FF
3	Standby			
2	Sleep		Brown	A52A2A
1	Hibernate			
0	Shut	Nonoperational (-1)	Black	000000

Monitoring EnergyWise Devices with NPM

NPM provides the EnergyWise Summary view and related EnergyWise resources to help you monitor the energy expended on your network and the energy savings provided by EnergyWise-enabled devices. The following sections describe the EnergyWise Summary view and related EnergyWise resources.

Notes:

- Fully upgrade the IOS of all EnergyWise-enabled devices on your network. For more information, consult your device documentation or www.cisco.com.
- If the EnergyWise Summary view does not display in the Orion Web Console menu bar, see Adding the EnergyWise Summary View.

EnergyWise Summary View and Resources

By default, the EnergyWise Summary view provides the following resources:

All Nodes

The All Nodes resource included on the EnergyWise Summary view is configured to display your entire network in terms of EnergyWise capability. All nodes on your network are included in one of the following groups:

- The **EnergyWise Capable** group includes all monitored devices on which the EnergyWise technology is available but not yet enabled.
- The **EnergyWise Enabled** group includes all monitored devices on which the EnergyWise technology is both available and enabled.
- The **Not EnergyWise Capable** group includes all monitored devices that do not feature the EnergyWise technology.

EnergyWise NCM Information

Network Configuration Manager (NCM) is the Orion module used for network configuration and change management. This resource provides some basic information about how Orion NCM can be used to manage EnergyWise settings and policies on your network. For more information about Orion NCM, including the option to download a free trial, click **Download NCM**.

EnergyWise Reports

The EnergyWise Reports resource provides a list of reports detailing current EnergyWise readiness and energy savings across your network.

Overall EnergyWise Savings

The Overall EnergyWise Savings resource provides a chart displaying the difference between the maximum amount of power that can be consumed and the actual amount of power that is consumed by all EnergyWise-enabled devices on your network as a percentage of the maximum amount of power that can be consumed.

Notes:

- Graphed **bars represent average savings over the designated interval.**
- Maximum and actual power consumption may be equivalent if you have not yet enabled an EnergyWise management policy on your network.

Overall Historical Power Consumption

The Overall Historical Power Consumption resource displays a chart of both the actual and the maximum amount of power consumed by all EnergyWise entities on your network.

Note: Maximum and actual power consumption may be equivalent if you have not yet enabled an EnergyWise management policy on your network.

Additional EnergyWise Resources

In addition to the resources provided by default on the EnergyWise Summary view, SolarWinds NPM provides the following EnergyWise resources for inclusion on other Orion Web Console views, as indicated.

Note: For more information about the EnergyWise Summary view and its resources, see EnergyWise Summary View and Resources.

Device Power Consumption

The Device Power Consumption resource displays a chart of both the actual and the maximum power consumed by a selected EnergyWise entity.

Note: Maximum and actual power consumption may be equivalent if you have not yet enabled an EnergyWise policy on the selected entity.

EnergyWise Interface Details

This resource provides both information about the selected interface entity and the ability to immediately set the current Power Level of the selected interface entity. For more information about setting the current Power Level, see Managing EnergyWise Interface Entity Power Levels.

The EnergyWise Interface Details resource provides the following information about the selected interface entity:

- The Name listing provides the user-friendly EnergyWise entity name that has been defined for the viewed interface entity.
- The Power Level listing provides the colored icon and label associated with the power level currently reported by the viewed interface entity.

  Note: The Power Level may be temporarily reset by clicking **Set Power Level** in this resource. For more information, see Managing EnergyWise Interface Entity Power Levels.

- The Policy Level listing provides the colored icon and label indicating the power level of the policy currently applied to the viewed interface entity.

  Notes:

  - The Policy Level is the same Power Level that is reported in the EnergyWise Policy Overview Calendar for the currently viewed interface entity at the current local time of the viewed interface entity.
  - Policies are set either on the monitored device or with a configuration management utility like Orion Network Configuration Manager. For more information about Orion NCM, see www.solarwinds.com.

- The Keywords listing provides any keywords that have been defined for the viewed interface entity.

EnergyWise Node Details

The EnergyWise Node Details resource provides the following information about the selected node entity:

- The Domain Name listing provides the user-friendly name of the EnergyWise domain that has been defined for the viewed node entity.
- The Maximum Importance field indicates the importance level assigned to the viewed node.
- The Number of Neighbors field indicates the number of other currently monitored EnergyWise entities that are capable of communicating EnergyWise directives to the viewed node entity.
- The Status field communicates whether or not EnergyWise power management is currently enabled on the viewed node entity.

EnergyWise Policy Overview Calendar

The EnergyWise Policy Overview Calendar resource provides a visual record of policy- or configuration-based power level assignments for the viewed entity. EnergyWise recurrence policies assign power levels on an hourly basis, and this resource reports the assigned power levels, by the hour, for the viewed entity over a selected week.

Notes:

- All time references are in terms of the viewed entity and are not necessarily the time of the SolarWinds NPM server.
- Policies are configured either on the monitored device itself or with a configuration management utility like Orion Network Configuration Manager (Orion NCM). For more information about Orion NCM, see www.solarwinds.com.

Entity Power Consumption

The Entity Power Consumption resource provides a chart displaying both the maximum amount of power that can be consumed and the actual amount of power that is consumed by the viewed EnergyWise-enabled entity.

Note: Maximum and actual power consumption may be equivalent if you have not yet enabled an EnergyWise policy on the selected device.

Adding the EnergyWise Summary View

The following procedure adds the EnergyWise Summary View to the Orion Web Console Views menu bar.

To add the EnergyWise Summary view to the web console Views menu bar:

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 **Customize Menu Bars** in the Customize grouping of the Orion Website Administration page.
3. Click **Edit** beneath the web console menu bar to which you want to add a link to the EnergyWise Summary view.
4. Click and drag the **EnergyWise** button from the Available items list on the left to the correct relative location in the Selected items list on the right.

Note: Selected items display from left to right in the selected menu bar as they are listed from top to bottom.

5. Click **Submit**.

Managing EnergyWise Interface Entity Power Levels

Although entity power levels are typically set using recurrence policies enacted by a configuration management utility like SolarWinds Network Configuration Manager (SolarWinds NCM), with SolarWinds NPM you can temporarily change the current power level of a selected EnergyWise interface entity from either the Interface Details view for the selected EnergyWise interface entity the Web Console Node Management utility.

In either case, the following procedure provides the steps required to temporarily change the currently active power level of an EnergyWise interface entity.

Notes:

- Any change made to the power level of a monitored EnergyWise entity is only effective until the next scheduled application of a defined recurrence policy. Policies are configured either manually on the monitored device itself or with a configuration management utility like SolarWinds NCM. For more information about SolarWinds NCM, see www.solarwinds.com.
- A known issue exists in some Cisco IOS versions where EnergyWise levels are reported as values **1-11** and not as values **0-10**. Beginning with SolarWinds NPM 10.1.2, reported levels are automatically corrected within SolarWinds NPM. SolarWinds NPM also properly handles this issue in the event that the IOS on a monitored device is not affected by this known issue.

To reset the current power level of a monitored EnergyWise entity:

1. Log in to the Orion Web Console using an account with node management or administrator privileges.
2. ***If you want to set the entity power level from the Interface Details view,*** click **Set Power Level** in the EnergyWise Interface Details resource.
3. ***If you want to use the Web Console Node Management utility,*** complete the following steps:

    a. Click **Home** in the Views toolbar, and then click **Manage Nodes** in the All Nodes resource.

b. Locate the device to edit using either of the following methods:
   - Use the search tool above the node list to search your database for the parent node of the EnergyWise interface entity you want to reset.
   - Select an appropriate **Group by:** criterion, and then click the appropriate group including the parent node of the EnergyWise interface entity you want to reset.

c. Click **+** to expand the parent node of the EnergyWise interface entity you want to reset, and then check the interface entity.

d. Click **More Actions > Override Power Level**.

4. Select the appropriate power level, and then click **OK**.

Monitoring Wireless Networks

NPM can monitor any 802.11 IEEE-compliant autonomous access point (AP) or wireless controller. Details about your access points (AP), wireless clients, wireless controllers, thin APs, and rogue APs can all be monitored using NPM. Wireless device monitoring is configured, customized, and managed using the Orion Web Console, as shown in the following sections.

Getting Started

Orion Network Performance Monitor automatically recognizes your wireless APs and controllers as wireless devices after they have already been added to the Orion database. For more information on adding devices to Orion, see Discovering and Adding Network Devices.

The wireless interfaces are not found during discovery process. Instead, after the wireless device is added to Orion and an inventory search is performed, each wireless interface found is added to the database and polling begins.

Migrating Data from the Wireless Networks Module

If you have already used an older version of the Wireless Network module to poll your wireless devices, SolarWinds NPM will automatically migrate your historical data to the new format used since SolarWinds NPM version 9.5.

Notes:

- The wireless migration will not be performed during installation or configuration. The migration is performed in batches during scheduled database maintenance. For more information, see Database Maintenance.
- The migration will notify users when a given node is migrated and when all nodes have been migrated in the Orion event log.
- You will not see historical data immediately because this process is throttled.

Viewing Wireless Data

The Wireless Summary view in the Web Console displays a list of all wireless access points (APs) and clients connected to each AP. Access point details include IP address, device type, SSID, channels used, and the number of clients currently connected. Client details include client name, SSID, IP Address, MAC Address, Received Signal Strength Indication (RSSI), time connected, data rate, bytes received and bytes transmitted.

Notes:

- The following wireless connections are not currently monitored IPv6 statistics:
  - between wireless users and access points
  - between thin access points and controllers
- The wireless details views uses device-specific node details views to display statistics. For more information, see Views by Device Type.

To view wireless access points and clients:

1. Log in to the Orion Web Console as an administrator.
2. Click **Wireless** in the Views toolbar.
3. ***If you want to view access points,*** select **Access Points** from the **Show** list.
4. ***If you want to view clients,*** select **Clients** from the **Show** list.
5. ***If you want to filter the view using groups,*** select a method to group access points or clients from the **Group by:** list.
6. ***If an access point has clients currently connected,*** expand the access point name to show the list of clients connected.
7. ***If you want to search for access points or clients,*** type your search string in the **Search** field, and then click **Search**.

Clicking any access point opens the Node Details view for the selected access point.

Removing a Wireless Device

Removing wireless devices is performed the same way as removing any node from an Orion product. For more information, see Deleting Devices from Monitoring.

Chapter 7: Monitoring Your Virtual Infrastructure

SolarWinds Orion Integrated Virtual Infrastructure Monitoring (IVIM) built into SolarWinds NPM lets you monitor today's modern network fabric of virtual networks, virtualized data centers, and private clouds. The deep visibility into your virtualized environments helps you ensure that network performance helps and not hinders your virtualization projects.

SolarWinds IVIM is capable of monitoring Microsoft Hyper-V and VMware ESXi and ESX Servers versions 4.1 and higher.

For more information about requirements, see Minimum Requirements in the SolarWinds Virtual Manager documentation.

SolarWinds IVIM features available from the Orion Web Console:

VMware Monitoring

Monitor your entire VMware virtual infrastructure from the highest to the lowest level: vCenter → datacenter → cluster → ESX hosts → individual virtual machines. Track availability and performance metrics including CPU, memory, storage, and network bandwidth utilization.

Virtual Machine Auto-Summary

Automatically discover identify and monitor new virtual machines added to any VMware host server or updated during vMotion.

Virtualization Alerting and Reporting

SolarWinds Orion's native alerting and reporting capabilities extend seamlessly to your virtual infrastructure.

For more extensive virtualization monitoring, integrate SolarWinds NPM with SolarWinds Virtualization Manager. For more information, see Virtualization Manager at www.solarwinds.com.

The following sections provide instructions and details for using SolarWinds IVIM in the Orion Web Console:

- Requirements for Monitoring ESXi and ESX Servers
- Managing VMware Credentials in the Web Console
- Adding VMware Servers for Monitoring
- Virtualization Summary
- Viewing ESX Host Details
- Configuring virtualization polling settings

For more information about SolarWinds IVIM integrated within the Orion Web Console, see Using the SolarWinds IVIM in the SolarWinds Virtualization Manager documentation.

Requirements for Monitoring ESXi and ESX Servers

The following table provides minimal requirements for effectively using SolarWinds NPM to monitor your VMware ESXi and ESX Servers.

Note: For more information about requirements, see Minimum Requirements in the SolarWinds Virtual Manager documentation.

Requirement	Description
SNMP	SolarWinds NPM uses SNMP to monitor all ESXi and ESX Servers. For more information about enabling SNMP, consult your ESX or ESXi server vendor documentation.
VMware API	VMware API polls most performance data from devices running ESXi and ESX Server versions 4.1 or newer. For more information about creating required credentials, see Creating ESX Server Credentials for SolarWinds NPM.
VMware Tools	VMware Tools must be installed on all virtual machines you intend to monitor. VMware Tools are not required on virtual machines running on monitored ESXi and ESX servers. However, installing VMware Tools on virtual machines hosted by monitored ESXi and ESX Servers allows you to access additional information, such as IP addresses.

The following table provides a summary of the methods used by SolarWinds NPM to monitor VMware ESX Servers and their component features.

Features	4	4i	5i
Datacenter	VMware API		
ESX Cluster	VMware API		
Virtual Center	VMware API		
Detection as ESX Server	VMware API		
Volumes	SNMP	N/A	SNMP

Features	4	4i	5i
Interfaces	SNMP	SNMP (partial)	SNMP
CPU	VMware API		
Memory	VMware API		
Total CPU (ESX Details view)	VMware API		
Total Memory (ESX Details view)	VMware API		
Network Traffic Utilization (ESX Details view)	VMware API		
Guest VM List (ESX Details view)	VMware API		

Creating ESX Server Credentials for SolarWinds NPM

SolarWinds NPM uses the VMware API to poll most of its performance data from devices running ESX Server versions 4.1 or newer. You must create credentials on your ESX Servers for the SolarWinds NPM polling engine.

To create the credentials, log on to the ESX server and create a new user.

Note: Credentials created for the NPM polling engine must have read-only rights as a minimum.

For more information about creating ESX Server credentials, consult your vendor documentation.

Managing VMware Credentials in the Web Console

If you have to update the user name or password of a VMware credential, you can do so from the VMware Credentials Library tab.

To update a VMware credential:

1. Log in to the web console.
2. Click **Settings**.
3. Click **Manage Virtual Devices** in the Node & Group Management section.
4. Click the **VMware Credentials Library** tab.
5. Check the credential you need to update, and then click **Edit Credential**.
6. Make the necessary updates, and then click **OK**.

Adding VMware Servers for Monitoring

VMware Vcenter, ESX servers, and virtual machines are added to the Orion database in the same ways other devices are added for monitoring in the Orion Web Console.

Polling for VMware Nodes Using the Network Sonar Wizard

The Network Sonar Wizard is the recommended method for adding VM Servers for monitoring in the Orion Web Console. With Network Sonar Discovery, you can define all required credentials at once on the Local ESX Credentials for VMware view. For more information, see Network Discovery Using the Network Sonar Wizard.

Note: When configuring Network Sonar Discovery, confirm that you check **Poll for VMware** on the VMware page of the Network Sonar Wizard. Nodes cannot be identified as VMware devices unless **Poll for VMware** is enabled.

To add VMs from the VMware Assets resource:

1. Log in to the Orion Web Console.
2. Click **Home > Virtualization**.
3. Click the **[+]** next to any ESX or Vcenter server listed in the **Virtualization Assets** resource to expand the list of virtual machines.

4. Click a virtual machine that is not currently managed by SolarWinds Orion. Unmanaged VMs are listed in italic type.
5. Click **Yes, Manage this Node**.
6. ***If the VM is not running VMware Tools***, manually enter the IP address of the VM in the **Hostname or IP Address** field.
7. Check additional options required to monitor the VM, and then click **Next**.
8. Follow the remainder of the Add Node wizard to completion, and then click **OK, Add Node**.

Virtualization Summary

The Virtualization Summary view shows the overall status of your virtualized infrastructure.

To view the Virtualization Summary:

1. Log in to the Orion Web Console.
2. Click **Home > Virtualization**.

The Virtualization Summary view is pre-configured to display relevant resources. It consists of three subviews:

- Summary
- VMware
- Hyper-V

Each subview contains the following resources, and displays information about your whole virtual infrastructure, about VMware or Hyper-V only, as indicated by the subview name.

Virtualization Assets	Top 10 Hosts by Percent Memory Used
Virtualization Assets Summary	Top 10 Hosts by Network Utilization
VMware vCenters with Problems	Top Hosts by CPU Load
Virtual Clusters with Problems	Top 10 Hosts by Number of Running VM's

Hosts with Problems	
Guests with Problems	

To change any resource properties or contents, click **Edit** in the resource box.

For more information about virtualization icons used in the resources, see "Understanding Object Statuses" in the SolarWinds Virtual Manager documentation.

Viewing ESX Host Details

The ESX Host Details page opens when you click an ESX Host server in the Virtualization Summary.

This page displays the following resources, by default:

Average Response Time & Packet Loss Graph	AppStack Environment
Virtualization Assets	List of Virtual Machines
CPU Load & Memory Utilization Gauge	Average Response Time & Packet Loss
ESX Host Details	Min/Max Average CPU Load
Management	Top CPU's by Percent Load
Node Details	Disk Volumes
Event Summary	Active Alerts on This Node
Polling Details	Virtual Machine Memory Consumption
Availability Statistics	Virtual Machine Network Traffic
Virtual Machine CPU Consumption	
Guests with Problems	

Custom properties for Nodes	

For more information about virtualization icons used in the resources, see "Understanding Object Statuses" in the SolarWinds Virtual Manager documentation.

To change any resource properties or contents, click **Edit** in the resource box.

Configuring virtualization polling settings

Virtualization polling is performed through the following credentials, based on the server vendor.

- Hyper-V nodes are accessed with Windows credentials.
- VMware vCenter servers are accessed with local vCenter credentials.
- VMware ESX servers are accessed with local ESX credentials.

Assigning credentials to Hyper-V servers

To assign credentials to Hyper-V servers, perform the following steps:

1. On the Virtualization Polling Settings page, select Hyper-V.
2. Select a Hyper-V server from the list, and then click **Edit Properties**.
3. Under **Polling Method > Windows Servers**, choose a credential from the list, or select **New Credential** from the list, and then specify a new credential set.
4. Click **Test** to verify the credential set, and then click **Submit** at the bottom of the page.

Assigning credentials to VMware servers

To assign credentials to VMware servers, perform the following steps:

1. On the Virtualization Polling Settings page, select VMware.
2. Select a VMware server from the list, and then click **Assign ESX Credential**.
3. Choose an existing credential from the list, or specify a new credential set.
4. Click **Test** to verify the credential set, and then click **Assign Credential** to assign it to the VMware server.

Chapter 8: Monitoring Hardware Health

Monitoring hardware health allows you to get immediate insight into hardware issues on your network. If you are monitoring selected Cisco, Dell, F5, HP, and Juniper devices, hardware health can tell you which of these devices are in Up, Warning, Critical, or Unknown states.

SolarWinds NPM monitors hardware health by polling appropriate hardware health statistics from a MIB tree on your devices. For Cisco devices, you can change the currently used MIB. For more information, see Changing MIB Used for Polling Hardware Health Statistics.

Hardware monitoring is achieved by polling via SNMP. To poll the data, the hardware health poller must be enabled. For more information, see Enabling and Disabling or Adjusting Hardware Health Monitors for Individual Nodes.

Monitored Hardware Sensors

Sensor	Up	Warning	Critical	Unknown
Fan status				
Power Supply status				
Temperature				

Enabling Hardware Health Monitoring

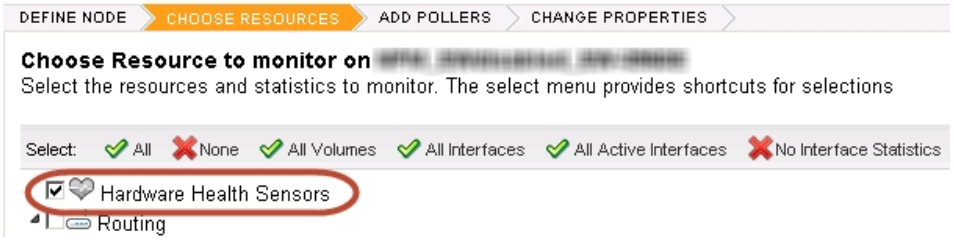
If you add nodes using the Network Sonar Discovery, the hardware health sensors are automatically enabled for devices that support hardware health monitoring. For more information, see Network Discovery Using the Network Sonar Wizard.

When adding individual nodes with the Add Node wizard, you can enable or disable hardware health monitoring in the wizard.

You can always check whether hardware health statistics are being collected on the Node Details view for the appropriate device. The Node Details view allows you to enable or disable hardware health monitoring, as appropriate.

Add Node Wizard

From the Add Node wizard, the option to display Hardware Health of Servers is available after a node has been defined. Check this box to enable hardware health monitoring.



Enabling or Disabling Hardware Health Monitoring for Individual Nodes

You can always enable or disable hardware health monitoring for individual nodes.

To enable hardware monitoring:

1. Click the Home tab in the Orion Web Console.
2. In the **All Nodes** group, click the node you want to monitor.
3. In the **Node Details** group of the Node Details view, click the **List Resources** button.
4. Make sure the **Hardware Health Sensors** box is selected and click **Submit**.

To disable hardware monitoring for a node:

1. Navigate back to the List Resources screen for the node (see steps 1-3)
2. Clear the **Hardware Health Sensors**, then click **Submit**.

Enabling and Disabling or Adjusting Hardware Health Monitors for Individual Nodes

Manage Hardware Sensors page lists all currently monitored sensors. By default, all sensors available in the selected MIB are monitored on devices for which you selected that you want to monitor hardware health sensors when adding them into the Orion database.

You can enable or disable individual sensor, or change thresholds for displaying hardware health status. For more information about changing thresholds, see Editing Thresholds for Hardware Health.

Updates Visible After the Next Poll

All changes will be applied in the Orion Web Console with the next poll. To find out the current polling interval, go to Settings > Polling Settings in the Thresholds and Polling grouping, and note the Default Interface Statistics Poll Interval.

You can also update the hardware health resources for a node manually. To do so, go to the appropriate node details view, go to the appropriate node view, and click **Poll Now** in the Management resource.

Enabling Hardware Sensors

Hardware health information is collected only for nodes where appropriate hardware sensors are enabled.

To enable hardware monitoring for a device:

1. Go to **Manage Hardware Sensors** view (Settings > Node & Group Management > Manage Hardware Sensors).
2. Find the sensor(s) you want to manage. You can either use the **Group by** pane, or use the **Search** box.

   Tip: To find all sensors available on a node, select Node in the **Group by** list, and then select the appropriate node.

3. Select the sensor which you want to enable and click **Enable**.

Disabling Hardware Sensors

If you do not want to collect hardware health information for a sensor, or for all sensors on a node, disable them.

To disable sensors:

1. Go to **Manage Hardware Sensors** view (Settings > Node & Group Management > Manage Hardware Sensors).
2. Find the sensor(s) you want to manage. You can either use the **Group by** pane, or use the **Search** box.

   Tip: To find all sensors available on a node, select Node in the **Group by** list, and then select the appropriate node.

3. Select the sensor(s) which you want to enable and click **Disable**.

Editing Thresholds for Hardware Health

The hardware states displayed in the Orion Web Console change based on thresholds set for the sensors. You can either use thresholds available on the device, set a sensor to always appear to be up or customize thresholds as appropriate.

After a hardware sensor reaches the appropriate threshold value, it triggers an event, and the alert "Hardware is in warning or critical state." For more information about alerts, see Creating and Managing Alerts.

To edit thresholds:

1. Go to **Manage Hardware Sensors** view (Settings > Node & Group Management > Manage Hardware Sensors).
2. Find the sensor(s) you want to manage. You can either use the **Group by** pane, or use the **Search** box.

   Tip: To find all sensors available on a node, select Node in the **Group by** list, and then select the appropriate node.

3. Select the sensor(s) for which you want to change thresholds and click **Edit Thresholds**.
4. Select how you want to change the selected hardware sensor's status:

   Use Orion Defaults

   Use thresholds configured on the device. This is the default setting for Orion sensors.

   Force to Up

   Display the selected sensor always as UP, ignoring the real data from the sensor.

   Set Custom Thresholds

   Use the dynamic query builder to define the status for the selected sensor.

5. Click **Submit** to apply your changes.

Changing MIB Used for Polling Hardware Health Statistics

Hardware sensors information on Cisco devices can be polled using one of the following MIBs.

- CISCO-ENTITY-SENSOR-MIB (default MIB)
- CISCO-ENVMON-MIB

Each MIB contains different OIDs, and appropriate information for individual nodes might be included only in one of them. If you thus see inconsistencies between the actual hardware health and the status shown in the Orion Web Console, you can change the MIB used for polling hardware health statistics.

You can either change the MIB used for polling hardware health statistics globally, for all nodes monitored in the Orion database, or you can customize the MIB for individual nodes.

To change the MIB tree used for polling hardware health globally:

1. Log on to the Orion Web Console as an administrator.
2. Click **Settings**, and then click **Polling Settings** in the Thresholds and Polling grouping.
3. Scroll down to the **Hardware Health Polling** section and select the appropriate MIB in the **Preferred Cisco MIB** list.
4. Click **Submit** to apply your settings.

This procedure changes the default MIB used for polling all hardware sensors on all monitored nodes.

To change the MIB for polling hardware health statistics on a node:

1. Open the appropriate Node Details view, and click **Edit Node** in the Management resource.
2. Scroll down to the **Hardware Health Polling** section and select the appropriate MIB.
3. Click **Submit** to apply your changes.

Note: Changing MIB for a node overrides the general settings. Once you customize the MIB for polling hardware health sensors, it will not be subject to change if you change the general settings.

Changing Hardware Health Units in Hardware Health Resources

By default, hardware health resources display temperature in degrees Fahrenheit.

To change the temperature unit used in hardware health resources:

1. Log on to the Orion Web Console.
2. Navigate to a node details view.
3. Go to the Current Hardware Health resource, and click **Edit**.
4. Select the appropriate unit for temperature display (**Fahrenheit** or **Celsius**).
5. Click **Submit** to apply your changes.

The selected unit will be applied in all hardware health resources in the Orion Web Console. This setting is user-specific, and it is connected with your user account.

Note: You can also access the temperature unit setting via Settings > Manage Accounts > select a user > Edit > Hardware Package Settings > select the default temperature unit (Celsius or Fahrenheit).

Troubleshooting Hardware Health

This section describes possible causes and solutions concerning hardware resources either not being reported or being reported incorrectly.

Incorrect Hardware Health Statistics

If you can see that Orion Web Console does not display correct status information about your sensors, you can consider changing the MIB tree used for polling your Cisco device. For more information, see Changing MIB Used for Polling Hardware Health Statistics.

Temperature Shown in Unsuitable Units

Temperature statistics can be displayed in degrees Celsius or Fahrenheit. For more information about changing the temperature units, see Changing Hardware Health Units in Hardware Health Resources.

Data Is Not Available in Custom Hardware Health Charts

When monitoring hardware health, there might be sensors which do not report values, just the sensor status. These sensors cannot be displayed in charts because the data used for creating the chart are missing.

Chapter 9: Common NPM Tasks

The following chapter provides a number of common network performance monitoring scenarios for which NPM provides solutions.

Creating an Alert to Discover Network Device Failures

With alerting, Orion platform products give you the ability to immediately discover whenever any device on your network is experiencing a problem.

The procedures in the topics below create an alert that uses a custom location property to alert you to a node failure on your monitored network:

- Creating a Custom Property
- Creating an Alert Using a Custom Property

Creating a Custom Property

The Custom Property Editor allows you to choose from a collection of many commonly used properties, or to build your own custom properties. Once your custom property is defined, the Import Wizard allows you to populate your new property from either a text- or comma-delimited file. For more information, see Importing Custom Property Data.

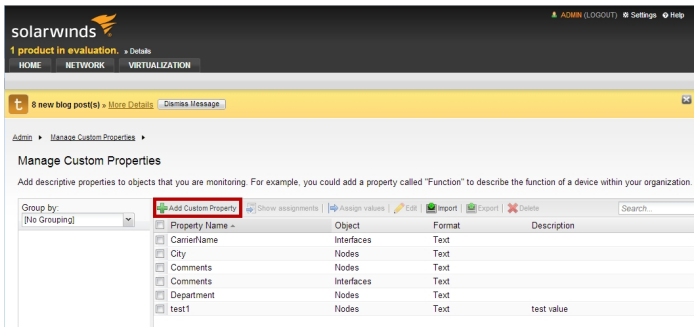
Alternatively, if you only have a few individual changes or additions, you may choose to make those changes using the **Edit** view. For more information, see Editing Custom Properties.

The following procedure shows how to create a custom location property that is applied to monitored nodes.

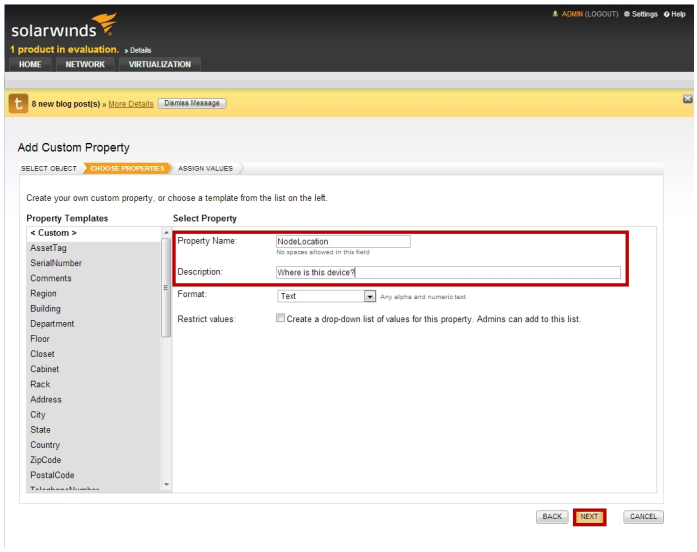
To create and apply a custom location property:

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**.

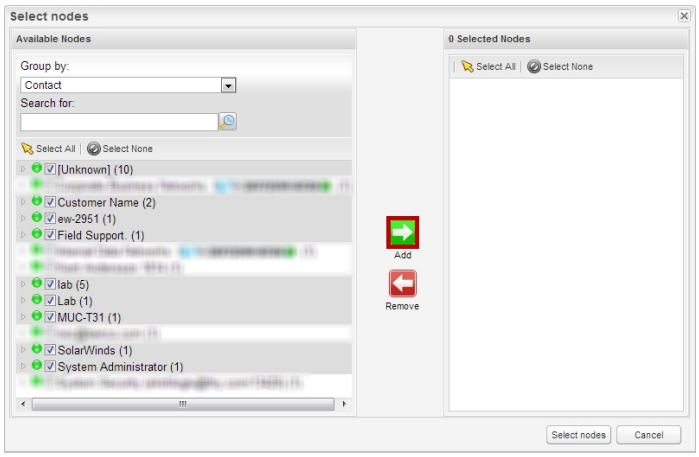


4. Select **Nodes**, and then click **Next**.
5. Enter **NodeLocation** as the **Property Name**, provide an appropriate **Description**.

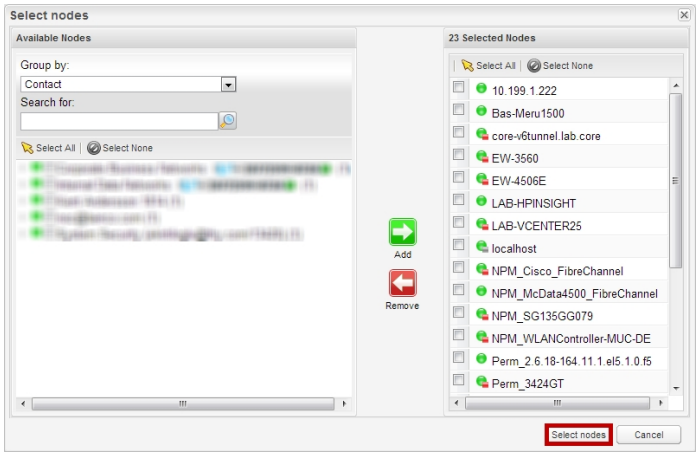


6. If you want this to be a mandatory property required for all nodes, click on **Required**.
7. Click **Next**.
8. Click **Select Nodes**.

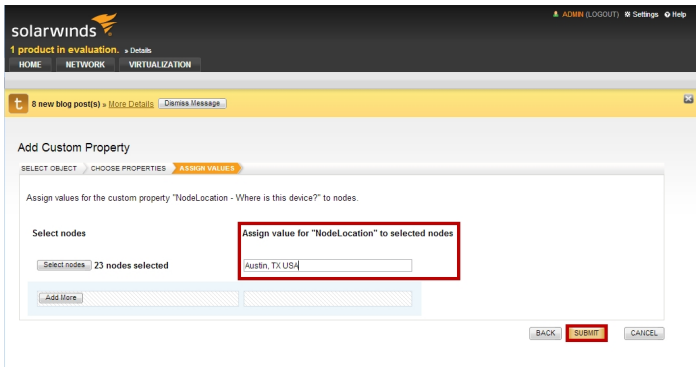
9. Select all the nodes to which you want to assign the same value for **NodeLocation**, and click **Add**.



10. When all nodes that can be given the same value are selected, click **Select nodes**.



11. Enter the **NodeLocation** for this selection of nodes, and click **Submit**.



The **NodeLocation** custom property is now defined for all selected nodes.

12. **To add values to other nodes,** select **NodeLocation**, and click **View/Edit Values**. Enter the values in the **NodeLocation** column, and click **Save Changes** when completed.

Use a Custom Property in Alerts

The following example creates multiple alerts using the *NodeLocation* custom property defined in Creating a Custom Property. An alert triggers when a node goes down. Upon triggering, the alert will write to a local log file, send a syslog message, and send an SNMP trap.

Note: The **${**variable**}** syntax is required for variables. For more information on the use of variables, see Orion Variables and Examples.

To create a new alert:

1. Click **Settings > Manage Alerts**.
2. Select the check box next to **Node is down,** and then click the **Duplicate & Edit** button.
3. Click **Trigger Condition**, and add a child condition. A child condition should already exist for a node being down.
4. Select the node object, and choose **NodeLocation** in the field drop-down. Enter a comparison and value.
5. Click the **Trigger Actions**, and then click **Add Action**.

6. Select **Log the Alert to a file**, and then click **Configure Action**.
    a. Enter the log filename in the **Alert Log Filename** field.
    b. In the **Message** text box, type the following:
    Node ${N=SwisEntity;M=Caption} is currently down.
    c. Click **Add Action**.
7. Click **Add Action**, and select **Send a Syslog Message**. Click **Configure Action**.
    a. Type **127.0.0.1** as the **Hostname or IP Address of the Syslog Server**, and then type the following in the **Message** field:
    Node ${N=SwisEntity;M=Caption} is currently down.
    b. Click **Add Action**.
8. Click **Add Action**, and select **Send SNMP Trap**. Click **Configure Action**.
    a. Type **127.0.0.1** as the **SNMP Trap Destination**, and then type the following in the **Alert Message** field:
    Node ${N=SwisEntity;M=Caption} is currently down.
    b. Click **Next**.
    c. Click **Add Action**.
9. Click **Summary**, and click **Submit**.

You can test your alert, and view the results of each of your alert actions as follows. See Testing Alerts for more information.

- You can view results of your Syslog message action in the Web Console or through the Syslog Viewer on your SolarWinds Orion server.
- To view the results of your SNMP Trap action, click **Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer**.

Scheduling and Emailing Business Hours Reports

Orion Report Writer is a component available to all Orion products. Using Orion Report Writer and web-based Report Scheduler, you can create reports that you can then distribute as regularly scheduled emails. The following sections create and schedule for email delivery an example report of interface traffic during peak business hours.

Creating a Business Hours Report

The following procedure creates a monthly report of interface traffic during peak business hours, defined as between 7:00 AM and 7:00 PM.

To create a business hours interface traffic report:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Report Writer**.
2. In the left pane, click Historical Traffic Reports > Average and Peak Traffic Rates – Last Month.
3. On the General tab, edit the **Report Group**, Report Title, and Description as appropriate.
4. On the Filter Results tab, click **Browse (...)**.
5. Select **Add a new elementary condition**.
6. In the new field, click the first asterisk (*), and then select **Date/Time (Traffic Filtering Only) > Time of Day (24 hour format)**.
7. Click **is equal to**, and then select greater or equal.
8. Click the second asterisk (*), and then enter the start time of your peak business hours in 24-hour hh:mm format (e.g. 07:00).
9. Click **Browse (...)**, and then select **Add a new elementary condition**.
10. Click the first asterisk (*), and then select **Date/Time (Response Time Filtering Only) > Time of Day (24 hour format)**.
11. Click **is equal to**, and then select less.
12. Click the second asterisk (*), and then enter the end time of your peak business hours in 24-hour hh:mm format (e.g. 19:00).
13. Click **Browse** (...), and then select Add a new elementary condition.

14. Click the first asterisk (*), and then select **Date/Time (Traffic Filtering Only) > Day of Week**.
15. Click **is equal to**, and then select not equal.
16. Click the second asterisk (*), and then select **Saturday**.
17. Click **Browse (...),** and then select **Add a new elementary condition**.
18. Click the first asterisk (*), and then select **Date/Time (Response Time Filtering Only) > Day of Week.**
19. Click **is equal to**, and then select not equal.
20. Click the second asterisk (*), and then select **Sunday**.
21. Click **Preview** on the right of the Report Designer pane.
22. Click **File > Save**.

The report is now saved to the Reports folder on your Orion server. It will list as a member of the Report Group provided on the General tab in Report Designer.

Scheduling and Emailing a Report

The following procedure schedules a selected report for distribution using email.

To schedule an emailed report:

1. Log in to the Orion Web Console.
2. Click **Home > Reports**.
3. Click **Manage Reports** in the upper right.
4. Click the **Schedule Manager** tab.
5. Click **Create New Schedule**. The Add Report Schedule page is displayed.
6. Enter an appropriate **Schedule Name** and **Description of Report Schedule**.
7. Click **Assign Report**, select the report(s) to be included in this schedule, and click **Assign Report(s)**.
8. Click **Next** to display the **Frequency** view.

9. Click **Add Frequency** and then complete the following steps:
    a. Enter a name for this frequency.
    b. Select:
        - **Specific Date(s)** to select specific dates and times
        - **Daily** to schedule the report actions every day
        - **Weekly** to schedule the report actions once or more a week
        - **Monthly** if you want to select the month and the day of the month to schedule the report actions.
10. Click **Next** to display the Actions view.
11. Click **Add Action**, and select the **Email** action, and then click **Configure Action**.
12. Enter a **Name** for the action.
13. Define recipients.
    a. In the **To** field, enter the email addresses of all recipients, separated by semicolons.
    b. ***To add CC or BCC addresses***, click **CC** and/or **BCC**, and enter the email addresses of these recipients.
    c. ***To change the default name and address of the sender***, click "-" and enter the appropriate **Name of Sender** and **Reply Address**.
14. Click **Message**, and enter the **Subject** and **Message** for the email. You can compose the message as **HTML** or **Plain Text**.
    a. ***If you also want a printable version of your emailed reports***, check **Retrieve a Printable Version of Reports**.
    b. Check the format(s) in which you want to provide the emailed report: **PDF**, **CSV**, **Excel**, or **HTML**.
    c. ***To include the URL of the emailed report so the recipients can access it remotely***, check **Include Report's URL**.
15. Click **SMTP Server** and define it.
    - ***If you have already configured an SMTP server***, select the **Name of SMTP Server**, and click **Save**.

- ***If you have not already configured an SMTP server***, select **Add New Server**, and complete the following steps:

    a. Provide the **Hostname or IP Address** of your SMTP Server and the designated **SMTP Port Number**.

    Note: The SMTP server hostname or IP address field is required. You cannot send an email without identifying the SMTP server.

    b. ***To use SSL encryption for your emailed report,*** check **Use SSL**. This changes the SMTP port number to 465.

    c. ***If your SMTP server requires authentication***, check **This SMTP Server requires Authentication**, and provide requested credentials.

16. Click **Add Action**.
17. Click **Next** to display the Summary view.
18. ***If the schedule summary is correct***, click **Create Schedule**.

    The schedule is applied for the selected report and displayed in the Schedule Manager.

Creating Geographic or Departmental Views

Using groups, it is a straightforward process to create custom web console views displaying information about monitored objects distinguished by geographic or departmental location. The following procedures create custom views that are then populated with appropriate group-based resources.

Creating a Custom Group

The following procedure creates a custom group of monitored objects in a defined geographic location.

To create a custom group:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Log in to the web console as an administrator.
3. Click **Settings** in the top right corner of the web console, and then click **Manage Groups** in the Node & Group Management grouping of the Orion Website Administration page.
4. Click **Add New Group**, and then provide an appropriate Name and Description for the custom group. For example, a group named **Austin** could be described as, **All monitored network objects in the Austin office**.
5. Click **Next**.
6. In the Available Objects pane, check all monitored objects fitting the group definition. For example, using the example above, select all objects located in the Austin office.
7. Click **Add to Group**.
8. Select all monitored objects in the new group pane on the right, and then click **Create Group**.

The new group of monitored objects located in the same geographic location is now listed on the Manage Groups view.

Creating a Custom View

The following procedure creates a custom view that will be used to display monitoring information g for devices in a selected group.

To create a custom, group-based view:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Log in to the web console as an administrator.
3. Click **Settings** in the top right corner of the web console.
4. Click **Add New View** in the Views grouping of the Orion Website Administration page.
5. In the Name of New View field, provide a name for the custom view.
6. In the Type of View selection field, select **Group Details**.
7. Click **Submit**.
8. ***To add a resource,*** repeat the following steps for each resource:

    a. Click **+** next to the column in which you want to add a resource.

    b. Check all resources you want to add, and click **Add Selected Resources**.

    Notes:

    - Use the **Group by:** field on the left to limit the resource list or use the **Search** field at the top to locate specific resources.
    - Resources already in your view will not be checked on this page listing all web console resources. It is, therefore, possible to pick duplicates of resources you are already viewing.
    - Some resources may require additional configuration. For more information, see Resource Configuration Examples.
    - Several options on the Add Resources page are added to the list of resources for a page, but the actual configuration of a given map, link, or code is not added until the page is previewed.
9. ***To change the width of a column,*** enter the width in pixels in the **Width** field beneath the column.

10. ***To delete a resource from a column,*** select the resource, and then click **X** next to the resource column to delete the selected resource.
11. ***To copy a resource in a column,*** select the resource, and then click  next to the resource column to delete the selected resource.
12. ***To move a resource to another column***, use the back and forward arrow icons next to the resource column to transfer the resource to the previous or next column.
13. ***If you are using subviews and want to move a resource to another tab***, click on ***Move to a different tab*** to open a window enabling you to move to a selected tab and column.
14. ***To rearrange the order in which resources appear in a column,*** select resources, and then use the up and down arrow icons to rearrange them.
15. ***If you have finished configuring your view,*** click **Preview**.

    Note: A preview of your custom web console displays in a new window. A message may display in the place of some resources if information for the resource has not been polled yet. For more information, see Resource Configuration Examples.
16. Close the preview window.
17. ***If you are satisfied with the configuration of your view,*** click **Done**.

Capacity Forecasting

NPM allows you to display usage trends of various system resources and to predict capacity issues before they happen. Capacity forecasting enables you to plan accordingly and take appropriate measures before full usage issues occur.

Capacity forecasting is available for the following metrics of nodes, interfaces, and volumes monitored by NPM:

- CPU utilization on nodes
- Memory usage on nodes
- Space usage on volumes
- Receive (in) utilization on interfaces
- Transmit (out) utilization on interfaces

NPM calculates capacity usage trends based on historical data. The more historical data is available, the more precise is the calculated forecast.

Forecast Calculation Methods

The capacity forecast is calculated twice, using the following methods:

- **Peak calculation** forecasts trends using daily maximum values. This method is suitable for important devices and connections, where it is important to completely avoid reaching a certain usage level (threshold).
- **Average calculation** forecasts trends using daily average values. This method is suitable for non-critical network devices or connections where short periods exceeding the threshold level are acceptable.

You can set the forecast calculation method either globally, for all monitored objects, or customize the capacity forecasting method for individual objects (nodes, interfaces, or volumes).

Requirements

Capacity forecasting is automatically available for nodes, interfaces, and volumes that meet the following requirements:

- Appropriate nodes, interfaces, and volumes must be managed in SolarWinds NPM.

- You need to have enough historical data in the database. By default, 7 days of data are required.

Forecasting Capacity Usage for Nodes, Interfaces, or Volumes

NPM can analyze the capacity usage of your nodes, interfaces, and volumes. Polled data are used to calculate when available resources will be fully used. The information is provided both in a table form, and in intuitive graphs.

Capacity forecasting in NPM allows you to:

- Locate pending capacity problems.
- View usage trends and forecast in graphs.
- See an overview of trends and forecast in the table form.

Locating Pending Capacity Problems

To locate which nodes, interfaces, or volumes will soon need more capacity than available, consult the **Top XX Capacity Problems** resource. The resource lists a customized number of objects whose usage trend is rising.

If you do not see the resource in a view, you can add it. For more information, see Adding Capacity Forecasting Resources.

Viewing Capacity Usage Trends and Forecast in Graphs

To see a graphical display of capacity usage trends calculated by both methods, go to the details view for the node, volume, or interface and consult the appropriate forecast chart:

- CPU Capacity Forecast Chart
- Memory Capacity Forecast Chart
- Storage Capacity Forecast Chart
- Interface Utilization Receive Forecast Chart
- Interface Utilization Transmit Forecast Chart

Charts allow you to customize the time shown, to zoom in and out. They are accompanied by a table which provides the capacity usage trend, the time period when the capacity usage reaches the warning and critical thresholds, as well as a forecast of when all available capacity will be used.

If you do not see the resource in a view, you can add it. For more information, see Adding Capacity Forecasting Resources.

Viewing Capacity Usage Trends and Forecast in Tables

For a brief overview of usage trends for a node, volume, or interface, go to the details view for the object, and consult the appropriate capacity forecast resource:

- **Node Capacity** provides an overview of both CPU load and percent memory usage in the past 7 days, a forecast when the warning and critical thresholds will be exceeded, and when the resource will be fully used.
- **Volume Capacity** provides an overview of volumes capacity usage in the past 7 days, a forecast when the warning and critical thresholds will be exceeded, and when the volume capacity will be fully used.

Forecasts in this resource are calculated using the default method (peak or average) specified for the appropriate resource. For more information, see Changing Capacity Forecasting Settings Globally.

If you do not see the resource in a view, you can add it. For more information, see Adding Capacity Forecasting Resources.

Adding Capacity Forecasting Resources

If you cannot see the appropriate resource on a view, you can add it. However, capacity forecasting resources display only on views for which they are relevant. For example, interface utilization resources can only be added on interface detail views.

To add a capacity forecasting resource:

1. Log in to the Orion Web Console and go to the view where you want to add the resource.
2. Click **Customize Page** in the top right corner.
3. Click the + icon on the Edit view page, and type "forecast" or "capacity" into the **Search** field.
4. Select the appropriate resource, and then click **Submit**.
5. Click **Submit** to add the resource on the view.

Changing Capacity Forecasting Settings Globally

Capacity forecasting settings include the calculation method and thresholds for appropriate metrics. You can change the settings either globally, for all monitored objects, or customize them for individual nodes, volumes, and interfaces. The following section explains changing capacity forecast settings globally.

For more information about customizing thresholds and forecast calculation method for individual objects, see Customizing Capacity Forecasting Settings for Individual Nodes, Interfaces or Volumes.

Nodes/Volumes

To change capacity forecasting settings for nodes and volumes:

1. Go to **Settings > Orion Thresholds**.

   Note: If you already are in a capacity forecasting resource, click **Edit**, and then click **Orion General Thresholds**.

2. Specify values for **Critical Level** and **Warning Level** for appropriate metrics:
   - **AVG CPU Load** for CPU usage on nodes
   - **Disk Usage** for volume capacity usage
   - **Percent Memory Used** changes the method used for memory usage on nodes
3. For each metric, select the appropriate calculation method.
   - Calculate exhaustion using average daily values
   - Calculate exhaustion using peak daily values
4. Click **SUBMIT**.

Interfaces

To change capacity forecasting settings for interfaces:

1. Go to **Settings > NPM Thresholds**.

   Note: If you already are in an interface capacity forecasting resource, click **Edit**, and then click **NPM Thresholds**.

2. Go to the **Interface Percent Utilization** section, define appropriate Critical and Warning threshold values for the metric.

3. Select the appropriate calculation method:
    - Calculate exhaustion using average daily values
    - Calculate exhaustion using peak daily values
4. Click **SUBMIT**.

Customizing Capacity Forecasting Settings for Individual Nodes, Interfaces or Volumes

You can set different forecast calculation methods and thresholds for individual nodes and volumes. For interfaces, the calculation method is set globally, and you can customize only the thresholds.

For important nodes, interfaces or volumes, you can set warning and critical thresholds to lower percentage values, thus giving you enough time to take appropriate measures before capacity issues occur.

To customize capacity forecasting settings for nodes:

1. Log into the Orion Web Console as an administrator.
2. Open the Edit Properties page for the appropriate node.

    Go to **Settings > Manage Nodes**, select the appropriate node, and then click **Edit Properties**.

    If you are in a capacity forecasting resource, click **Edit** in the resource, and then click the link to the node's Edit Properties page.
3. Now on the **Edit Properties** page, scroll down to **Alerting Thresholds**.
4. Metrics relevant for interface capacity forecasting:
    - CPU Load
    - Memory Usage
5. Select the **Override Orion General Threshold** box for the metrics whose capacity forecasting settings you want to change.
6. Define the appropriate **Warning** and **Critical** threshold levels for the node.

7. Select the appropriate method for calculating trends:
   - Calculate exhaustion using average daily values
   - Calculate exhaustion using peak daily values

   Note: If you want to use baseline thresholds, click **Use Dynamic Baseline Thresholds**. For more information, see Orion Baseline Data Calculation.

8. Click **Submit** to apply your changes.

To customize capacity forecasting settings for interfaces:

1. Log into the Orion Web Console as an administrator.
2. Open the Edit Properties page for the appropriate interface.

   Go to **Settings > Manage Nodes**, select the appropriate interface, and then click **Edit Properties**.

   If you are in an interface capacity forecasting resource, click **Edit** in the resource, and then click the link to the interface's Edit Properties page.

3. Now on the **Edit Properties** page, scroll down to **Alerting Thresholds**.

   Metrics relevant for interface capacity forecasting:
   - Receive Interface Utilization
   - Transmit Interface Utilization

4. Select the **Override Orion General Threshold** box for the resource group whose thresholds you want to change.
5. Customize the appropriate **Warning** and **Critical** threshold levels.

   Note: If you want to use baseline thresholds, click **Use Dynamic Baseline Thresholds**. For more information, see Orion Baseline Data Calculation.

6. Click **Submit** to apply your changes.

To customize capacity forecasting settings for volumes:

1. Log into the Orion Web Console as an administrator.
2. Go to **Settings > Manage Nodes**.
3. Select the appropriate volume, and then click **Edit Properties**.

Note: To find the volume, locate the appropriate node and click the + sign to display interfaces and volumes on the node.

4. Select the **Override Orion Capacity Thresholds** box for **Percent Disk Usage**.
5. Customize the appropriate **Warning** and **Critical** threshold levels.
6. Select the appropriate method for calculating trends:
   - Use Average values
   - Use Peak values
7. Click **Submit** to apply your changes.

Chapter 10: Managing Web Accounts

Orion Web Console user accounts, permissions, and views are established and maintained with the Account Manager in the **Settings** page.

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

Creating New Accounts

New web console user accounts may be created by web console administrators.

Note: To maintain administrative privileges, Windows individual and group user accounts must be defined in the same domain as the SolarWinds server to which they are given access.

To create a new user account:

1. Log in to the Orion Web Console as an administrator, and then click **Settings** in the top right of the web console.
2. Click **Manage Account** in the Accounts grouping of the Orion Website Administration page, and then click **Add New Account**.
3. Select the type of account you want to add, and then click **Next**.
4. ***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 User Accounts.
5. ***If you selected Windows individual account,*** complete the following steps:
    a. Provide the **User Name** and **Password** for a user that has administrative access to your Active Directory or local domain.
    b. In the Search for Account area, enter the **User name** of the Active Directory or local domain user for whom you want to create a new web console account, and then click **Search**.
    c. In the Add Users area, select the users for whom you want to create new web console accounts, and then click **Next**.

6. ***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**.

When the new account is created, the Edit User Account view displays, showing all configurable account options. For more information about editing account settings, see Editing User Accounts.

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.

Editing User Accounts

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

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

- User Account Access Settings
- Setting Account Limitations
- Defining Pattern Limitations
- Setting Default Account Menu Bars and Views
- Configuring an Account Report Folder
- Configuring Audible Web Alerts

User Account Access Settings

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

To edit a 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 User 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:

   - 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.
   - 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.

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 Monitoring Devices in the Web Console.

10. ***If you want to allow the user to edit and manage reports directly from the Orion Web Console, set Allow Report Management Rights to Yes.***

    Note: By default, report management rights are not granted.

11. ***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.

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

13. 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. Right-click menu options also depend on installing the SolarWinds Desktop Toolset and running the Toolset Integration Tray application on each client computer.

14. ***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.

15. 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.

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. The following procedure sets user account limitations.

For more information about creating account limitations, see Creating 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, check 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 Orion NetFlow Traffic Analyzer (NTA) initially caches account limitations, it may take up to a minute for account limitations related to Orion NTA to take effect in Orion NTA.
- 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.

e. Define the limitation as directed on the Configure Limitation page that follows. For more information about defining pattern-type limitations, see 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, check 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 Orion NetFlow Traffic Analyzer (NTA) initially caches account limitations, it may take up to a minute for account limitations related to Orion NTA to take effect in Orion NTA.
      - 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.

   e. Define the limitation as directed on the Configure Limitation page that follows. For more information about defining pattern-type limitations, see 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.
   - Because Orion NetFlow Traffic Analyzer (NTA) initially caches account limitations, it may take up to a minute for account limitations related to Orion NTA to take effect in Orion NTA.
   - Group limitations are not applied until after group availability is calculated.

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

When limiting user access to certain network objects, try using limitations to specific objects and avoid pattern limitations. Validating pattern limitations is more time and performance consuming.

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 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 NPM 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 an Account Report Folder

Reports may be assigned to an account by creating sub-directories within the Reports directory. Desired reports are included within the sub-directory, and the sub-directories are then made available for assignment to an account. This provides a level of security when reports are included in a view or added as custom menu items.

To configure an account report folder:

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. Select the account you want to configure, and then click **Edit**.
4. ***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 NPM installation directory: **C:\Program Files\SolarWinds\Orion**.
5. 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**.

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

Orion provides predefined account limitations that use built-in Orion 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 a Custom Property.

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

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 about custom properties, 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.
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.

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**.

Configuring Automatic Login

The Orion Web Console allows you to log in using any of the following methods:

- Windows Active Directory Authentication, available in all Orion products released after SolarWinds NPM version 10.1.
- Windows Pass-through Security. If you choose to employ Windows Pass-through Security, SolarWinds NPM users can be authenticated through Windows Security, with no need to log in using a separate SolarWinds NPM 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 NPM prioritizes user login in the following manner:

1. Windows Active Directory Authentication is enabled. To enable Windows Active Directory Authentication, check 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 products released before Orion NPM version 10.1, you may take advantage of the Windows Pass-through Security functionality when IIS NT Security is enabled. Orion users can be authenticated through Windows Security, with no need to log in using a separate Orion 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 Orion Platform 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 Orion 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.

2. ***If you are using Local Computer Authentication Format for passthrough accounts,*** create these accounts in the Orion Web Console Account Manager using Computer\UserID as the **User Name**, as follows:

   - **SolarWindsS2\Edward**
   - **Server3\JonesR**

   Note: For more information about creating accounts using the Orion Web Console Account Manager, see Creating New Accounts.

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. Check **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**, check **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.

   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 NPM 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 Orion 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 Manager. 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.

Chapter 11: Managing Groups and Dependencies

Dependencies and groups enable you to manage your network effectively. Groups give you the ability to logically organize monitored objects, regardless of device type or location, and dependencies allow you to more faithfully represent what can actually be known about your network, eliminating “false positive” alert triggers and providing more accurate insight into the state of your network.

Managing Groups

You can manage Orion objects such as nodes, volumes, applications, interfaces, and even other groups as groups. You create, delete, and modify groups from the **Manage Groups** page.

Note: Nesting a group within another does not create a strict parent/child relationship. You can include any group as a member in any number of other groups.

To access the Manage Groups page:

1. Log on to the Orion Web Console.
2. Click **Settings** in the top right of the web console.
3. Click **Manage Groups** in the Node & Group Management grouping of the Orion Website Administration page.

The following sections provide more information about creating and managing groups in Orion:

- Creating Groups
- Editing Existing Groups
- Deleting Groups
- Managing the Display of Group Status

Creating Groups

Creating a group is a straightforward process of selecting the Orion objects you want the group to contain. At creation time, you can also decide how you want SolarWinds Orion to roll up the status of the group members.

It is also possible to specify group members on the basis of shared properties by adding them with a dynamic query. Orion objects added through dynamic queries are automatically added or removed from the group.

To create a new group:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Groups** in the Node & Group Management grouping of the Orion Website Administration page.
3. Click **Add New Group**.

4. Enter a name for the group in the **Name** field.
5. Enter a description for the group in the **Description** field.
6. Click **Advanced**.
7. Select the **Status rollup mode** from the drop-down menu. This can be **Show best status**, **Mixed status show warning** or **Show worst status**. For more information, see Managing the Display of Group Status.
8. ***To change the refresh frequency for objects in the group***, enter a new value in the **Refresh frequency** field.
9. ***If Custom Properties have been set up for groups, fields for each will be displayed***, allowing you to enter values for this Group.

   Note: If you want to create custom properties, click **Manage Custom Properties** to do so in a new tab. For more information, see Creating Custom Properties.
10. Click **Next**.
11. ***To manually select objects for this group***, follow these steps:

    a. From the **Show Only** drop-down list, select the type of Orion object to add as a group member.

    b. From the **Group by** drop-down list, select how you want to group these objects, or select **[No Grouping]** to display all.

    c. Check the checkbox of the Orion objects and click **Add to Group**.
12. ***To dynamically select group members based on shared properties***, follow these steps:

    a. Click **Add dynamic query**.

    b. Type a name for the query in the **Dynamic query object name** field.

    c. Select an Orion object type from the **Orion Object is** drop-down list.

    d. Click **Add Condition**, and select the property, argument and value for each condition you want to use.
    Note: Use the question mark (**?**) character as a multiple character wildcard. Use the underscore (**_**) character as a single character wildcard.

e. Click **Preview** to verify that the dynamic query is selecting your intended objects.

f. Click **Save**.

13. Continue adding individual objects or dynamic queries until you have finished building your group.
14. Click **Create Group**.

Editing Existing Groups

You can edit the properties of an existing group or add and remove objects.

To edit properties of an existing group:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Groups** in the Node & Group Management grouping of the Orion Website Administration page.
3. Check the group you want to edit, and then click **Edit Properties**.
4. Edit the **Name** and **Description** of the selected group, as appropriate.
5. Click **Advanced**.
6. ***To change the display of the group's status,*** select the **Status rollup mode** from the drop-down menu. This can be **Show best status**, **Mixed status show warning** or **Show worst status**. For more information, see Managing the Display of Group Status.
7. ***To change the refresh frequency for objects in the group***, enter a new value in the **Refresh frequency** field.
8. ***If Custom Properties have been set up for groups***, fields for each will be displayed, allowing you to edit values for this Group.

   Note: To create custom properties, click **Manage Custom Properties** to do so in a new tab. For more information, see Creating Custom Properties.
9. ***To manage the members of the selected group,*** click **Add & Remove Objects**.
10. ***To manually add objects for this group***, follow these steps:

    a. From the **Show Only** drop-down list, select the type of Orion object to add as a group member.

b. From the **Group by** drop-down list, select how you want to group these objects, or select **[No Grouping]** to display all.

c. Check the checkbox of the Orion objects and click **Add to Group**.

11. ***To add a new query to dynamically select objects*** , follow these steps:

    a. Click **Add dynamic query**.

    b. Type a name for the query in the **Dynamic query object name** field.

    c. Select an Orion object type from the **Orion Object is** drop-down list.

    d. Click **Add Condition**, and select the property, argument and value for each condition you want to use.
    Note: Use the question mark (**?**) character as a multiple character wildcard. Use the underscore (_) character as a single character wildcard.

    e. Click **Preview** to verify that the dynamic query is selecting your intended objects.

    f. Click **Save**.

12. ***To edit an existing query***, follow these steps:

    a. Click **Edit dynamic query**.

    b. ***To edit the query name***, edit the **Dynamic query object name** field.

    c. ***To edit the object type***, select the new object type from the **Orion Object is** drop-down list.

    d. ***To edit a query condition***, edit the property, argument and value as required.

    Note: Use the question mark (**?**) character as a multiple character wildcard. Use the underscore (_) character as a single character wildcard.

    e. Click **Preview** to verify that the edited dynamic query is selecting your intended objects.

    f. Click **Save**.

13. To remove an object or query from a group, select the query or object by clicking the box before it, and click **Remove**.

14. Click **Submit** to save the edited objects and queries.
15. Click **Submit** again to save the group.

Managing Group Members

The following procedure manages the objects included within a defined group.

To add and remove the objects of an existing group:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Click **Settings** in the top right of the web console, and then click **Manage Groups** in the Node & Group Management grouping of the Orion Website Administration page.
3. Check the group you want to edit, and then click **Add & Remove Objects**.

Deleting Groups

Deleting an existing group is a straightforward process, as shown in the following procedure.

To delete a group:

1. Click **Settings** in the top right of the web console
2. Click **Manage Groups** in the Node & Group Management grouping of the Orion Website Administration page.
3. Check the group you want to delete, and then click **Delete**.

Managing the Display of Group Status

The status of any particular group is determined by the status of the members of the group. There are three methods for determining the status displayed for a selected group of monitored objects:

Note: For more information, see Status Icons and Identifiers.

- **Show Best Status** is useful for displaying groups that are defined as collections of redundant or backup devices. The following table indicates how the **Show Best Status** option operates:

Note: Compare Group Status results under the Show Best Status option with results for the same groups of objects under the Show Worst Status option.

Object States	Group Status
(Up, Warning, Down)	(Up)
(Warning, Down)	(Up)
(Warning, Down, Unknown)	(Warning)

- **Show Worst Status** ensures that the worst status in a group of objects is displayed for the whole group. The following table indicates how the **Show Worst Status** option operates:

Object States	Group Status
(Up, Warning, Down)	(Down)
(Warning, Down)	(Warning)
(Warning, Down, Unknown)	(Down)

- **Mixed Status shows Warning** ensures that the status of a group displays the worst warning-type state in the group. If there are no warning-type states, but the group contains a mix of up and down states, then a Mixed Availability ( ) warning status is displayed for the whole group. The following table indicates how the **Mixed Status shows Warning** option operates:

Object States	Group Status
	(Critical)
	(Critical)
	(Mixed Availability)

The following procedure configures the method used to determine group status.

To configure the method used to determine the status of a selected group:

1. Click **Settings** in the top right of the web console, and then click **Manage Groups** in the Node & Group Management grouping of the Orion Website Administration page.
2. Check the group you want to edit, and then click **Edit Properties**.
3. Expand **Advanced**, and then select a **Status rollup mode**, as follows:
    a. ***To roll up the worst status of the group members***, select **Show Worst Status**.
    b. ***To roll up the best status of the group members***, select **Show Best Status**.
    c. ***To display a warning status if the group members have a mixture of different statuses***, select **Mixed Status shows warning**.
4. Click **Submit**.

Managing Dependencies

Dependencies account for topological constraints on your network. These constraints may be either the result of the design of a specific device, such as interfaces on a switch or router, or the result of the physical architecture of the network itself. The *Unreachable* status accounts for cases where a device may appear to be down, but its status is actually indeterminate due to another device being down or unresponsive.

Interfaces are unique because they cannot be defined as child objects in the product. SolarWinds products determine the interface status by polling the parent node. If the parent node is physically down or unresponsive to the selected polling method, all interfaces on the parent node are reported as Unreachable.

For example, when a switch goes down or becomes unresponsive, all interfaces on the switch are also unresponsive, even though they may working. The child interfaces display as Unreachable because their parent node reports as down.

You can also define dependencies among distinct devices, such as a subnet of devices on your network that depends on a single WAN link to connect with the rest of your network. If you define a group consisting of the devices in this dependent subnet, you can define a dependency where the dependent subnet is a child group to the parent router that serves as the WAN link to the rest of your network. For more information about groups, see Managing Groups.

Your SolarWinds product can create 1:1 parent/child node dependencies automatically when you enable **Auto Dependencies** in the Polling Settings page.

Dependencies are most useful when designing alerts. If you have an alert configured to trigger when the status of a monitored object is down, you only want that alert to trigger if a monitored object is actually down. Without dependencies, all monitored objects on an unresponsive, monitored node report as down. By establishing dependencies these child objects display as Unreachable instead of down, which prevents false down object alerts.

Note: The status of objects in child groups is determined separately from the related parent object's status.

Creating a New Dependency

Creating a new dependency is a straightforward process of selecting the parent and children objects, as shown in the following procedure.

To create a new dependency:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Dependencies** in the Node & Group Management grouping of the Orion Website Administration page.
3. Click **Add new dependency**.
4. On the Select Parent page, complete the following steps:
    a. Use the **Show only:** and **Group by:** selection fields to customize the list of displayed objects and groups.
    Note: The properties listed in the **Group by:** selection field are dynamic.
    b. Select the parent object or group in the main pane, and then click **Next**.
    Note: If you want to define a dependency so that the reported states of child objects are dependent on the status of multiple parent objects, create a group including all parent objects, and then select it on this view. For more information, see Creating Groups.
5. On the Choose Child page, complete the following steps:
    a. Edit the **Dependency name**, as appropriate.
    b. Use the **Show only:** and **Group by:** selection fields to customize the list of displayed objects and groups.
    Note: Properties listed in the **Group by:** selection field are dynamically dependent on the selection in the **Show only:** field.
    c. Select the child object or group in the main pane, and then click **Next**.
    Note: If you want to define a dependency so that the reported states of multiple child objects are dependent on the status one or more parent objects, create a group including all child objects, and then select it on this view. For more information, see Creating Groups.

6. On the Review Dependency view, review the current settings for the configured dependency.
   Notes:
   - If any advanced alerts are configured on parent or child objects, they will be listed on this view. Click **+** to expand alert details.
   - In the event that a parent object is down, alerts configured on any child objects in a dependency will not trigger because the child object status is Unreachable.
7. Click **Submit** to accept the dependency definition.

Editing an Existing Dependency

Editing an existing dependency is a straightforward process, as shown in the following procedure.

Note: Automatic Dependencies cannot be edited.

To edit an existing dependency:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Dependencies** in the Node & Group Management grouping of the Orion Website Administration page.
3. Check the dependency you want to edit, and then click **Edit**.
4. On the Select Parent page, complete the following steps:
   a. Use the **Show only:** and **Group by:** selection fields to customize the list of displayed objects and groups.
      Note: Properties listed in the **Group by:** selection field are dynamically dependent on the selection in the **Show only:** field.
   b. Select the parent object or group in the main pane, and then click **Next**.
      Note: If you want to define a dependency so that the reported states of child objects are dependent on the status of multiple parent objects, create a group including all parent objects, and then select it on this view. For more information, see Creating Groups.

5. On the Choose Child page, complete the following steps:
    a. Edit the **Dependency name**, as appropriate.
    b. Use the **Show only:** and **Group by:** selection fields to customize the list of displayed objects and groups.
    Note: Properties listed in the **Group by:** selection field are dynamically dependent on the selection in the **Show only:** field.
    c. Select the child object or group in the main pane, and then click **Next**.
    Note: If you want to define a dependency so that the reported states of multiple child objects are dependent on the status one or more parent objects, create a group including all child objects, and then select it on this view. For more information, see Creating Groups.
6. On the Review Dependency view, review the current settings for the configured dependency.
    Notes:
    - If any advanced alerts are configured on parent or child objects, they will be listed on this view. Click **+** to expand alert details.
    - If a parent object is down, all alerts configured on any child objects in a dependency on the down parent object are automatically suppressed.
7. Click **Submit** to accept the dependency definition.

Deleting an Existing Dependency

Deleting an existing dependency is a straightforward process, as shown in the following procedure.

Note: Automatic Dependencies cannot be deleted.

To delete an existing dependency:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Click **Settings** in the top right of the web console, and then click **Manage Dependencies** in the Node & Group Management grouping of the Orion Website Administration page.
3. Check the dependency you want to delete, and then click **Delete**.
4. Click **Yes** to confirm deletion of the selected dependency.

Viewing Alerts on Child Objects

In the event that a parent object is down, all advanced alerts configured on any child objects in a dependency on the down parent object are automatically suppressed. The following procedure displays all advanced alerts currently configured on any child objects in a selected dependency.

To view alerts on child objects in a selected dependency:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Dependencies** in the Node & Group Management grouping of the Orion Website Administration page.
3. Check the dependency that includes the child object on which the alerts you want to view are configured, and then click **Alerts on Child**.

Chapter 12: Creating and Managing Alerts

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

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

You can create alerts for any monitored object. Most Orion platform products allow you to alert against at least Interfaces, Volumes, and Nodes.

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

- Alert Preconfiguration Tasks
- Best Practices and Tips for Alerting
- Navigating to the Alert Manager
- Creating New Alerts
- Alert Me When a Server is Down

Use the following topics to get started with web-based alerts if you have upgraded to Core version 2015.1.2:

- Changes in the Alerting Engine
- Setting Custom Status
- Building Complex Conditions

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

Alert Preconfiguration Tasks

Some alerts require extra configuration, separate software installations, or specific information input.

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

- Sending an Email/Page
- Dialing a Paging or SMS Service
- Playing a Sound
- Sending an SNMP Trap
- Creating Text to Speech Output

Note: Make sure there are monitored objects in the SolarWinds Orion database before creating or configuring alerts. Monitored objects can include items such as nodes, databases, and applications.

Sending an Email/Page

This action sends an email from the product to a selected recipient. First, configure the default SMTP server the product uses to send email. You can change the default SMTP server later or use different SMTP servers for specific alerts.

Configure the SMTP server in the alert action or from the **Settings** page. You need the following information:

- The SMTP host name or IP address
- The SMTP port number
- Whether the SMTP server uses SSL
- The SMTP credentials, if necessary
- Default sender email address

For instructions on creating an action to send an email/page, see Sending an Email/Page.

Dialing a Paging or SMS Service

This action forwards alerts to a paging or SMS service. Enable this capability by downloading and installing NotePager Pro from Notepage.net to your SolarWinds Orion server.

For instructions on configuring this action, see the NotePage Technical Support page, at http://www.notepage.net/solar-winds/technicalsupport.htm.

Playing a Sound

The Play a Sound action uses the SolarWinds desktop notification client to play the sound on your computer when an alert arrives.

You must download and install the client on every computer that you want to play a sound when an alert arrives. After installing the desktop notification client, configure which sound you want to play when an alert is received.

Computers that do not have the desktop notification client installed on them do not play a sound when an alert arrives. If you want an alert notification sound to play on your desktop or laptop, you must install and configure the desktop notification client on that computer.

Download the desktop notification client from <*Your SolarWinds Orion server*>/DesktopNotificationTool/SolarWinds.DesktopNotificationTool.msi. Run the installer and follow the on-screen instructions to install the client.

The desktop notification client requires the following information to connect to your SolarWinds Orion server and receive alerts:

- Orion Server Name or IP Address
- Orion User Name
- Password

You can use the server name and credentials that you use to logon to your SolarWinds product.

For instructions on creating an action to play a sound, see Playing a Sound.

Sending an SMNP Trap

Configure this action to enable SolarWinds NPM to send an SNMP notification. Creating this action requires the following information:

- UDP port number
- SNMP version number
- SNMP credentials

For instructions on creating an action to send an SNMP trap, see Sending an SNMP Trap.

Creating Text to Speech Output

The Text to Speech Output action uses the SolarWinds desktop notification client and your computer's speech synthesizer to convert text messages-to-speech messages. The action notifies users of new alerts by reading the alert out loud. This capability is especially helpful for users who are visually impaired or who are not always at their desks to read alerts onscreen.

Download and install the client on each computer that you want to play a sound. Then configure which synthesizer you want to play.

For instructions on set up an action to create text-to-speech output, see Using Text to Speech Output.

Configuring the Default Email Action

Email alert actions require a designated SMTP server. The Settings page enables you to configure a default SMTP server and any default sender or recipient details.

Note: Separate email addresses with a semicolon.

To configure default email alert action settings:

1. Click **Settings > Configure Default Send Email Action**.
2. Under the **Default Recipients** heading, provide the email addresses of all default recipients for any email alert action, like the following:
   `email@company.com; email2@company.com; distrolist@company.com`
3. Under the **Default Sender Details** heading, provide the default **Name of Sender** and the default **Reply Address.**
4. Under the **Default SMTP Server** heading complete the following steps:
   a. Provide the **Hostname or IP Address** of your SMTP Server and the designated **SMTP Port Number**, such as *192.168.10.124*, port *25*. This is a required field.
   b. If you want to use SSL encryption for your alert emails, select **Use SSL**.
   Note: Opting to use SSL automatically changes the SMTP port number to 465.
   c. If your SMTP server requires authentication, select **This SMTP Server requires Authentication**, and then provide requested credentials.

Best Practices and Tips for Alerting

Use the following best practices and tips to help you configure and test your alerts.

Use the Out of the Box Alerts as Templates

SolarWinds recommends using the alerts that are included when you install the product as templates for your new alerts.

Find an alert that is similar to one you want to create and click the **Duplicate & Edit** button. Not only does this pre-populate fields for you, but it also allows you to skip to specify parts of the Alert Wizard that have data you want to change.

Restrict Who Receives Alerts

During your initial evaluation and testing, send alerts to a few people instead of sending alerts to a large distribution list. This can prevent overloading your email server while you fine-tune your alerts.

Plan which Devices to Monitor

To reduce the number of alerts sent out, consider which devices are most important. For example, you may want to receive alerts only for mission critical interfaces instead of every interface on a device.

Establish Dependencies

Establishing dependencies prevents you from receiving duplicate alerts that stem from a single network event. For example, you may want to be emailed if servers in your server farm go down, but if the router goes down and the servers can no longer be polled, you do not want to receive notifications for all of your servers.

Navigating to the Alert Manager

Use the Alert Manager to create, edit, delete, enable, or disable alerts. You can access the Alert Manager in one of four ways:

- Settings Page (Recommended)
- Active Alerts Details
- All Active Alerts Resource
- Node Details

Settings Page (Recommended)

SolarWinds recommends using the Settings page to navigate to the Alert Manager.

1. Click **Settings**.
2. Under Alerts & Reports, click **Manage Alerts**.

All Active Alerts Resource

From the All Active Alerts resource, click **Manage Alerts** in the right side.

Active Alerts Details

From the Active Alerts Details page, click **Manage Alerts** in the Management resource.

Node Details

On the Node Details page, navigate to the **All Alerts this Object can trigger** resource.

Click **Manage Alerts**.

Creating New Alerts

SolarWinds provides an Alert Wizard to guide you through creating or editing alerts.

To create a new alert definition, navigate to the Alert Manager, and click **Add New Alert**.

You can also select an alert that is similar to the alert you want to create and click **Duplicate & Edit**.

Note: You can skip to different steps after you have saved an alert or if you clicked **Duplicate & Edit**.

Properties

Provide information about the alert, including its name, severity, how frequently you want to evaluate the conditions, and if you want to restrict access to the alert using account limitations.

See Setting Alert Properties for more information.

Trigger Condition

Use the trigger condition to define what event must occur to activate your alert. Trigger conditions can be as simple as a node going down or as complex as multiple SQL statements.

Note: While SolarWinds provides a method to create SQL conditions manually, SolarWinds support is not provided. Visit thwack, SolarWinds' community website, for support from other users.

See Setting Trigger Conditions and Building Complex Conditions for more information.

Reset Condition

Use the reset condition to define what must occur to remove an alert instance from the active alerts list. For example, the "Email me when a Node goes down" alert automatically resets when the node comes back up. You can use the built-in reset conditions or create your own.

See Setting Reset Conditions for more information.

Time of Day

Schedule when you want to monitor your network for the trigger conditions you created for the alert. You can create multiple schedules that control when an alert is enabled or disabled. For example, you can disable an alert during maintenance windows.

See Setting the Time of Day or Schedule for more information.

Trigger Actions

Use trigger actions to define what happens when the trigger conditions are met. By default, a triggered alert creates an entry in the Active Alerts resource with a configurable message.

All other trigger actions, such as Send an Email/Page or Write to a Log, must be configured.

See the following for more information:

- Setting Trigger Actions
- Available Alert Trigger Actions

Reset Actions

Use reset actions to perform specific tasks when an alert is no longer active, such as writing to the log that the issue has been acknowledged. Reset actions are usually used to notify others that the situation has been resolved or to write the resolution to a log file.

See Setting Reset Actions for more information

Summary

See Reviewing the Alert Summary for more information.

Setting Alert Properties

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

Enter the following information as necessary:

Name of alert definition

This is a required field. SolarWinds recommends a name that describes the condition and most visible alert action. For example, you can use "Email NetAdmins when router goes down" as the name of an alert. The name is displayed in the Alert Manager and can be used to sort your alerts. If you intend to create a large number of alerts, you may want to consider a naming convention that allows you to quickly scan through the Alert Manager.

Description of alert definition

Describe the alert. This is displayed on the Manage Alerts page, so important information should be near the front.

Enabled (On/Off)

Choose to evaluate the alert immediately after it is created and saved. The alert is enabled. If you are in the process of refining your alert, you may want to disable this alert until it is ready for use.

Evaluation Frequency

SolarWinds recommends using intervals longer than 1 minute to evaluate alert conditions. Shorter frequencies may put an undue burden on your network performance or computing resources.

If you elect to alert on an event, such as a changed IP address, the condition is not evaluated by frequency, but by when the change is reported based on the polling interval.

Reduce the evaluation frequency to decrease your poller and database loads.

Severity of Alert

This controls the appearance of the alert in the Active Alerts resource and allows you to group or filter alerts more easily.

Alert Custom Properties

These help organize your alerts. For example, you can create a "Responsible Team" custom property and use it to help audit who receives specific alerts. You must create a custom property for alerts before you can assign a custom property to an alert.

Use custom properties to group your alerts in the Alert Manager or to create reports about alerts.

Alert Limitation Category

Use this to restrict who can view the alerts. For example, managed service providers can restrict alerts to their specific customers. If you create a new limitation, go to **Settings > Users** and add the new limitation to the appropriate user accounts.

Setting Trigger Conditions

The trigger condition is the most complex step in creating an alert. Before you begin, you may want to revisit the Best Practices and Tips for Alerting topic. To see an example of completed trigger conditions, see the Alerting When a Server is Down topic.

Trigger conditions are built using child conditions that are evaluated in order. Child conditions are represented as a line item under the **Actual Trigger Condition**. You can have multiple trigger condition blocks with multiple child conditions.

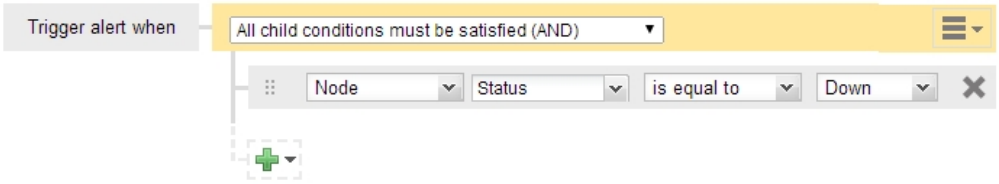
Filter your environment to just the objects you want to monitor in **The scope of alert**. Use the **Show List** link to view all of the objects that the alert monitors.

To set trigger conditions:

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

You can monitor all objects in your environment or filter your environment to a specific set of objects.

3. Create your trigger condition.



   a. Choose if the child conditions must be true or false to trigger the alert.
      - **All child conditions must be satisfied (AND)** - Every child condition must be met
      - **At least one child condition must be satisfied (OR)** - At least one child condition must be true
      - **All child conditions must NOT be satisfied** - Every child condition must be false
      - **At least one child condition must NOT be satisfied** - At least one child condition must be false
   b. Click the + sign to add child conditions.
      - **Add Single Value Comparison (Recommended)** - The child condition evaluates a single field, like Status
      - **Add Double Value Comparison** - The child condition evaluates two conditions, such as Status and OS
      - **Add And/Or block** - Adds a sub condition block

Tip: Use the **X** at the end of each child condition to delete it, or use the drop-down at the top of the block to delete the entire condition.

c. Select the object you want the child condition to evaluate, and then select which field you want to evaluate. In the example screenshot, the object is "*Node*" and the field is "*Status*".

   Tip: You can evaluate objects based on variables or macros.

d. Select how you want to compare the polled value of the field to the value entered here, and then enter the value. In the example screenshot, the comparison is "*is equal to*" and the value is "*Down*".

e. To use more complex conditions, such as evaluating when an application on a specific server is down and different application on another server is down, enable complex conditions under **Advanced options**. See Building Complex Conditions for more information, or visit thwack, SolarWinds' community website, for support from other users.

f. Choose how long the condition must exist before an alert is triggered. This prevents receiving alerts when the alert condition, such as high CPU utilization, occurs briefly or only once during a certain time period.

   - To immediately send an alert when the condition is met, clear any selection for **Condition must exist for more than**.
   - To wait before sending an alert, select **Condition must exist for more than**, and enter how long the condition must exist. This option prevents multiple alerts firing if the condition is temporary.

Setting Reset Conditions

Reset conditions prevent multiple alerts firing for the same alert instance. You can also create reset actions that occur when the reset conditions are met.

For example, you can create an alert that triggers when nodes in your lab go down. If node 192.168.4.32 goes down, the alert fires for that specific instance of the trigger condition and any escalation levels you create will continue until you acknowledge or reset the alert. Once the alert is acknowledged or reset, all trigger actions stop and a new alert fires the next time node 192.168.4.32 goes down.

Note: When the alert is reset, escalation actions are halted and the alert can fire again for the same alert instance.

Select one of the following reset conditions:

- **Reset this alert when trigger condition is no longer true (Recommended)**

  SolarWinds recommends using this reset condition. If the trigger condition is no longer true when the objects are next polled, this selection will automatically reset the alert.

  You may want to use the **Condition must exist for more than** option in the trigger conditions in conjunction with this reset condition. Trigger conditions that involve volatile components, such as high CPU utilization, can trigger excessively with this reset condition.

- **Reset this alert automatically after**

  Select this to reset an unacknowledged alert after a certain amount of time has passed even if the alert has not been acknowledged. If this interval is less than the amount of time you wait for different escalation levels, the escalation levels that occur after this interval do not fire.

  For example, if an alert has not been acknowledged after 48 hours and the trigger condition still exists, you can use this to retrigger your alert actions. The alert is reset and triggers as soon as the trigger condition is detected, which is as soon as the objects are polled for this example.

- **No reset condition - Trigger this alert each time the trigger condition is met**

  The alert fires each time the trigger conditions are met.

  For example, when the alert for node 192.168.4.32 going down fires, a new alert for 192.168.4.32 fires every time the node is down when it is polled.

- **No reset condition**

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

- **Create a special reset condition for this alert**

  Select this to build a specific reset condition.

  For example, you can choose to reset the condition when the node has been up for more than 10 minutes.

  See Setting Trigger Conditions or Building Complex Conditions for more information on creating conditions.

Setting the Time of Day or Schedule

You can configure when an alert monitors your network. By default, alerts monitor your network for changes all the time.

Note: Alerts must be enabled to allow schedules to run.

To schedule your alert:

1. Select **Specify time of day schedule for this alert**
2. Click **Add Schedule**.

You can have multiple schedules for a single alert. For example, you can schedule the alert to monitor your network during off hours, and disable the alert during your maintenance windows.

Enter the following information to schedule a monitoring period:

- **Schedule Name**

  This is not required, but may help you organize or troubleshoot your schedules. If you do not enter a name, a name is automatically generated from the time period.

- **Enable or Disable alert during following time period**

  If you choose to disable the alert, it is enabled all other times unless otherwise scheduled.

- **Frequency**

  Choose when to monitor on a high level, such as daily, weekly, or monthly.

- **Enable every**

  These options change based on the frequency.

  - ***If you selected Daily...***

    You can choose to enable or disable the alert every few days, up to every 31 days. You can also select specific business days. For example, you may want to disable network or disk activity alerts if you run daily, off-site backups of your critical data.

    - **Enter a time period**
    - To monitor or not for the entire 24 hour period, select **All Day**.
    - To monitor or not during a specific time period during the day, enter a time and click **Add Time Period**.
    - To monitor or not for a time period that spans midnight enter a time in the **From** field that is later in the day than the time in the **To** field. For example, to schedule an alert between 11PM to 3AM, enter 11PM (or 23:00) in the **From** field and 3AM (or 3:00) in the **To** field.

  - ***If you selected Weekly...***

    Choose which days the alert is enabled or disabled. You may want to disable alerts during a weekly maintenance window.

    - **Enter a time period**
    - To monitor or not for the entire 24 hour period, select **All Day**.
    - To monitor or not during a specific time period during the day, enter a time and click **Add Time Period**.
    - To monitor or not for a time period that spans midnight enter a time in the **From** field that is later in the day than the time in the **To** field. For example, to schedule an alert between 11PM to 3AM, enter 11PM (or 23:00) in the **From** field and 3AM (or 3:00) in the **To** field.

- ***If you selected Monthly...***

  Choose which months the alert is enabled or disabled. This option is useful when you have quarterly or monthly maintenance windows.

  Choose either a specific date or a day.

  - **Enter a time period**
  - To monitor or not for the entire 24 hour period, select **All Day**.
  - To monitor or not during a specific time period during the day, enter a time and click **Add Time Period**.
  - To monitor or not for a time period that spans midnight enter a time in the **From** field that is later in the day than the time in the **To** field. For example, to schedule an alert between 11PM to 3AM, enter 11PM (or 23:00) in the **From** field and 3AM (or 3:00) in the **To** field.

- **Starting on**

  Choose a date to being the schedule.

  - **Right now** - Start the schedule immediately.
  - **Specific Date** - Select a time and day to begin the schedule.

- **Ending on**

  Choose and end date for the schedule, if necessary.

3. Click **Add Schedule** to create the schedule.

Setting Trigger Actions & Escalation Levels

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

Trigger Actions

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

To add a trigger action:

1. Click **Add Action**.
2. Select an action from the list.

   See Alert Trigger Actions for a complete list of available actions.
3. Click **Configure Action**.
4. Enter the necessary information for the action.

   Each action requires different information. Select from the list of Alert Trigger Actions for more information per action.

   Some actions require extra configuration steps, specific information, or special software. See Preconfiguration Tasks.

   Each action has the following sections:

   - **Name of action** - This is not required, but can make it easier to organize your Trigger actions.
   - **Time of Day...** - You can choose different actions to occur at different times of the day or month. For example, if you want to send a page, you might send it to a different person on weekends or holidays than during the week.
   - **Execution settings** - You can select both options, neither option, or a single option.
     - Do not execute this action if the alert has been acknowledged already (Recommended)
     - Repeat this action every X minutes until the alert is acknowledged
5. Click **Add Action**.

Escalation Levels

Escalation levels in Orion platform products refer to user-defined time intervals between when an alert is activated and when a user acknowledges that alert. You can configure the alert to perform different actions per escalation level.

Escalation Level 1 contains all initial actions that you want to occur when the trigger conditions are met and the alert activates.

Escalation Levels 2 and above include all actions you want to occur if no one acknowledged the alert during the previous escalation levels.

For example, if an alert for a critical server activates and all of the recipient or first-level responders are out for training and do not acknowledge the alert, then the actions fire in the second escalation level. These actions may include emailing managers or other backup staff.

To escalate alerts:

1. In an existing alert, click **Trigger Actions**.
2. Below the action, click **Add Escalation Level**.
3. Choose how long you want to wait after the previous escalation level before performing the actions in the new escalation level.
4. Enter new actions in this escalation level.

You can copy all of the actions as Reset Actions to record that the issue has been acknowledged or resolved. Click **Copy Actions to Reset Actions Tab**.

Setting Reset Actions

Choose actions that occur when the reset conditions are met and the alert is no longer active.

To add a reset action:

1. Click **Add Action**.
2. Select an action from the list.

   See Alert Actions for a complete list of available actions.

3. Click **Configure Action**.
4. Enter the necessary information for the action.

   Each action requires different information. Select from the list of Alert Actions for more information per action.

   Some actions require extra configuration steps, specific information, or special software. See Preconfiguration Tasks.

Each action has the following sections:

- **Name of action** - This is not required, but can make it easier to organize your Trigger actions.
- **Time of Day...** - You can choose different actions to occur at different times of the day or month. For example, if you want to send a page, you might send it to a different person on weekends or holidays than during the week.
- **Execution settings** - You can select both options, neither option, or a single option.
  - Do not execute this action if the alert has been acknowledged already (Recommended)
  - Repeat this action every X minutes until the alert is acknowledged

5. Click **Add Action**.

To perform the same actions as when the alert was triggered, click **Copy Actions From Trigger Actions Tab**. Use the copied trigger actions as a base and modify them to reflect that the alert is no longer active.

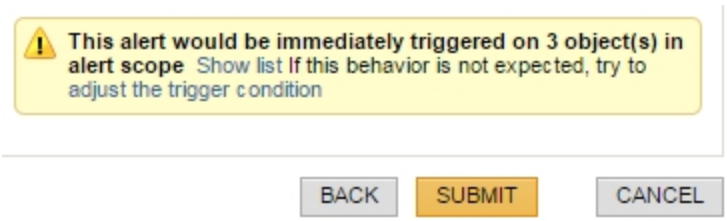
Reviewing the Alert Summary

The Summary tab allows you to check your alert definition before you save any changes.

To modify any section, click **Edit** next to that section.

To integrate your alerts with other SolarWinds products, such as AlertCentral or Web Help Desk, expand Alert Integration. Select as many variables as you need to ensure that the variables are correctly translated for the other products to use.

Before you click **Submit**, review the information box above it. This box lists the number of objects that will trigger the alert immediately based on your current trigger condition.



Commonly Created Alerts

The following is a list of frequently created alerts. The topics walk you through the easiest method to create the alert and include tips on how to build more complex alerts.

Alert Me When a Server is Down

Use the following procedure to create an alert that writes to a log and emails a message to you when a Windows server goes down.

To create a new alert:

1. Click **Settings > Manage Alerts**.
2. Search for "Email me when a Node goes down".
3. Select the check box next to the alert, and click **Duplicate & Edit**.
4. Enter a name for the alert, such as "Notify me when a Node goes down".
5. Enable the alert.
6. Click **Trigger Condition** or **Next**.
7. In **The scope of alert**, select **Only following set of objects.**
8. Select *Node Machine Type is equal to Windows 2008 Server* as the child condition.>

   Tip: You can further refine your scope by entering another AND condition. For example, you can enter *Node IP Address starts with 10.10.45* to restrict the scope of the alert to a specific subnet.

9. The **actual trigger condition** should be *Node Status is equal to Down*.

   Tip: Select and enter a value for **Condition must exist for more than** to prevent being alerted when a node enters the down state frequently within a set amount of time. This will prevent you from receiving alerts until the node has been in the down state for longer than the time you have selected.

   Ninja Tip: You can further suppress alerts by enabling complex conditions in the Advanced options. This allows you to choose to wait until multiple nodes are down before triggering a single alert.

10. Click **Reset Condition**. The default action should be to reset the alert when the node is up.
11. Click **Trigger Actions**.
12. Under **Trigger Actions**, click **Add Action**.
13. Select **Log the Alert to a file**, and then click **Configure Action**.
    a. Click **Browse** (**…**) to open the default directory.
    b. Browse to an appropriate folder, and then type **ExampleAlertLog** as the alert log file name.
    c. Click **Save**.
    d. In the **Message** text box, type *Node ${N=SwisEntity;M=Caption} is currently down.*
    e. Click **Add Action**.
14. Click **Add Escalation Level**, and enter 5 minutes to wait for 5 minutes before escalating to the next level.
15. Click **Add Action** in Escalation Level 2, and select **Send an Email/Page**. Click **Configure Action**.
    a. Enter your email as the recipient.
    b. Add a message.
    Tip: You can use variables to customize your message. You can also use a variable that allows you to acknowledge an alert from email (*${N=Alerting;M=AcknowledgeUrl}*).
    c. Enter your SMTP server information if you have not already done so.
    Tip: You can enter a default SMTP server that is used for all your email in **Settings > Configure Default Send Email Action**.
    d. Go to **Execution settings** to click **Add Action**.
    e. Click **Add Action**.
16. Click **Copy Actions to Reset Actions Tab**, and then click **Next**.
17. Click **Edit** next to your logging action, and modify your message to *Node ${N=SwisEntity;M=Caption} is back up*.

18. Click **Edit** next to your email action, and modify your message. You can also delete the email if you do not want to know if the situation has been resolved.
19. Click **Summary**, and review your alert definition.
20. Click **Submit**.

Use a Custom Property in Alerts

The following example creates multiple alerts using the *NodeLocation* custom property defined in Creating a Custom Property. An alert triggers when a node goes down. Upon triggering, the alert will write to a local log file, send a syslog message, and send an SNMP trap.

Note: The **${**variable**}** syntax is required for variables. For more information on the use of variables, see Orion Variables and Examples.

To create a new alert:

1. Click **Settings > Manage Alerts**.
2. Select the check box next to **Node is down,** and then click the **Duplicate & Edit** button.
3. Click **Trigger Condition**, and add a child condition. A child condition should already exist for a node being down.
4. Select the node object, and choose **NodeLocation** in the field drop-down. Enter a comparison and value.
5. Click the **Trigger Actions**, and then click **Add Action**.
6. Select **Log the Alert to a file**, and then click **Configure Action**.
    a. Enter the log filename in the **Alert Log Filename** field.
    b. In the **Message** text box, type the following:
    Node ${N=SwisEntity;M=Caption} is currently down.
    c. Click **Add Action**.

7. Click **Add Action**, and select **Send a Syslog Message**. Click **Configure Action**.
    a. Type **127.0.0.1** as the **Hostname or IP Address of the Syslog Server**, and then type the following in the **Message** field:
    Node ${N=SwisEntity;M=Caption} is currently down.
    b. Click **Add Action**.
8. Click **Add Action**, and select **Send SNMP Trap**. Click **Configure Action**.
    a. Type **127.0.0.1** as the **SNMP Trap Destination**, and then type the following in the **Alert Message** field:
    Node ${N=SwisEntity;M=Caption} is currently down.
    b. Click **Next**.
    c. Click **Add Action**.
9. Click **Summary**, and click **Submit**.

You can test your alert, and view the results of each of your alert actions as follows. See Testing Alerts for more information.

- You can view results of your Syslog message action in the Web Console or through the Syslog Viewer on your SolarWinds Orion server.
- To view the results of your SNMP Trap action, click **Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer**.

Viewing Triggered Alerts

To view active triggered alerts, click **Alerts** in the Home view.

You can also add the **All Active Alerts** resource to any view.

Acknowledging Alerts

When an alert has triggered and becomes active, you can then acknowledge it. After an alert is acknowledged, alert actions in higher escalation levels are halted and the time it was acknowledged and the account that acknowledged it is recorded. You can also add notes that other users can read.

Depending on your organization, acknowledging an alert can have different purposes outside of halting further notifications. The most common purposes are to provide an audit trail or to prevent multiple people from working on the same issue.

To acknowledge an alert:

1. Log in to the Orion Web Console using an account that has been granted alert acknowledgment privileges.
2. Click **Alerts** on the Views toolbar.
3. Click **Acknowledge** next to the alerts you want to acknowledge.

Tip: Depending on how you configure the email, you can acknowledge an alert directly from an email notification.

To group active alerts:

1. Use the Group by drop-down to select how you want your alerts grouped.
2. Use the double-arrows on the left to expand or contract the Group by control.

To filter active alerts:

1. Click the filter icon on the column by which you want to filter alerts.
2. Enter your filter term. The filter appears above the grid.
3. Click the **X** next to the filter term to remove the filter.

To hide acknowledged alerts:

1. Click **More** on the right of the grid.
2. Select **Hide Acknowledged Alerts**.

Testing Alerts

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

Testing Trigger Conditions

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

Testing Trigger or Reset Actions within the Alert

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

Note: The Send Email/Page action does not have to fire. You can view what the message will look like when the trigger or reset action fires without sending a message.

1. Open an alert you want to test.
2. Click **Trigger Actions** or **Reset Actions**.
3. Click **Simulate** next to the alert action you want to test.
4. Select an object to resolve any variables you have used in your alert action.
5. Click **Execute**. To test email actions without sending an email, click **Simulate**.

Testing Actions in the Action Manager

You can also test actions in the **Action Manager**. This is part of the **Alert Manager**.

Note: The Send Email/Page action does not have to fire. You can view what the message will look like when the trigger or reset action fires without sending a message.

1. Select the action you want to test.
2. Click **Test.**

3. Select an object to resolve any variables you have used in your alert action.
4. Click **Execute**. To test email actions without sending an email, click **Simulate**.

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

- To view the results of your email alert action, open **EvaluationAlertLog** in your Orion folder, typically **<Volume:>\Program Files\SolarWinds\Orion**.
- To view results of your Syslog message action, click **Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Syslog Viewer**.
- To view the results of your Syslog message action, click **Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer**.

Managing Alerts

You can add, edit, enable, disable, import, export, and delete alerts from the Alert Manager.

Adding and Editing Alerts

Use the **Add New Alert** or the **Duplicate & Edit** buttons to create new alerts. Select an alert and use the **Edit Alert** button to edit it.

Use the following topics to learn more about creating and editing alerts.

- Creating New Alerts
- Commonly Created Alerts

Enabling and Disabling Alerts

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

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

Exporting or Importing Alerts

You can use the Export/Import button to export or import alert definition files. Alerts are exported to XML and can only be imported from XML.

Important: Confidential information, such as SMTP server credentials, may be included with the exported XML file. Please check the exported file for such information or delete the information from the alert before you export it.

SolarWinds customers share their customized alerts in the SolarWinds thwack community. Visit thwack.solarwinds.com, download and import alerts by your peers. For example, to import an alert that notifies you if Cisco ASA fails over, see the following article: https://thwack.solarwinds.com/docs/DOC-170819.

Deleting Alerts

Use the **Delete** button to remove an alert.

Building Complex Conditions

Complex conditions are generally enabled by users who are comfortable with building normal trigger conditions or who have trialed alerts using the normal trigger conditions and require more control over the trigger conditions to better refine the environmental conditions that trigger an alert.

Important: Do not use complex conditions until you have tested the trigger conditions individually. Creating an alert with complex conditions without testing it may prevent you from receiving important alerts.

To enable complex conditions:

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

You can use complex conditions to do the following:

- Wait for multiple objects to meet the trigger condition before alerting
- Evaluate multiple condition blocks
- Evaluate multiple object types

Waiting for Multiple Objects to Meet the Trigger Condition

Once you have enabled complex conditions, you can choose to trigger alerts only when multiple objects meet the trigger condition.

After you have enabled complex conditions, the following option is available in your trigger condition:

This setting then combines all alerts that would be sent for each object into a single alert.

Important: Do not use this setting until you are confident that the trigger condition is correct. This setting can prevent important alerts from triggering.

To trigger an alert only when multiple objects meet the trigger condition:

1. Enable complex conditions.
2. In the trigger condition, select **Alert can be triggered if**.
3. Enter how many objects must meet the trigger condition before sending an alert.

Evaluating Multiple Condition Blocks

You can use complex conditions to evaluate multiple condition blocks, or sections. For example, you may want to create an alert when an application is down and when your fail-over server is active for more than an hour.

How Condition Blocks Are Evaluated

Condition blocks are evaluated simultaneously. Take the following example:

```
(Condition A) & (Condition B) & (Condition C)
```

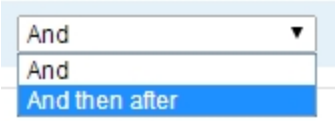
The condition blocks are evaluated at the same time. If they are all true based on the conditions, the alert triggers. If Condition A and Condition C are true and Condition B is not true, the alert does not fire.

Condition blocks are evaluated using variations of AND, so the trigger condition in each section must be met.

A condition block can be evaluated at a different time than other condition blocks. In the example where you want to be alerted if the backup system is active for more than an hour, you can choose to wait an hour after the primary condition block, where the application going down is the trigger condition, before evaluating whether the backup system is still active.

To choose to wait before evaluating a secondary condition block:

1. Enable complex conditions.
2. Click **Add Section**.
3. Select **And then after** from the drop-down menu between the two condition sections.



4. Choose how long to wait before evaluating the next section.
5. Create the next condition block.

Evaluating Multiple Object Types

To evaluate multiple object types, you should use complex conditions. Complex conditions can be used to alert on different object types within the same alert. For example, you can create an alert to notify you when IIS is down and the free space on the volume is less than 30 GB.

To choose different object types:

1. Enable complex conditions.
2. Click **Add Section**.
3. Choose a different value in **I want to alert on**.

Available Alert Actions

Orion platform products provide a variety of actions to signal an alert condition on your network. For information on configuring each action, refer to the following list.

The following actions are available:

- Changing Custom Property
- Dialing Paging or SMS Service
- Emailing a Web Page
- Executing an External Program
- Executing a Visual Basic Script
- Logging an Alert to a File
- Logging an Alert to the NPM Event Log
- Managing the resource allocation of a virtual machine
- Deleting a snapshot of a virtual machine
- Moving a virtual machine to a different host
- Moving a virtual machine to a different storage
- Pausing a virtual machine
- Powering off a virtual machine
- Powering on a virtual machine
- Restarting a virtual machine
- Suspending a virtual machine
- Taking a snapshot of a virtual machine
- Playing a Sound
- Restarting IIS Site or Application Pools
- Sending a Windows Net Message
- Sending an SNMP Trap
- Using Get or Post URL Functions
- Sending a Syslog Message
- Sending an Email/Page
- Setting Custom Status

- Using Text to Speech Output
- Logging an Alert to the Windows Event Log

Changing Custom Property

Use the following procedure to modify a custom property through an alert action.

To configure a custom property action for an alert:

1. When editing or adding an alert, click **Add Action**.
2. Select the **Change Custom Property** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Custom Property Settings:**
    a. Select the **Custom Property Name** from the drop down list.
    b. Enter a **Custom Property Value** in the field provided.
    c. Optionally click **Insert Variable** to add variables using the following procedure:
        i. Select a **Variable Category**, and then select the variable to add.
        ii. To define a SQL variable, check **Define SQL Variable**.
        iii. Click **[+]** next to the name of a variable to add one or more variables to the **Custom SQL Variable** window.
        iv. When done, click **Insert Variable**.

6. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action.** If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

7. Expand **Execution Settings**.
    a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
8. When done, click **Add Action**.

Dialing Paging or SMS Service

If NotePager Pro is installed, SolarWinds can be configured to communicate alerts using paging and SMS services. For more information about installation and configuration, see "SolarWinds Network Performance Monitor Integration" at www.notepage.net.

Emailing a Web Page

The **Edit E-mail Web Page Action** window includes several sections for configuration. The following procedure configures an e-mail URL action for an alert.

To configure an email web page action for an alert:

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Email a Web Page** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Recipients**:
    a. Complete the **To**, **CC**, and **BCC** fields.
    b. You can optionally edit sender details by expanding **[+] Sender Details** and editing the **Name of Sender** and the **Reply Address**. **Note:** You must provide at least one email address in the **To** field, and multiple addresses must be separated with commas. Some pager systems require a valid reply address to complete the page.
5. Expand **Message**.
    a. Enter the **Subject** and **Message** of your alert trigger email/page. **Note:** Messaging is disabled if both the **Subject** and **Message** fields

are empty.

b. Optionally click **Insert Variable** to add variables using the following procedure:

   i. Select a **Variable Category**, and then select the variable to add.

   ii. ***To define a SQL variable,*** check **Define SQL Variable**.

   iii. Click **[+]** next to the name of a variable to add one or more variables to the **Custom SQL Variable** window.

   iv. When done, click **Insert Variable**.

c. For the **Optional Web Server Authentication** section, select **User currently logged in**, **Another user**, or **No user defined**.

6. Expand **SMTP Server**.

   a. Enter the Name of the **SMTP Server**.

   b. Enter the **Hostname or IP Address of your SMTP Server** and the designated **SMTP Port Number**.
   Note: The SMTP server hostname or IP address field is required. You cannot send an email/page alert without identifying the SMTP server.

   c. To use SSL/TLS encryption for your alert email, check **Use SSL**.

   d. If your SMTP server requires authentication, check **This SMTP Server requires Authentication**.

   e. Choose a **Secondary SMTP Server** from the list, if desired.

7. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule.

   a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action.** If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

8. Expand **Execution Settings**.

   a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action**

every X minutes until the alert is acknowledged. If you choose the latter, specify the frequency to have this action repeated.

9. When done, click **Add Action**.

Executing an External Program

There are several circumstances where you may want to execute a program when a specific network event occurs. Use the **Edit Execute Program Action** window to specify the executable that should be started when the specified alert is triggered or reset, as shown in the following procedure.

External programs selected for this action must be executable using a batch file called from the command line. Programs executed this way run in the background. However, you can set the SolarWinds Alerting Engine Service to **Interact with Desktop**. SolarWinds recommends that scripts and batch files be placed on the root of c:\ to simplify the path for the batch file.

To configure an alert to execute an external program:

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Execute an External Program** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Execute an External Program settings**:
    a. Enter the **Network path to external program** in the field provided. **For example:** Use `c:\test.bat`, where `c:\` is the disk on your main Orion poller and `test.bat` is your external program to be executed.
    b. Select either **Define User** or **No User Defined** for *Optional Windows Authentication*
5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action.** If you choose the latter, Click **Add**

Schedule and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

6. Expand **Execution Settings**.
    a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
7. When done, click **Add Action**.

Executing a Visual Basic Script

In some situations, you may want to execute a Visual Basic (VB) script when a network event occurs. The **Edit Execute VB Script Action** window is used to specify the name and complete path of the file that shall be executed when the specified alert is triggered or reset.

To configure alerts to execute a Visual Basic (VB) script:

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Execute an External VB Script** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Execute an External VB Script settings**:
    a. Select a **VB Script Interpreter** from the drop down list.
    b. Enter the **Network path to the external VB Script** in the field provided.
    For example: Use `c:\test.vbs`, where `c:\` is the disk on your main Orion poller and `test.vbs` is your external VB Script to be executed.
    c. Select either **Define User** or **No User Defined** for *Optional Windows Authentication*

5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule.

    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action.** If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

6. Expand **Execution Settings**.

    a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.

7. When done, click **Add Action**.

Logging an Alert to a File

SolarWinds can be configured to log alerts to a designated file. The following procedure logs an alert to a designated file.

To configure an alert log file action for an alert:

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Log the Alert to a File** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.

4. Under **Log to File Settings**:
    a. Enter the log filename in the **Alert Log Filename** field.
    b. Optionally click **Insert Variable** to add variables using the following procedure:
        i. Select a **Variable Category**, and then select the variable to add.
        ii. To define a SQL variable, check **Define SQL Variable**.
        iii. Click **[+]** next to the name of a variable to add one or more variables to the **Custom SQL Variable** window.
        iv. When done, click **Insert Variable**.
    c. Enter a maximum log file size in MB (0 = unlimited).
    d. Enter the **Message** of your alert trigger in the field provided.
    e. Optionally click **Insert Variable** to add variables using the following procedure:
        i. Select a **Variable Category**, and then select the variable to add.
        ii. To define a SQL variable, check **Define SQL Variable**.
        iii. Click **[+]** next to the name of a variable to add one or more variables to the **Custom SQL Variable** window.
        iv. When done, click **Insert Variable**.
5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action.** If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

6. Expand **Execution Settings**.
    a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
7. When done, click **Add Action**.

Logging an Alert to the NPM Event Log

You can specify that an alert should be logged to the NetPerfMon (NPM) Event Log either on the SolarWinds Orion server or on a remote server. The following procedure logs an alert to the NPM Event Log on a designated server.

To configure alert logging to the NetPerfMon Event Log:

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Log the Alert to the NetPerfMon Event Log** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Log the Alert to the NetPerfMon Event Log settings**:
    a. Enter the **Message** of your alert trigger in the field provided.
    b. Optionally click **Insert Variable** to add variables using the following procedure:
        i. Select a **Variable Category**, and then select the variable to add.
        ii. To define a SQL variable, check **Define SQL Variable**.
        iii. Click **[+]** next to the name of the variable to add one or more variables to the **Custom SQL Variable** window.
        iv. When done, click **Insert Variable**.

5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action.** If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
6. Expand **Execution Settings**.
    a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
7. When done, click **Add Action**.

Managing the resource allocation of a virtual machine

This alert management action is available if the integration with Virtualization Manager is enabled.

To configure an alert to change the allocated resources on a virtual machine, perform the following procedure:

1. When you are editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select **Manage VM - Change CPU/Memory Resources**, and then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.

4. Under **Select Virtual Machine to Manage Resource Allocation**, specify the virtual machine on which you want to adjust the number of CPUs, the memory capacity, or both.
    a. To change the resource allocation of the virtual machine that triggered the alert, click **Execute this action on the VM that triggered this alert**.
    Note: This option is only available if the alert is built to trigger for virtual machines.
    b. To change the resource allocation of a different virtual machine, click **Select specific VM from my environment**, and then search for the virtual machine on which you want to execute the action.
5. To power off the virtual machine before changing the resource allocation, and then power it on again after the resource allocation has been changed, select the relevant option. If the option is not selected, the action will be performed live on the virtual machine.
6. Under **Specify New Resources**, specify whether you want to add more resources to the virtual machine, or replace the existing resources with new resources, and then specify the parameters of the new resource or resources.
    a. Select **Number of processors**, and then specify the number of processors to allocate to the virtual machine.
    b. Select **Memory**, and then specify the memory capacity to allocate to the virtual machine.
7. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, click **Add Schedule**, enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

8. Expand **Execution Settings**.
    a. Select either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
9. When done, click **Add Action**.

The alert action is now configured in a way that the specified CPU and memory resources will be allocated to the virtual machine when the alert is triggered.

Deleting a snapshot of a virtual machine

This alert management action is only available if the integration with Virtualization Manager is enabled.

To configure an alert to delete a snapshot of a virtual machine, perform the following procedure:

1. When you are editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select **Manage VM - Delete Snapshot**, and then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Select Virtual Machine to Delete Snapshot**, specify the virtual machine from which you want to delete a snapshot.
    a. To delete a snapshot of the virtual machine that triggered the alert, click **Execute this action on the VM that triggered this alert**.
    Note: This option is only available if the alert is built to trigger for virtual machines.
    b. To delete a snapshot of a different virtual machine, click **Select specific VM from my environment**, and then search for the virtual machine on which you want to execute the action.

5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, click **Add Schedule**, enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
6. Expand **Execution Settings**.
    a. Select either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
7. When done, click **Add Action**.

The alert action is now configured in a way that the snapshot of the specified virtual machine will be deleted when the alert is triggered.

Moving a virtual machine to a different host

This alert management action is only available if the integration with Virtualization Manager is enabled.

To configure an alert to move a virtual machine to a different host, perform the following steps:

1. When you are editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select **Manage VM - Move to a Different Host**, and then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.

4. Under **Select Virtual Machine to Move to a Different Host**, specify the virtual machine that you want to move.
    a. To move the virtual machine that triggered the alert, click **Execute this action on the VM that triggered this alert**.
    Note: This option is only available if the alert is built to trigger for virtual machines.
        - To apply the action only to virtual machines of a specific vendor, select the relevant option, and then specify whether you want to perform to action on Hyper-V or VMware virtual machines.
    b. To move a different virtual machine, click **Select specific VM from my environment**, and then search for the virtual machine on which you want to execute the action.
5. To power off the virtual machine before moving it to a different host, and then power it on again after the action has been completed, select the relevant option. If the option is not selected, the action will be performed live on the virtual machine.
6. Under **Select Target Host**, search for the host where you want to move the selected virtual machine.
7. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, click **Add Schedule**, enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
8. Expand **Execution Settings**.
    a. Select either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
9. When done, click **Add Action**.

The alert action is now configured in a way that the specified virtual machine will be moved to a different host when the alert is triggered.

Moving a virtual machine to a different storage

This alert management action is only available if the integration with Virtualization Manager is enabled.

To configure an alert to move virtual machine data to a different storage, perform the following steps:

1. When you are editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select **Manage VM - Move to a Different Storage**, and then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Select Virtual Machine to Move to a Different Storage**, specify the virtual machine that you want to move.
    a. To move the virtual machine that triggered the alert, click **Execute this action on the VM that triggered this alert**.
    Note: This option is only available if the alert is built to trigger for virtual machines.
        - To apply the action only to virtual machines of a specific vendor, select the relevant option, and then specify whether you want to perform to action on Hyper-V or VMware virtual machines.
    b. To move a different virtual machine, click **Select specific VM from my environment**, and then search for the virtual machine on which you want to execute the action.
5. To power off the virtual machine before moving it to a different storage, and then power it on again after the action has been completed, select the relevant option. If the option is not selected, the action will be performed live on the virtual machine.

6. Under **Select Target Datastore**, search for the datastore where you want to move the selected virtual machine.
    a. In a VMware environment, select one of the available datastores.
    b. In a Hyper-V environment, select one of the available datastores, and then click either **Use the default location** to move the virtual machine to the default location of the datastore, or click **Specify custom path**, and then enter a custom location.
7. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, click **Add Schedule**, enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
8. Expand **Execution Settings**.
    a. Select either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
9. When done, click **Add Action**.

The alert action is now configured in a way that the specified virtual machine will be moved to a different datastore when the alert is triggered.

Pausing a virtual machine

This alert management action is only available if the integration with Virtualization Manager is enabled.

This action can only be configured for Hyper-V virtual machines.

To configure an alert to pause a virtual machine, perform the following steps:

1. When you are editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select **Manage VM - Pause**, and then click **Configure Action**.

3. Enter a name for the action in the **Name of Action** field.
4. Under **Select Virtual Machine to Pause**, specify the virtual machine that you want to pause.
    a. To pause the virtual machine that triggered the alert, click **Execute this action on the VM that triggered this alert**.
    Note: This option is only available if the alert is built to trigger for virtual machines.
    b. To pause a different virtual machine, click **Select specific VM from my environment**, and then search for the virtual machine on which you want to execute the action.
5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, click **Add Schedule**, enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
6. Expand **Execution Settings**.
    a. Select either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
7. When done, click **Add Action**.

The alert action is now configured in a way that the specified virtual machine will be paused when the alert is triggered.

Powering off a virtual machine

This alert management action is only available if the integration with Virtualization Manager is enabled.

To configure an alert to power off a virtual machine, perform the following steps:

1. When you are editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select **Manage VM - Power Off**, and then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Select Virtual Machine to Power Off**, specify the virtual machine that you want to power off.
    a. To power off the virtual machine that triggered the alert, click **Execute this action on the VM that triggered this alert**.
    Note: This option is only available if the alert is built to trigger for virtual machines.
    b. To power off a different virtual machine, click **Select specific VM from my environment**, and then search for the virtual machine on which you want to execute the action.
5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, click **Add Schedule**, enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
6. Expand **Execution Settings**.
    a. Select either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
7. When done, click **Add Action**.

The alert action is now configured in a way that the specified virtual machine will be powered off when the alert is triggered.

Powering on a virtual machine

This alert management action is only available if the integration with Virtualization Manager is enabled.

To configure an alert to power on a virtual machine, perform the following steps:

1. When you are editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select **Manage VM - Power On**, and then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Select Virtual Machine to Power On**, specify the virtual machine that you want to power on.
    a. To power on the virtual machine that triggered the alert, click **Execute this action on the VM that triggered this alert**.
    Note: This option is only available if the alert is built to trigger for virtual machines.
    b. To power on a different virtual machine, click **Select specific VM from my environment**, and then search for the virtual machine on which you want to execute the action.
5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, click **Add Schedule**, enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
6. Expand **Execution Settings**.
    a. Select either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
7. When done, click **Add Action**.

The alert action is now configured in a way that the specified virtual machine will be powered on when the alert is triggered.

Restarting a virtual machine

This alert management action is only available if the integration with Virtualization Manager is enabled.

To configure an alert to restart a virtual machine, perform the following steps:

1. When you are editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select **Manage VM - Reboot**, and then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Select Virtual Machine to Reboot**, specify the virtual machine that you want to reboot.
    a. To reboot the virtual machine that triggered the alert, click **Execute this action on the VM that triggered this alert**.
    Note: This option is only available if the alert is built to trigger for virtual machines.
    b. To reboot a different virtual machine, click **Select specific VM from my environment**, and then search for the virtual machine on which you want to execute the action.
5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, click **Add Schedule**, enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
6. Expand **Execution Settings**.
    a. Select either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
7. When done, click **Add Action**.

The alert action is now configured in a way that the specified virtual machine will be restarted when the alert is triggered.

Suspending a virtual machine

This alert management action is only available if the integration with Virtualization Manager is enabled.

To configure an alert to suspend a virtual machine, perform the following steps:

1. When you are editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select **Manage VM - Suspend**, and then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Select Virtual Machine to Suspend**, specify the virtual machine that you want to suspend.
    a. To suspend the virtual machine that triggered the alert, click **Execute this action on the VM that triggered this alert**.
    Note: This option is only available if the alert is built to trigger for virtual machines.
    b. To suspend a different virtual machine, click **Select specific VM from my environment**, and then search for the virtual machine on which you want to execute the action.
5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, click **Add Schedule**, enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
6. Expand **Execution Settings**.
    a. Select either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.

7. When done, click **Add Action**.

The alert action is now configured in a way that the specified virtual machine will be suspended when the alert is triggered.

Taking a snapshot of a virtual machine

This alert management action is only available if the integration with Virtualization Manager is enabled.

To configure an alert to take a snapshot of a virtual machine, perform the following steps:

1. When you are editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select **Manage VM - Take Snapshot**, and then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Select Virtual Machine to Take Snapshot**, specify the virtual machine of which you want to take a snapshot.
    a. To take a snapshot of the virtual machine that triggered the alert, click **Execute this action on the VM that triggered this alert**.
    Note: This option is only available if the alert is built to trigger for virtual machines.
    b. To take a snapshot a different virtual machine, click **Select specific VM from my environment**, and then search for the virtual machine on which you want to execute the action.
5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action**. If you choose the latter, click **Add Schedule**, enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

6. Expand **Execution Settings**.
    a. Select either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
7. When done, click **Add Action**.

The alert action is now configured in a way that a snapshot will be taken of the specified virtual machine when the alert is triggered.

Playing a Sound

SolarWinds can be configured to play a sound upon alert trigger or reset. This alert action is frequently used in NOC environments. The SolarWinds Desktop Notification client must be installed on each computer that you want to play a sound. The following procedure configures a sound to play for an alert.

To configure a play sound action for an alert:

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard**.**
2. Select the **Play a Sound** option, and then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Play a sound settings**:
    a. If not installed, click **Download our desktop notification client** to download and install the notification client.
        i. From the notification client, select an alert sound.
    b. Optionally click **Insert Variable** to insert variables into the message body:
        i. Select a **Variable Category**, and then select the variable to add.
        ii. To define a SQL variable, check **Define SQL Variable**.
        iii. Click **[+]** next to the name of a variable to add one or more variables to the **Custom SQL Variable** window.
        iv. When done, click **Insert Variable**.

5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.

    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action.** If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

6. Expand **Execution Settings**.

    a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.

7. When done, click **Add Action**.

Restarting IIS Site or Application Pools

The following steps configure an alert to Restart an IIS Site/Application Pool on the trigger or reset action.

To configure SolarWinds to Restart an IIS Site/Application Pool upon alert:

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard**.**
2. Select the **Restart IIS Site/Application Pool** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Expand **Restart IIS Site/Application PoolSettings**.

    a. Select the **IIS Action to Perform** from the drop down list.

    b. Specify the Site/Application Pool to Use, either **Taken from alert trigger** or **Use a different IIS Server**.
    Note: If selecting **Use a different IIS Server**, enter the **IIS Server** and the **Site/Application Pool** from the drop down lists.

5. Expand **Time of Day**.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action.** If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
6. Expand **Execution Settings**.
    a. Select either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
7. Click **Add Action**.

Sending a Windows Net Message

Alerts can be configured to display a pop-up Windows Net Message either on a specific computer or on all computers in a selected domain or workgroup. The following steps configure Windows Net messaging for triggered or reset alerts.

Note: The only operating systems supporting Windows Net Messaging on which SolarWinds supports SolarWinds installations are Windows Server 2003 and Windows XP. SolarWinds only supports evaluation installations of SolarWinds on Windows XP.

To send a Windows Net message upon alert:

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Send Net Message** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Send a Net Message settings**:
    a. Optionally check **Send to all Computers in the Domain or Workgroup**.

b. Enter Computer Name or IP address in the field provided.
Note: You can enter multiple computers or IP addresses by separating them with commas.

c. Enter the **Message** of your alert trigger in the field provided.

d. Optionally click **Insert Variable** to add variables using the following procedure:

i. Select a **Variable Category**, and then select the variable to add.

ii. To define a SQL variable, check **Define SQL Variable**.

iii. Click **[+]** next to the name of a variable to add one or more variables to the **Custom SQL Variable** window.

iv. When done, click **Insert Variable**.

5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.

a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action.** If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

6. Expand **Execution Settings**.

a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.

7. When done, click **Add Action**.

Sending an SNMP Trap

The following steps configure an alert to send an SNMP trap on the trigger or reset action.

To send an SNMP trap:

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Send SNMP Trap** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Send SNMP Trap Message**:
    a. Enter **SNMP Trap Destinations** in the field provided.
    Note: Multiple IP Addresses should be separated by commas or semicolons.
    b. Select a **Trap Template** from the drop down lists.
5. Enter the **Message** of your alert trigger in the field provided.
    a. Optionally click **Insert Variable** to add variables using the following procedure:
        i. Select a **Variable Category**, and then select the variable to add.
        ii. To define a SQL variable, check **Define SQL Variable**.
        iii. Click **[+]** to add one or more variables to the **Custom SQL Variable** window.
        iv. When done, click **Insert Variable**.
6. Expand **SNMP Properties**.
    a. Enter a **UDP Port** number in the field provided.
    b. Select an **SNMP Version** from the drop down list.
    c. Enter the **SNMP Community String** in the field provided.
7. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action.** If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

8. Expand **Execution Settings**.
    a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
9. When done, click **Add Action**.

Using Get or Post URL Functions

SolarWinds can be configured to communicate alerts using HTTP GET or POST functions. As an example, a URL may be used as an interface into a trouble ticket system, and, by correctly formatting the GET function, new trouble tickets may be created automatically. The following procedure configures SolarWinds to use GET or POST HTTP functions to communicate alert information.

To configure SolarWinds to use GET or POST URL functions with alerts:

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Send a GET or POST Request to a Web Server** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **HTTP request settings**:
    a. Enter a URL in the field provided.
    b. Select either **Use HTTP GET** or **Use HTTP POST**.
5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action.** If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

6. Expand **Execution Settings**.
    a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
7. When done, click **Add Action**.

Sending a Syslog Message

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

To configure an alert to send a Syslog message:

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Send a SysLog Message** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Send a SysLog message settings**:
    a. Enter the **Hostname or IP Address of the Syslog Server** in the field provided.
    Note: Multiple Syslog servers should be separated by commas.
    b. Select a **Severity** and a **Facility** from the drop down lists.
5. Enter the **Message** of your alert trigger in the field provided.
    a. Optionally click **Insert Variable** to add variables using the following procedure:
        i. Select a **Variable Category**, and then select the variable to add.
        ii. To define a SQL variable, check **Define SQL Variable**.
        iii. Click **[+]** to add one or more variables to the **Custom SQL Variable** window.
        iv. When done, click **Insert Variable**.

6. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action.** If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
7. Expand **Execution Settings**.
    a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
8. When done, click **Add Action**.

Sending an Email/Page

The following procedure configures an email/page action for an alert.

To configure an email/page action for an alert:

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Send an Email/Page** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Recipients**:
    a. Complete the **To**, **CC**, and **BCC** fields.
    b. You can optionally edit sender details by expanding **[+] Sender Details** and editing the **Name of Sender** and the **Reply Address**. **Note:** You must provide at least one email address in the **To** field, and multiple addresses must be separated with commas. Some pager systems require a valid reply address to complete the page.

5. Expand **Message**.
    a. Select the format (**Plain text** or **HTML**) for your alert email.
    b. Enter the **Subject** and **Message** of your alert trigger email/page.
    Note: Messaging is disabled if both the **Subject** and **Message** fields are empty.
    c. Optionally click **Insert Variable** to add variables using the following procedure:
        i. Select a **Variable Category**, and then select the variable to add.
        ii. To define a SQL variable, check **Define SQL Variable**.
        iii. Click **[+]** next to the name of a variable to add one or more variables to the **Custom SQL Variable** window.
        iv. When done, click **Insert Variable**.
6. Expand **SMTP Server**.
    a. Enter the Name of the **SMTP Server**.
    b. Enter the **Hostname or IP Address of your SMTP Server** and the designated **SMTP Port Number**.
    Note: The SMTP server hostname or IP address field is required. You cannot send an email/page alert without identifying the SMTP server.
    c. To use SSL/TLS encryption for your alert email, check **Use SSL**.
    d. If your SMTP server requires authentication, check **This SMTP Server requires Authentication**.
    e. Choose a **Secondary SMTP Server** from the list, if desired.
7. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action.** If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

8. Expand **Execution Settings**.
    a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
9. When done, click **Add Action**.

Setting Custom Status

The following procedure configures a Set Custom Status action for an alert.

The custom status does not affect the actual, polled values. For example, if the custom status is set to UP, but the server is down or unresponsive, packet loss continues to be 100%. Alerts based on the status do not trigger in this instance, but alerts based on a polled value, such as packet loss, do trigger.

Important: When the status is set with an alert, the status does not update to the actual, polled status. The status must be switched manually to a different status or configured to use the polled status. Change the status to use the polled status from the node details page or create a reset action to set the status to use the polled status.

To configure a custom status action for an alert:

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Set Custom Status** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Change Object Status Manually:**
    a. Select **Change to a specific status** if you are creating a trigger action.
        i. If you select, **Change to a specific status**, select the status from the drop down list.
    b. Select **Use polled status** if you are creating a reset action.

5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not affect the overall alert schedule.

    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action.** If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

6. Expand **Execution Settings**.

    a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.

7. When done, click **Add Action**.

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. SolarWinds uses Microsoft® Speech Synthesis Engine version 5.0. If you are under active SolarWinds maintenance, you may also install and use other text-to-speech engines by visiting the SolarWinds website. The following procedure configures text-to-speech output for an alert trigger or reset.

Note: Due to restrictions on Windows service applications, the Text to Speech action is not available to SolarWinds installations on Windows 7 or Windows Server 2008 and higher.

To configure a text-to-speech output action for an advanced alert:

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Text to Speech Output** option, then click **Configure Action**.
3. Enter a name for the action in the **Name of Action** field.
4. Under **Text to Speech Output settings**:

    a. If not installed, click **Download our desktop notification client** to download and install the notification client.

i. From the notification client, configure text to speech output.

b. Optionally click **Insert Variable** to insert variables into the **Text** field:

i. Select a **Variable Category**, and then select the variable to add.

ii. To define a SQL variable, check **Define SQL Variable**.

iii. Click **[+]** next to the name of a variable to add one or more variables to the **Custom SQL Variable** window.

iv. When done, click **Insert Variable**.

5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.

a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action.** If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.

6. Expand **Execution Settings**.

a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.

7. When done, click **Add Action**.

Logging an Alert to the Windows Event Log

You may specify that an alert be logged to the Windows Event Log either on the SolarWinds server or on a remote server. The following procedure logs an alert to the Windows Event Log on a designated server.

To configure alert logging to the Windows Event Log:

1. When editing or adding an alert, click **Add Action** in an Action section of the Alert Wizard.
2. Select the **Windows Event Log** option, then click **Configure Action**.

3. Enter a name for the action in the **Name of Action** field.
4. Under **Event Log Settings**:
    a. Select either **Use Event Log Message on Network Performance Monitor Server** or **Use Event Log Message on a Remote Server. Note:** If the latter option is selected, enter the **Remote Server Name or IP Address** in the field provided.
    b. Enter the **Message** of your alert trigger.
    c. Optionally click **Insert Variable** to add variables using the following procedure:
        i. Select a **Variable Category**, and then select the variable to add.
        ii. To define a SQL variable, check **Define SQL Variable**.
        iii. Click **[+]** next to the name of a variable to add one or more variables to the **Custom SQL Variable** window.
        iv. When done, click **Insert Variable**.
5. Expand **Time of Day**. Use this setting if you want to schedule this action. This schedule does not the overall alert schedule.
    a. Select either **Schedule is controlled on the alert level, no additional schedule for this action needed** or **Use special Time of Day schedule for this action.** If you choose the latter, Click **Add Schedule** and then enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
6. Expand **Execution Settings**.
    a. Check either **Do not execute this action if the alert has been acknowledged already (Recommended)** or **Repeat this action every X minutes until the alert is acknowledged**. If you choose the latter, specify the frequency to have this action repeated.
7. When done, click **Add Action**.

Changes in the Alerting Engine

As of SolarWinds Network Performance Monitor version 2015.1, alerts are no longer created with the desktop-based, Advanced Alerts Manager or Basic Alerts Manager. Alerts are instead created and managed in the SolarWinds Orion Web Console.

Alerts that you created in the desktop-based Alert Manager are migrated to the web-based alerting engine when upgrading to Core version 2015.1. Some alerts may not be successfully migrated and include information about why they were not migrated in the migration log. You can view the alert migration logs in the informational banners displayed after you update your installation.

Changed or removed functionality

The suppression section has not been carried over to web-based alerting. Use options, such as **Condition must exist for more than**, in the trigger conditions to accomplish similar tasks.

Database changes

The following are a list of tables that have been changed that you may be using in any custom SQL query:

- Engines has been renamed to AllEngines
- Nodes has been split into NodesCustomProperties, NodesData, and NodesStatistics
- History has been split into table-specific history tables, such as the AlertHistory table.

The new alerting engine also includes the following new alerting tables:

- AlertActive
- AlertActiveObjects
- AlertConditionState
- AlertHistory
- AlertMigrationLog
- AlertObjects
- AlertSchedules

For a list of database changes from SolarWinds Network Performance Monitor version 2014.2 to version 2015.1, including new tables, column changes, or data constraint or data type changes, see the online Database Changes spreadsheet.

Macro or variable changes

Some alert variables are also not available. See the Defunct Alert Macros topic for variables that cannot be used with the new alerting engine.

Alert Migration to the Web

The Advanced Alert Manager and the Basic Alert Manager are deprecated in SolarWinds Orion Core 2015.1 and later. A web-based alerting engine replaces the previous alerting engine and includes new alerting variables. See General Alert Variables for more information.

To facilitate using the web-based alerting engine, part of the upgrade process migrates alerts created with the desktop-based alerting engine to the web-based alerting engine. All alerts are migrated, including alerts that are disabled.

Migration Issues

Some alerts may not be successfully migrated. The migration log records all alerts that are migrated and includes error messages for alerts that either cannot be migrated or that are not migrated successfully.

Common reasons that migration may not be successful include:

- Invalid alert variables or macros - See Defunct Alert Variables for a list of variables that are not supported.
- Invalid conditions - Some conditions are no longer supported.
- Large alert scope - The number of objects that are relevant to an alert may be too large to migrate.

Limitations to Migrated Alerts

Once an alert has been migrated, you can only view the alert definition through the web-based Alert Manager. You can no longer click on the alert in the views.

Integrating Alerts with Other Products

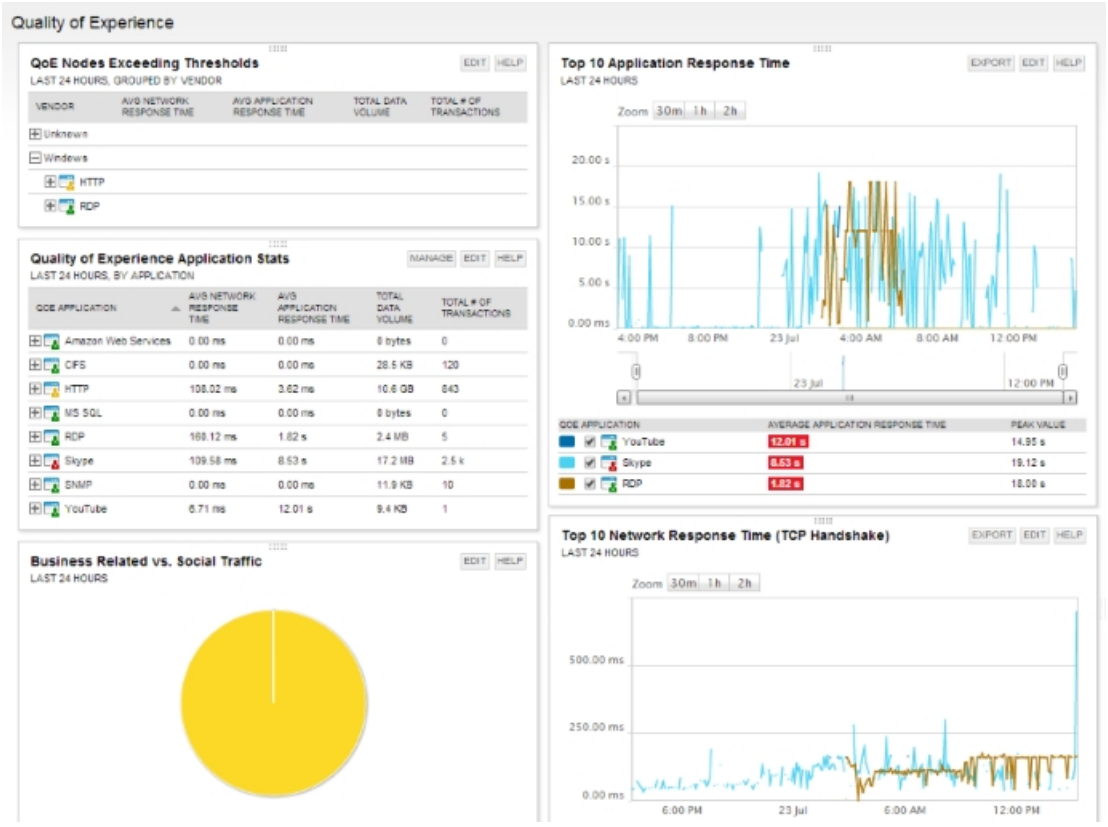
Alerts may be shared with selected other SolarWinds products that are not part of the SolarWinds Orion Platform, such as AlertCentral and WebHelpDesk.

To integrate alerts with other SolarWinds products:

1. On the Alert Summary page, expand **Alert Integration**.
2. Check **Integrate alert with other SolarWinds products and subscribers (Recommended)**.
3. Provide an appropriate **Alert Subject**. You can choose to use this name as the subject field for the alert.
4. Choose the alert **Severity**.
   Note: This information may be used to determine how a shared alert is handled by the product to which you are sharing the alert.
5. To include additional alert properties in the alert, click **Insert Variable** and choose which properties you want to include.
6. Click **Submit**.

Chapter 13: Monitoring Quality of Experience

Quality of Experience (QoE) is a new dashboard within NPM that allows you to monitor traffic on your network. QoE uses Packet Analysis Sensor to provide packet-level traffic information about key devices and applications that you specify.



Benefits of QoE

With QoE, you can:

- Compare statistics like network response time (TCP Handshake) and application response time (Time to First Byte) to determine if a perceived bottleneck is actually on your network, or if you need to call the server team.
- Use data volume trends to pinpoint traffic anomalies and investigate the cause.
- Monitor "risky" types of traffic.

There are three steps you must complete to start monitoring traffic on your network:

1. Deploy Packet Analysis Sensors (network and/or server) to Windows nodes where you want to collect traffic data.
2. In the web console, specify the nodes and applications for which you want to collect traffic.
   Note: Packet Analysis Sensors does not automatically discover nodes and applications. You must indicate the nodes and applications to monitor before you will see traffic data in the web console.
3. Allocate appropriate CPU cores and memory for the traffic load for each sensor.

Traffic data is captured using packet analysis sensors. These sensors collect packets using either a dedicated Windows SPAN or Mirror port monitor or directly on your Windows server. Packet Analysis Sensors capture packets from the local network interface (NIC) and then analyzes collected packets to calculate metrics for application performance monitoring. These metrics provide information about application health and allow you to identify possible application performance issues before they are reported by end-users.

With the ability to analyze packet traffic, QoE provides real observed network response time (NRT) and application response time (ART). In addition, Packet Analysis Sensors have the ability to classify and categorize traffic for over 1000 different applications by associated purpose and risk-level.

For more information about specific implementations of QoE, see Common Packet Analysis Sensor Deployment Scenarios.

System Requirements

Before you deploy a Packet Analysis Sensor to a device, review the following minimum system requirements.

You will need administrative privileges for each node or switch.

Sensors can **not** be installed on 32-bit computers and do **not** support communication over https.

Network Packet Analysis Sensors (NPAS)

Hardware/Software	Requirements
OS	Windows 7 or later, 64-bit Windows Server 2008 or later, 64-bit **Note**: 32-bit operating systems are not supported.
CPU Cores	2 CPU Cores + 1 CPU Core per 100 Mbps
Hard drive space	500 MB
RAM	1 GB + 1 GB per 100 Mbps (2 GB + 1 GB per 100 Mbps recommended)
Network	1Gbps maximum throughput
Other	SPAN, mirror port, or in-line tap on the monitored switch

Server Packet Analysis Sensors (SPAS)

Hardware/Software	Requirements
OS	Windows 7 or later, 64-bit Windows Server 2008 or later, 64-bit **Note**: 32-bit operating systems are not supported.
CPU Cores	2 CPU Cores + 1 CPU Core per 100 Mbps
Hard drive space	500 MB

Hardware/Software	Requirements
RAM	256 MB + 500 MB per 100 Mbps (256 MB recommended + 500 MB per 100 Mbps)
Network	1Gbps maximum throughput

Port Requirements

Port #	Protocol	Direction	Description
17778	TCP	Outgoing	Used to send information back to your SolarWinds server.
135	TCP	Incoming	Used by your SolarWinds server to deploy the sensors and to apply updates to the sensors.

Port Mirroring Requirements

When deploying a Network Packet Analysis Sensor, you must create a SPAN, mirror port, or in-line tap on the monitored switch. For virtual switches you may create promiscuous port groups or a vTap instead. This requires at least one extra network interface to collect data from the managed network interface, a server to monitor the copied traffic, and a network cable to connect the mirrored port to the physical server.

Please view your vendor specific documentation for instructions on how to set up port mirroring. You can create port mirrors for both physical switches and virtual switches.

For an example of how to create SPAN, see your switch's documentation.

How SolarWinds Packet Analysis Sensors Work

SolarWinds provides two types of Packet Analysis Sensors to monitor and analyze your network traffic.

- Packet Analysis Sensors for Networks (network sensor)—collect and analyze packet data that flow through a single, monitored switch for up to 50 discrete applications per node
- Packet Analysis Sensor for Servers (server sensor)—collect and analyze packet data of specific applications that flow through a single node

After a sensor is deployed and configured, it captures packets and analyzes them to calculate performance metrics for the monitored applications. An included communication agent allows the sensor to send back sampled packet data to the Orion server, which includes volume, transactions, application response time, and network response time for each application on a node. The packet data are then saved to the Orion database. The information is used to populate your QoE dashboard. You can configure how long you retain the packet data in the **Database Settings** section of the **Polling Settings** screen.

Network Packet Analysis Sensor (NPAS)

Your network administrator must create a dedicated SPAN, mirror port, or in-line tap monitor on the physical or virtual switch before you can deploy or configure a network sensor.

After you deploy and configure the network sensor to the node monitoring the switch, the sensor captures all packets that flow through the switch and quickly categorize the packets by application.

Packets that correspond to monitored applications are analyzed for Quality of Experience metrics, such as response times or traffic volume. Data are then sent to the Orion server using the SolarWinds communication agent.

Server Packet Analysis Sensor (SPAS)

A server sensor (SPAS) can monitor:

- a packet traffic on a single node.
- up to 50 applications per node.

A deployed SPAS captures packets to and from the node. It identifies packets that are sent to or from the monitored application and analyzes them for Quality of Experience metrics, such as response time or traffic volume. Data are then sent to the Orion server using the SolarWinds communication agent.

Limitations to Packet Analysis Sensors

The number of nodes you can monitor is limited by the data throughput per node, the number of cores, and the amount of RAM available on the monitoring server.

Use the following table to review the sensor limitations.

Sensor Limitations	Value
Maximum throughput (NPAS and SPAS)	1 Gbps
Maximum number of nodes per sensor (NPAS)	50 nodes
Maximum number of node/application pairs (NPAS and SPAS)	50,000 pairs
Maximum number of sensors deployed on your network	1,000 sensors
Maximum number of applications per node/sensor (NPAS and SPAS)	1,000 applications per node

The system requirements increase for every 100 Mbps of traffic.

Deploying Packet Analysis Sensors

Common Packet Analysis Sensor Deployment Scenarios

After you install your Orion platform product, deploy network sensors on a server dedicated to monitoring a network switch, or deploy server sensors directly on physical or virtual servers or workstations.

Based on how you want to aggregate the returned QoE metrics, there are three main deployment scenarios per sensor type.

Aggregation level	Sensor Deployment	Configuration
I have access to my network (NPAS)		
Per application	Deploy an NPAS to a port mirror that monitors all traffic to and from the application	Automatic
Per site	Deploy an NPAS to a port mirror that monitors all traffic to and from the site	Add a sampling of endpoints to the NPAS as managed nodes
Per client	Deploy an NPAS to a port mirror that monitors all traffic to and from the site	Add all of the endpoints to the NPAS as managed nodes
I have access to my application servers (SPAS)		
Per application	Deploy the SPAS directly on the application server	Automatic
Per site	Deploy the SPAS to select endpoints	Automatic
Per client	Deploy the SPAS to all endpoints	Automatic

Notes:

- When deploying network and server sensors on the same network, ensure that you do not monitor the same node with multiple sensors. This impacts

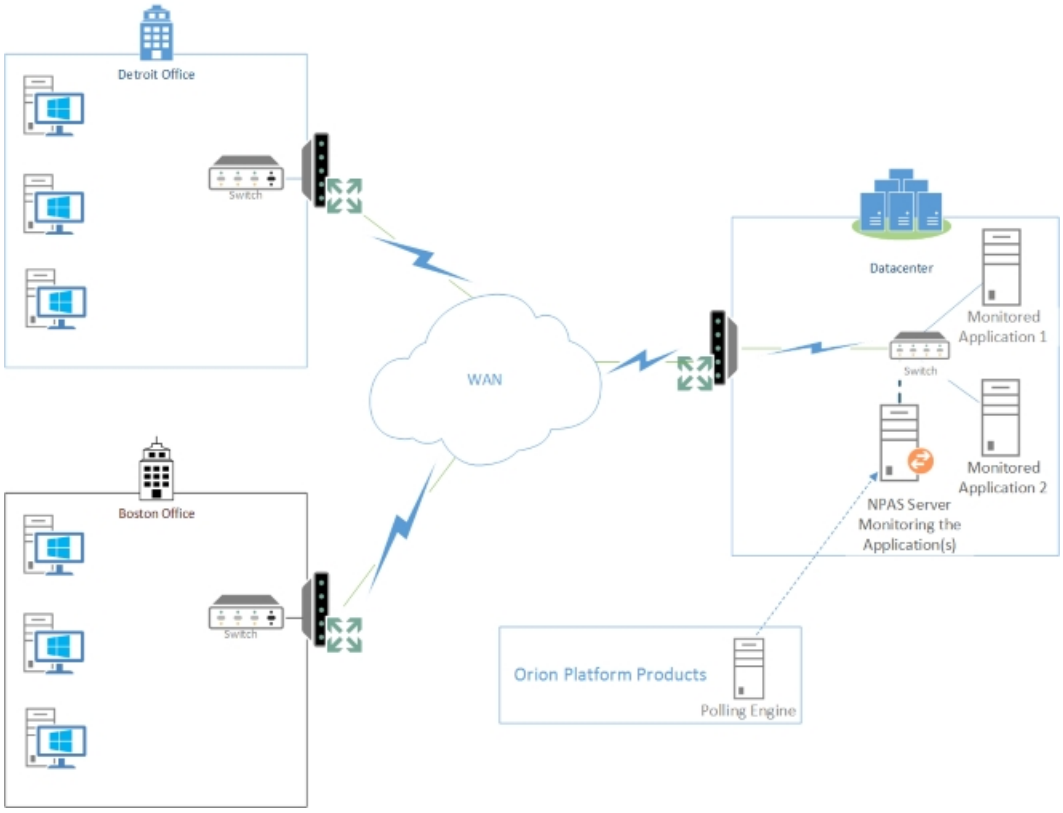
the QoE metrics.

- All monitored nodes must be managed by your Orion Platform product before they can be monitored by sensors.
- If the node is managed by your SolarWinds Orion server, applications and nodes are detected by default. If packet data is not collected, go to **Settings > QoE Settings > Global QoE Settings**, and activate the auto-detect option. You can also manually monitor applications and managed nodes or ignore them. See Monitoring QoE Applications and Defining Nodes for a Network Sensor for more information.

Aggregation per application

This deployment scenario provides a broad indication of the overall response time between computers and the monitored application.

Aggregation with access to network (NPAS)



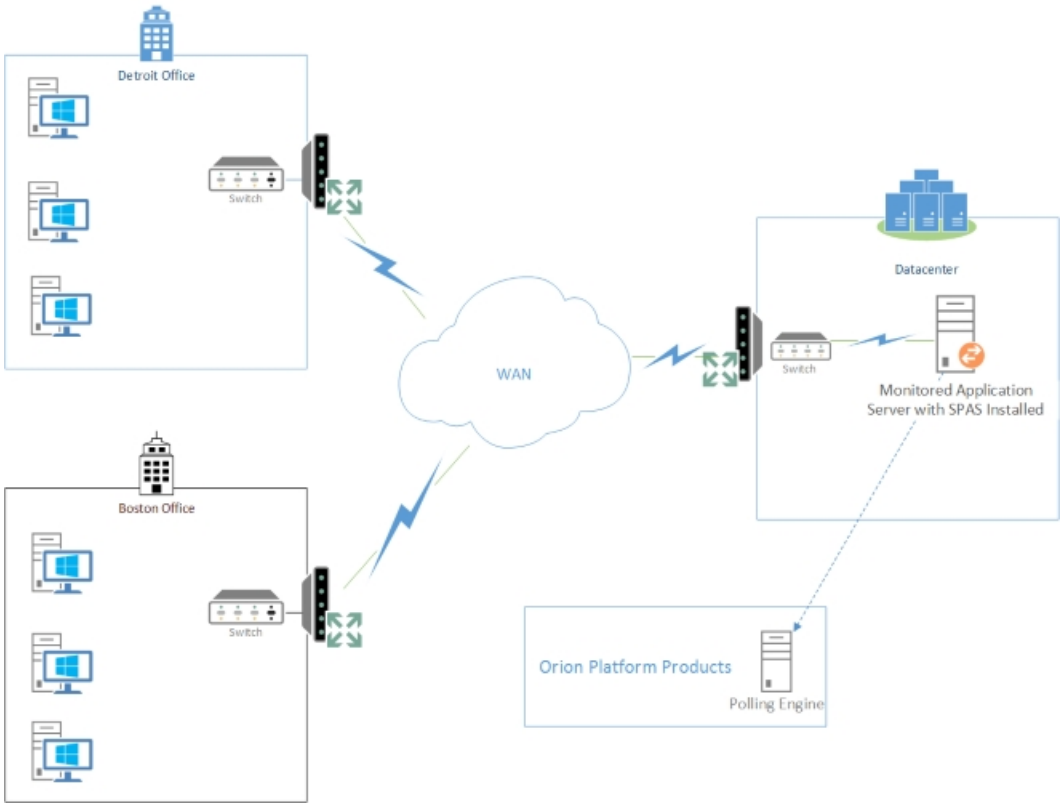
Notes:

- Create a port mirror, SPAN, or network tap on the switch with all the network traffic to or from the application. See System Requirements for more information.
- You can monitor multiple applications using the same NPAS.

To deploy the network sensor:

1. Click **Settings > QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor**.
2. Select the **Network** option, and then click **Add Nodes**.
3. Choose the node with the port mirror, SPAN or network tap set up to monitor your network switch.
4. Assign and test the credentials for the selected node.
5. Click **Add Node(s) and Deploy Agent(s)** to deploy the network sensor to the node.

Aggregation with access to application servers (SPAS)



To deploy from your Web Console:

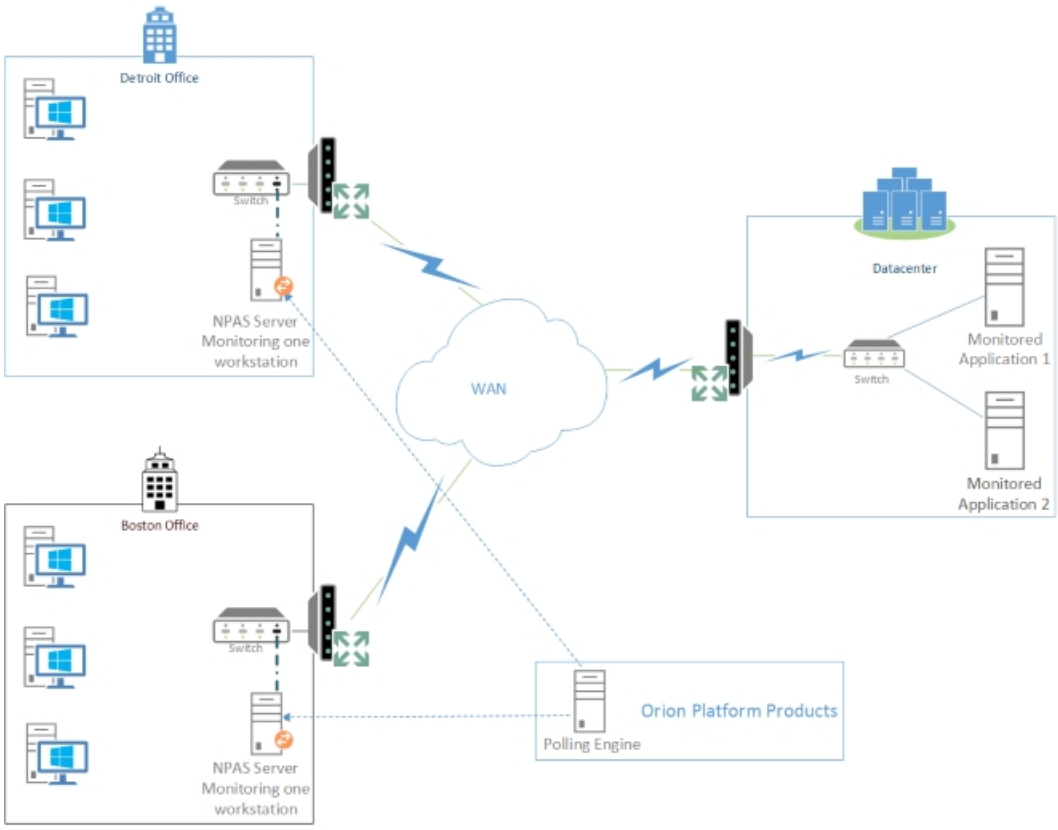
1. Click **Settings > QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor**.
2. Select the **Server** option, and then click **Add Nodes**.
3. Choose the nodes with the application you want to monitor.
4. Assign and test the credentials for each node.
5. Click **Add Node(s) and Deploy Agent(s)** to deploy an agent on the node.

Aggregation per site

This deployment scenario provides an aggregated response time per monitored site or network to the application. For example, the response time from your Detroit office to your datacenter is 1 second, but the response time from Boston to your datacenter is 7 seconds. If you used the aggregation per application deployment method, the response time for the application is 4 seconds.

This method requires you to identify users who best represent how the application is used. You then use the users' computers as data points to monitor with Packet Analysis Sensors.

Aggregation per site with access to network (NPAS)



Notes:

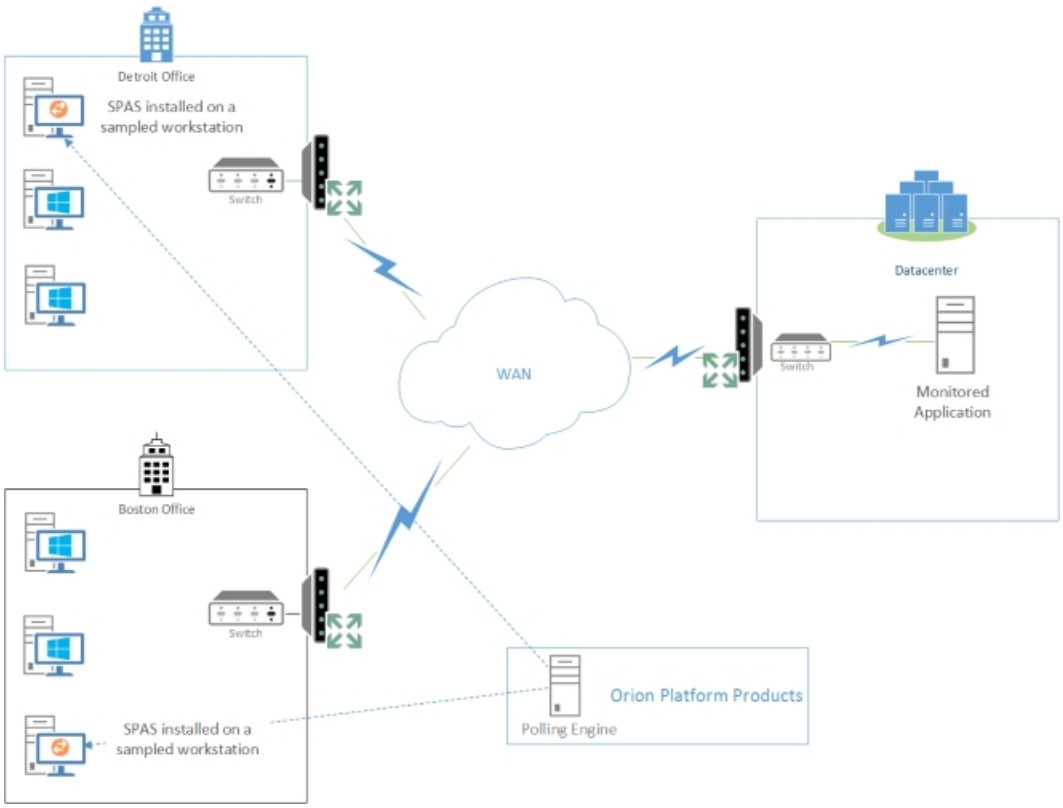
- Create a port mirror, SPAN, or network tap on the switch with all the network traffic to or from the site. See System Requirements for more information.

- Identify a sample set of users whose computers are monitored by the NPAS
- You can monitor multiple applications using the same NPAS.

To deploy the network sensor:

1. Click **Settings > QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor**.
2. Select the **Network** option, and then click **Add Nodes**.
3. Choose the node with the port mirror, SPAN or network tap set up to monitor your network switch.
4. Assign and test the credentials for the selected node.
5. Click **Add Node(s) and Deploy Agent(s)** to deploy the network sensor to the node.

Aggregation per site with access to application servers (SPAS)



Note: Identify a sample set of users whose computers are monitored by the SPAS

To deploy from your Web Console:

1. Click **Settings > QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor**.
2. Select the **Server** option, and then click **Add Nodes**.
3. Select the sampled set of user computers to monitor.
4. Assign and test the credentials for each node.
5. Click **Add Node(s) and Deploy Agent(s)** to deploy an agent on the node.

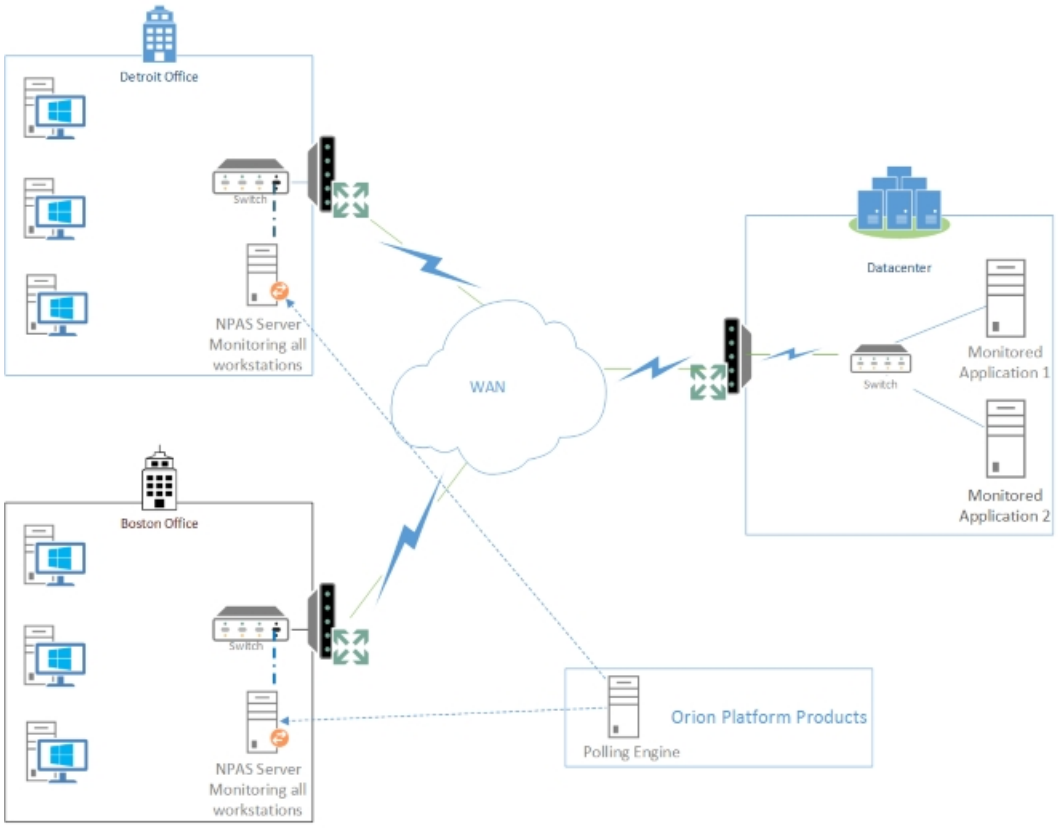
Aggregation per computer

This deployment scenario provides highly granular response times for the application because metrics for each computer are recorded.

One or two workstations can be experiencing long response times, which may not be caught when aggregated per site or per application.

This method requires all workstations to be managed within your Orion Platform product.

Aggregation per computer with access to network (NPAS)



Notes:

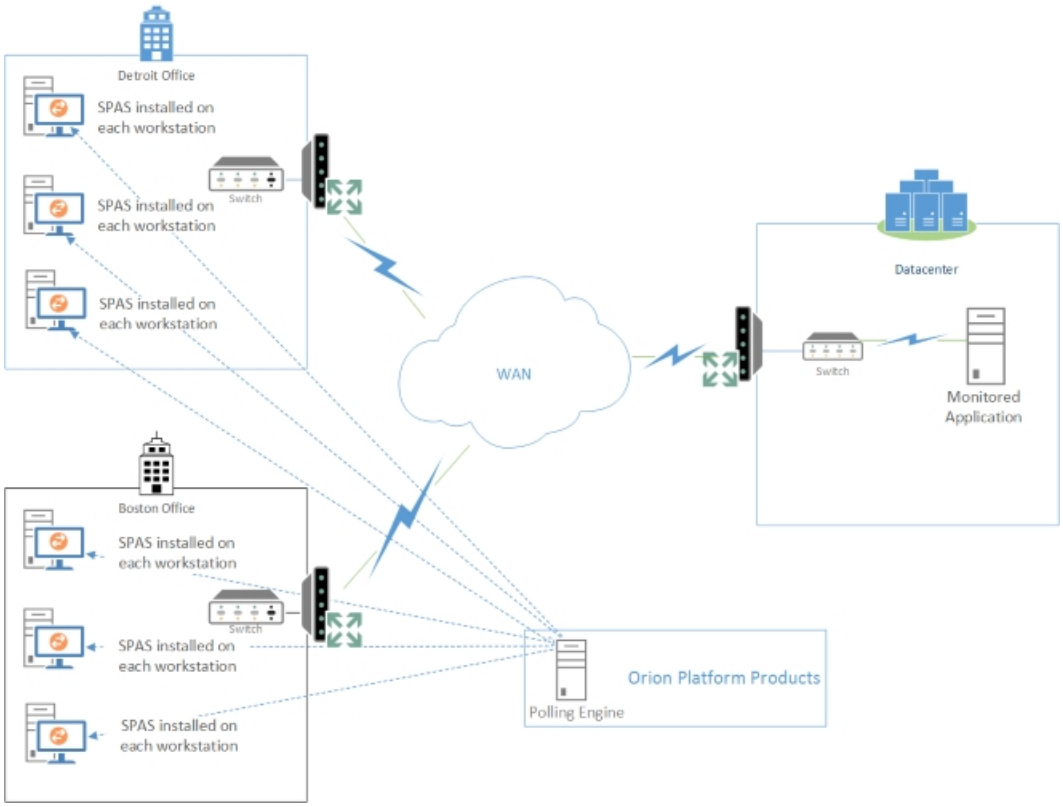
- Create a port mirror, SPAN, or network tap on the switch with all the network traffic to or from the site. See System Requirements for more information.
- You can monitor multiple applications using the same NPAS.

To deploy the network sensor:

1. Click **Settings > QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor**.
2. Select the **Network** option, and then click **Add Nodes**.
3. Choose the node with the port mirror, SPAN or network tap set up to monitor your network switch.
4. Assign and test the credentials for the selected node.

5. Click **Add Node(s) and Deploy Agent(s)** to deploy the network sensor to the node.

Aggregation per computer with access to application servers (SPAS)



To deploy from your Web Console:

1. Click **Settings > QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor**.
2. Select the **Server** option, and then click **Add Nodes**.
3. Select the all user computers to monitor.
4. Assign and test the credentials for each node.
5. Click **Add Node(s) and Deploy Agent(s)** to deploy an agent on the node.

Deploying a Network Sensor

Network sensors must be deployed on any server connected to a switched SPAN/mirror port or in-line tap.

Notes:

- If you deploy from the Additional Web Console, the node must be reachable from the main polling engine during deployment. Data from sensors are directed to the polling engine assigned to the node when the sensor was deployed.
- Network sensors can monitor up to 50 discrete applications through a single network interface, but they cannot monitor more than 1 GB throughput.

To deploy a Network sensor:

1. Click **Settings > QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor**.
2. Select the **Network** option, and then click **Add Nodes**.
3. Move the node that monitors your switch to the Selected Nodes panel, and click **Add Selected Node**.
4. Assign and test the credentials for the selected node.
5. Click **Add Node(s) and Deploy Agent(s)** to deploy an agent on the node.
6. Expand the network sensor you added, and click **Add Nodes to Monitor**.
7. Choose which node's traffic you want to monitor from the switch, and click **Next**.
8. Select the specific application to monitor, and click **Next**. QoE can automatically detect the first 50 applications, or you can add specific applications.

When sensor deployment is complete, the installation wizard displays a message.

To specify manually which nodes and applications to monitor, see Monitoring QoE Applications and Nodes. Nodes are automatically detected and added by default.

Deploying a Server Sensor

These sensors can only monitor the packet traffic of a single application. After you deploy a server sensor to the application node, the sensor captures packets to and from the node. It then identifies packets that are sent to or from the monitored application and analyzes them for Quality of Experience metrics, such as response time or traffic volume.

To deploy a server sensor:

1. Click **Settings > QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor**.
2. Select the **Server** option, and then click **Add Nodes**.
3. Choose the Windows nodes to which you want to deploy your server sensors, and then click **Add Selected Node**.
4. Assign and test credentials for each node on which you want to deploy sensors.
5. Click **Add Node(s) and Deploy Agent(s)** to deploy agents.
   Notes:
   - Deployment may take some time and will run as a background process.
   - QoE automatically chooses settings, including the interface to capture traffic data and limits to memory and CPU, during agent deployment. You can change these settings once deployment is complete by selecting the sensor and clicking **Edit**.
   - When installation is complete, you will see a message in the notification bar.
   - You can confirm the deployment status on the Manage QoE Packet Analysis Sensors page.

To specify manually which applications to monitor, see Monitoring QoE Applications. Applications are automatically detected and added by default.

Removing a Sensor

Removing a sensor from a node is a two steps process. First delete the sensor using the Web Console, and then remove the communication agent directly from the node.

To delete the sensor using the Web Console:

1. Click **Settings > QoE Settings > Manage QoE Packet Analysis Sensors**.
2. Select the node.
3. Click **Delete Sensor**.
4. Click **Delete** when prompted.

To remove the agent directly from the node:

1. Logon to the node with administrative credentials.
2. Navigate to **Control Panel > Programs and Features.**
3. Select `SolarWinds Agent`.
4. Click **Uninstall**.
5. Follow the onscreen prompts to completely uninstall the agent.

Monitoring QoE Applications and Nodes

By default, nodes and applications are automatically monitored by QoE when you deploy a Network or Server Sensor. You can modify this behavior and automatically filter which nodes or applications are monitored.

See Global QoE Settings for more information on how you can change these settings.

Note: Server Sensors automatically monitor the top 50 applications on the node they are installed on based on the global settings. You can change which applications are monitored after the sensor is deployed.

For more information, refer to the following topics:

- Manage Global QoE Settings
- Monitoring QoE Applications
- Defining Nodes for a Network Sensor
- Ignoring Applications or Nodes
- Defining Custom HTTP Applications

Manage Global QoE Settings

You can control how Packet Analysis Sensors behave by changing the settings on this page. Settings are distributed to sensors regularly when the agent is updated. You can manually update an agent from the Manage Agents page.

QoE Applications

Control how you monitor QoE applications for both Network Packet Analysis Sensors and Server Packet Analysis Sensors.

Auto-detect QoE applications

Use this to detect and monitor traffic associated with all applications that fulfill the auto-detection rules defined on this page. This is active by default. You must select applications manually when this option is disabled.

Note: If you automatically detect nodes, you should also automatically detect applications.

HTTP application domain detection level

Choose how granularly QoE breaks up http traffic to monitor.

- **Top level (http://*)** - Monitor all http traffic.
- **Second level (http://hostname/*)** - Separate and monitor http traffic based on domains.
- **Third level (http://hostname/path1/*)** - Separate and monitor http traffic based on the domain and 1st level directory within each domain.

Add auto-detected applications that are

Further refine the applications that are monitored by choosing to monitor all application traffic sources, traffic destinations, or all application traffic. Packet sources and destinations are based on the source or destination IP address included in the packet.

- **Transaction destinations (servers)** - Monitor applications that receive traffic based on the destination IP address of the packet.
- **Transaction sources (client)** - Monitor applications that generate traffic based on the source IP address of the packet.
- **Either a source or destination** - Monitor all application traffic.

For each node, include top *X* application that have at least *Y*% of total QoE traffic.

Filter the number of applications that are monitored to applications that generate a certain amount of network traffic.

Nodes with QoE Traffic

Control how you monitor QoE nodes for Network Packet Analysis Sensor.

Auto-detect QoE nodes

Use this to detect and monitor the first 50 nodes with network traffic. This is active by default. You must select nodes manually when this option is disabled.

Note: If you automatically detect nodes, you should also automatically detect applications.

Add auto-detected monitored nodes that are

Further refine the nodes that are monitored by choosing to monitor all nodes that are traffic sources, traffic destinations, or all nodes that generate or receive network traffic. Packet sources and destinations are based on the source or destination IP address included in the packet.

- **Transaction destinations (servers)** - Monitor nodes that receive traffic based on the destination IP address of the packet.
- **Transaction sources (client)** - Monitor nodes that generate traffic based on the source IP address of the packet.
- **Either a source or destination** - Monitor all traffic.

Monitoring QoE Applications

Applications are automatically monitored when traffic is detected by the Packet Analysis Sensor. However, you can manually select specific applications to monitor. QoE installs with the ability to monitor over 1000 pre-defined applications, including FTP, RDP, CIFS, SQL, and Exchange. You can also define your own custom HTTP applications.

Notes:

- Because of the hardware requirements needed to process large amounts of traffic, SolarWinds recommends that you preferentially monitor business-critical nodes and applications. For more information about recommended hardware specifications, see System Requirements.
- You should not assign more than 50 applications to a single node due to potential performance issues. However, you can monitor up to 1000 applications.

Monitoring Applications Automatically

While QoE sensors automatically detect and monitor applications by default, the settings may have changed or you may have upgraded from a previous version of QoE that does not automatically monitor applications.

Note: Only applications that meet the criteria selected in **QoE Applications** are monitored automatically.

To monitor application traffic automatically:

1. Click **Settings > QoE Settings > Manage Global QoE Settings**.
2. Select **Active** in **Auto-detect QoE applications**.
3. Change other settings to refine the number of applications you automatically monitor. See Global QoE Settings for more information on the settings.
4. Click **Submit**.

Monitoring Applications Manually

You may choose to add monitored applications manually to QoE.

To select specific applications for monitoring:

1. Click **Settings > QoE Settings > Manage QoE Applications**.
   Notes:
   - Applications are only listed if there are monitored nodes. You must first add a Network or Server Sensor before you can enable any applications. For more information, see Common Packet Analysis Sensor Deployment Scenarios.
   - Applications listed with the **Enabled/Disabled** toggle "ON" are currently being monitored on at least one node.
   - Applications can be disabled (the **Enabled/Disabled** toggle "OFF") which means that no traffic for the application is currently collected on any node.
2. Click **Add New**.
3. Select **Choose a pre-configured application**.
   Note: Applications that are already enabled will not appear in the list.
4. Use the **Search** or **Group By** options to find the application you want to monitor, select it, and then click **Next**.
5. On the **Configure Application** view, edit the **Category**, **Risk Level**, or **Productivity Rating** as necessary, and then click **Next**.
6. On the **Configure Data Collection** view, choose the node(s) you want to monitor for this type of traffic.
   Note: Only nodes that have already been specified as nodes to monitor on the Manage QoE Nodes page appear in this list.
7. Click **Next**.
8. Review your choices on the **Summary** page, then click **Finish**.

Your newly enabled application will appear on the **Manage QoE Applications** page in alphabetical order.

Defining Nodes for a Network Sensor

Nodes are automatically detected and monitored when network traffic is detected either originating from or terminating at a node. However, you can manually specify the nodes instead. After the network sensor has been successfully deployed, add applications and nodes to monitor. For information about adding applications, see Monitoring QoE Applications.

Note: You can monitor up to 50 nodes per network sensor.

Adding Nodes Automatically

While Network Sensors automatically detect and monitor nodes by default, the settings may have changed or you may have upgraded from a previous version of QoE that does not automatically monitor nodes. QoE automatically monitors the first 50 nodes with traffic.

Notes:

- Automatic node discovery may not be 100% accurate due to devices with the same IP addresses in your network.
- Only nodes that meet the criteria selected in **Nodes with QoE Traffic** are added automatically.

To monitor nodes automatically:

1. Click **Settings > QoE Settings > Manage Global QoE Settings**.
2. Select **Active** in **Auto-detect QoE nodes**.
3. Change other settings to refine the number of nodes you automatically monitor. See Global QoE Settings for more information on the settings.
4. Click **Submit**.

Adding Nodes Manually

You may choose to add monitored nodes manually to a Network Sensor. If a node is already monitored and you want to monitor it with a different sensor, you must delete the node from the original sensor before you can add it to the new network sensor.

To add nodes for a network sensor to monitor:

1. Navigate to the **Manage QoE Packet Analysis Sensors** page.
2. Expand the Network sensor that you want to add a node to.

3. Click the **Add Node to Monitor** button.
4. On the Create QoE Node page, choose the managed nodes you want to monitor with this network sensor.
5. On the Select QoE Applications page, choose the applications you want to monitor for these nodes. See Monitoring QoE Applications for more information.
6. Review your selections on the Summary page.
7. Click **Finish**.

View the nodes and applications selected by expanding the Network Sensor you just configured.

Ignoring Applications or Nodes

You can ignore traffic generated by applications or from a specific node.

Ignoring Applications

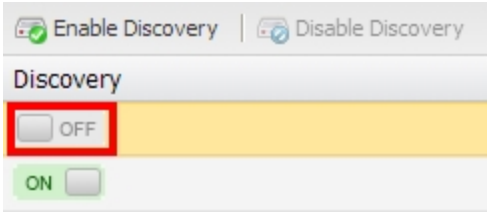
If you decide that you no longer want to monitor an application, you can disable discovery or monitoring for that application in the **Manage QoE Applications** page.

Note: These settings are on a global level. You cannot turn application discovery or monitoring on or off for specific sensors.

To ignore network traffic from an application:

1. Log into the web console using an account with administrative privileges.
2. Click **Settings** in the top right of the web console.
3. In the Settings grouping, click **QoE Settings**.

4. Click **Manage QoE Applications**.
5. Toggle Monitoring or Discovery **ON** or **OFF**.



Use the following table to determine which combination of settings you want to use.

	Monitoring ON	**Monitoring OFF**
Discovery ON	Applications can be automatically discovered and application traffic is monitored	Applications can be automatically discovered, but application traffic is not monitored
Discovery OFF	Applications cannot be automatically discovered, and application traffic is monitored	Applications cannot be automatically discovered, and application traffic is not monitored.

Ignoring Nodes

You can permanently ignore all traffic from specific nodes that you monitor on a network sensor. This is often used to reassign a node to a different network sensor.

Note: You cannot add a node back to its original network sensor.

To ignore all network traffic from a node:

1. Log into the web console using an account with administrative privileges.
2. Click **Settings** in the top right of the web console.
3. In the Settings grouping, click **QoE Settings**.
4. Click **Manage QoE Packet Analysis Sensors**.

5. Select a network sensor, and click **Edit**.
6. Select the node you want to remove, and click **Delete**.

Defining Custom HTTP Applications

In addition to choosing from pre-defined applications, you can also define custom HTTP applications, and then add them to nodes you are monitoring.

To create a custom HTTP application:

1. Navigate to **Settings**, then select **Manage QoE Applications**.
2. Click **Add New**.
3. On the **Select Application** page, select **Create a new HTTP application**, then click **Next**.
4. On the **Configure Application** page, enter the name and description of the application you're creating, then choose the Category, Risk Level, and Productivity Rating appropriate for the application.
5. Set the URL Filter. This specifies the HTTP application traffic to monitor. When you choose which filter to use in the drop-down, notice that the example changes to indicate how the accompanying text field will be used.

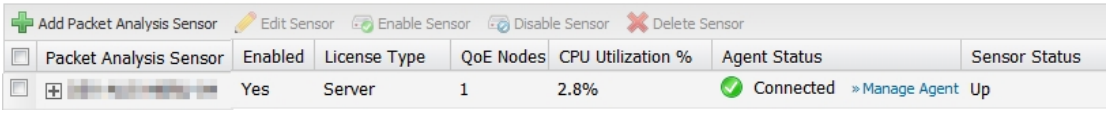
For example, selecting Hostname contains changes the help text to http://*...*/path/page.html. Any text you enter will be included in the filter where the "…" appears.

6. Enter the hostname or URL for your filter, then click **Next**.

7. On the **Specify Nodes** page, choose the node(s) you want to monitor for this type of traffic. Only nodes that have already been specified as nodes to monitor (on the **Manage QoE Nodes** page) will appear in this list.
8. Click **Next**. Review your choices on the **Summary** page, then click **Finish**.
9. Your new application will appear on the **Manage QoE Applications** page in alphabetical order.

Advanced Sensor Configuration

Sensors cannot be edited until they are fully deployed. You are notified when your sensor is deployed, or you can check the **Manage QoE Packet Analysis Sensors** page. The status of completely deployed and working sensors is **Up**.



When you click **Edit Sensor**, you can configure:

- the monitored interface
- the allocated CPU cores and memory

Configuring the Monitored Interface

When you deploy a sensor, the first available interface is monitored for traffic. Once the sensor is installed, you can go back and change the monitored interface, as indicated in the following procedure.

To change the interface monitored by a sensor:

1. Click **Settings > QoE Settings > Manage QoE Packet Analysis Sensors**.
2. Select the sensor to edit.
3. Click **Edit Sensor**.
4. Select the desired interface from the **Interface to capture QoE data** drop-down list.
5. Click **Save**.

Configuring the Number of CPU Cores and Allocated Memory

When a sensor is deployed, QoE automatically allocates one CPU core and 256 MB of memory to the sensor. After the sensor is installed, you can change the allocated CPU cores and memory.

For sensors, the memory usage scales with the traffic load. The more flows that are going on the line, the more memory you need.

Number of CPU Cores	Guidelines
1	Not Recommended
2	Suitable for 100 Mbps links
3-4	Gigabit links with low utilization
5-6	Gigabit links with medium utilization
7+	Gigabit links with high utilization

To change the sensor thresholds:

1. Click **Settings > QoE Settings > Manage QoE Packet Analysis Sensors**.
2. Select the sensor to edit.
3. Click **Edit Sensor**.
4. In the **Memory** field, select the number of GB you want to allocate to the sensor.
   Note: If you allocate less than the recommended amount of memory, you may see reduced performance.
5. In the **CPU Cores** field, select the number of CPU cores you want to allocate to the sensor.
   Note: If you allocate fewer than the recommended number of CPU cores, you may see reduced performance.
6. Click **Save**.

Configuring Thresholds

You can modify the application response time (ART), network response time (NRT), volume, and transaction thresholds that are used to alert you to irregularities in your network.

Note: It is best to allow the sensors to collect a few days' worth of data before setting thresholds.

To change the number of CPU cores and memory allocated to the sensor:

1. Click **Settings > QoE Settings > Manage QoE Applications**.
2. Select the application to edit.

3. Click **Edit**.
4. Click **Next**, and then click **Next** again.
5. On the Summary page, click the plus sign by **Thresholds**.
6. Select **Override Orion General Thresholds** next to each data type.
7. Change the threshold. You can use specific thresholds or you can use a dynamic threshold based on the baseline established. The default baseline is seven days, which is configurable in the **Orion Polling Settings** page.
8. Click **Finish**.

Packet Analysis Sensor Agents

The software that provides a communication channel between your SolarWinds server and the monitored object to which you have deployed your Packet Analysis Sensor is called an *agent*. Agents are used to provide packet-level traffic information about key devices and applications that you specify. The agent runs as a service, and it has a relatively small footprint (under 100MB installed).

For more information, see:

- Agent Requirements
- Deploying an Agent
- Agent Settings
- Managing Agents

Chapter 14: SolarWinds Orion Agents

An agent is software that provides a communication channel between the Orion server and a Windows computer. Agents are used to provide packet-level traffic information about key devices and applications that you specify. This can be beneficial in the following situations:

- Allows for polling host and applications behind firewall NAT or proxies
- Polling node and applications across multiple discrete networks that have overlapping IP address space
- Allows for secure encrypted polling over a single port
- Support for low bandwidth, high latency connections
- Polling nodes across domains where no domain trusts have been established
- Full end to end encryption between the monitored host and the Orion poller

The agent allows you to monitor servers hosted by cloud based services such as Amazon EC2, Rackspace, Microsoft Azure, or virtually any other Infrastructure as a Service (IaaS).

Once deployed, all communication between the Orion server and the agent occur over a single fixed port. This communication is fully encrypted using 2048 bit TLS encryption. The agent protocol supports NAT traversal and passing through proxy servers that require authentication.

Agent Requirements

Before you deploy agents to a target computer, review the following system requirements.

Notes:

- Agents run as a Windows service
- Agent communication to the Orion Server uses FIPS compatible encryption
- Agents do not work with AppInsight for SQL when the SQL server being monitored is in a cluster.
- Agents have parity with WMI in collecting information.

Important: JMX polling is not supported using an agent.

Supported Operating Systems

The following operating systems are supported for both 32-bit and 64-bit computers:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows 7, Windows 7 SP1
- Windows 8, Windows 8.1

  Important: Workstation operating systems are only supported with the Pro, Enterprise, and Ultimate editions.

Prerequisites

The following software packages are installed by the agent installer if necessary:

- Microsoft Visual C++ 2013 Redistributable Package for 32- or 64-bit
- .NET Framework 4.0 (You must install this manually if you are installing an agent on Windows Core.)

Agent Resource Consumption

The following table details agent resource consumption.

CPU	Less than 1% on average under normal operating conditions (0.24% on average)
Memory	Between 10 and 100 MB depending upon the number and types of jobs
Bandwidth	Roughly 20% (on average) of the bandwidth consumed by the WMI protocol for transmission of the same information For example, Agent: 1.3 KBPS versus WMI at 5.3 KBPS
Storage	100 MB when installed

A single polling engine can support up to 1,000 agents.

Agent Licensing

Agent software is free. You remain bound by the limits of the license you own regardless of how information is polled, either via an agent or another protocol.

Accounts and Security Requirements

The VeriSign Root Certificate Authority (CA) must be current. This is required because the agent software is signed using a VeriSign certificate. To install a certificate, see Certificates and the Agent.

After the agent is installed, it runs as the Local System account and does not require administrative permissions to function.

Agent Open Port Requirements

For agent-initiated communications, port 17778 must be opened on the Orion server (inbound) and allowed by the firewall. It is used on a continual basis once the agent has been deployed. Communication is initiated outbound from the agent to the Orion server.

For server-initiated communications, port 17790 must be opened (inbound) on the remote computer.

Requirements for Remote Deployment from the Server

If you want to deploy agents from the SolarWinds Orion server, the following requirements must be met:

- The account used for remote deployment must have access to the administrative share on the target computer: `\\<hostname_or_ip>\admin$\temp`
- User Account Control (UAC) must either be disabled on the target computer, or the built-in Administrator account must be used
- Approximately 100 MB of available hard drive space on the target computer

  Note: Other remote or mass deployment methods do not have the same requirements.

Open Ports Requirements for Remote Deployment from the Server

The following ports must be open to deploy agents from the SolarWinds Orion server:

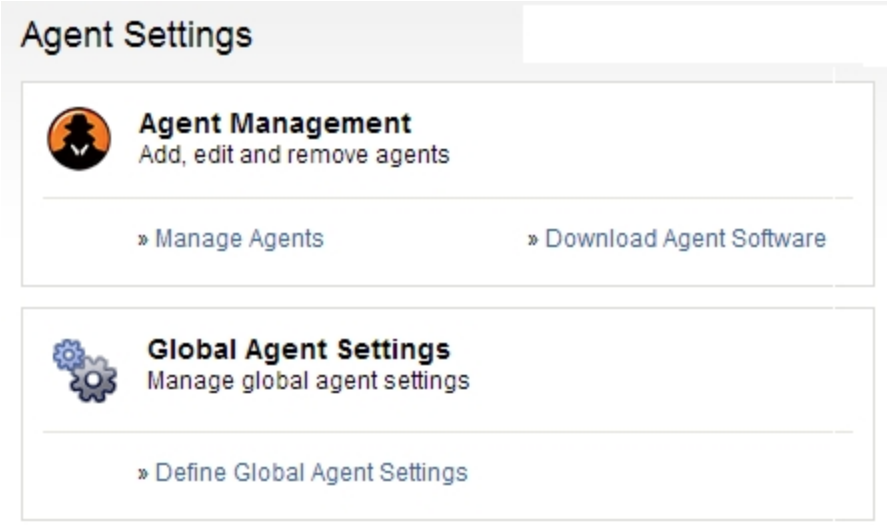
- **135:** Microsoft EPMAP (DCE/RPC Locator service). This port is required to be open on the client computer (Inbound) for remote deployment.
- **445:** Microsoft-DS SMB file sharing. This port is required to be open on the client computer (Inbound) for remote deployment.

Agent Settings

The *Agent Settings* page provides access to all of the settings and tools needed to install and manage agents.

Navigating to the Agent Settings page:

1. From the web console, navigate to **Settings > Agent Settings**.

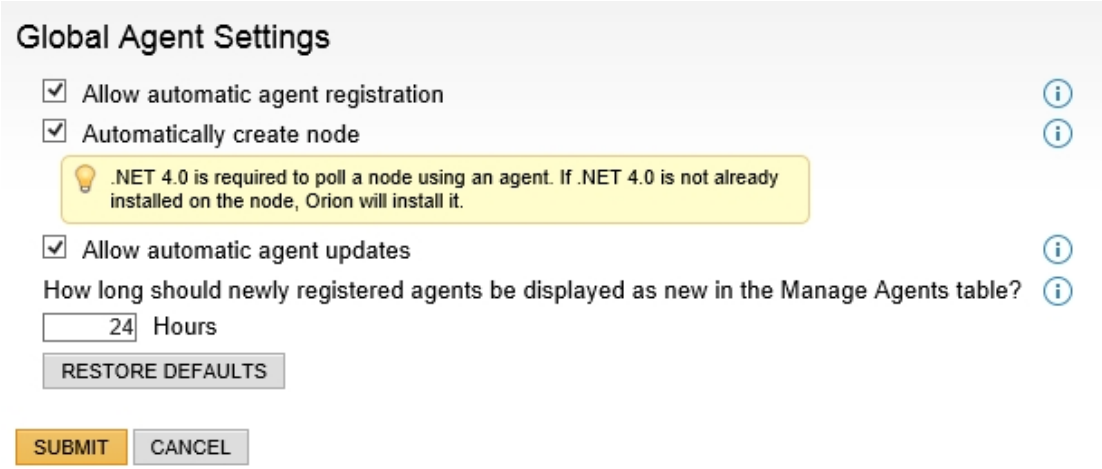


   - **Manage Agents:** Opens the *Manage Agents* page from which you can add a new agent, edit, update, or reboot an existing agent. For more information, see Managing Agents.
   - **Download Agent Software:** Opens the *Agent Downloads* page from which you can mass deploy or manually install an agent. For more information, see Deploying an Agent.
   - **Define Global Agent Settings:** Opens the *Global Agent Settings* page from which you can allow automatic agent registration and/or allow automatic agent updates.

Adjusting Global Agent Settings:

1. From the web console, navigate to **Settings > Agent Settings**
2. Click **Define Global Agent Settings** to be taken to the options illustrated

3. Select your choices. When done, click **Submit**.



   a. **Allow automatic agent registration:** Selecting this option will automatically register the agent, verifying communication with the Orion Server. If this option is disabled, you can register any waiting agents by navigating to **Settings > Manage Agents > Add Agent > Connect to a previously installed agent**.

   b. **Automatically create node:** Agents will automatically be registered as Orion nodes.

   c. **Allow automatic agent updates:** Selecting this option will allow the agent software to be automatically upgraded when updates become available. This process pushes a new version of the agent to client machines over the agent communication channel (no extra ports or permissions are needed). Once the agent receives the new version, it updates itself to the newer version. This process does not require rebooting.
   Note: If automatic updates are disabled and a new version of the software is installed on the server, it is possible that outdated agents will not be able to communicate with the server. Ensure that all agent versions match the version of the server.

   d. **XX Hours:** Allows you to control the length of time the agent will be displayed as being new in the **Manage Agents** table.

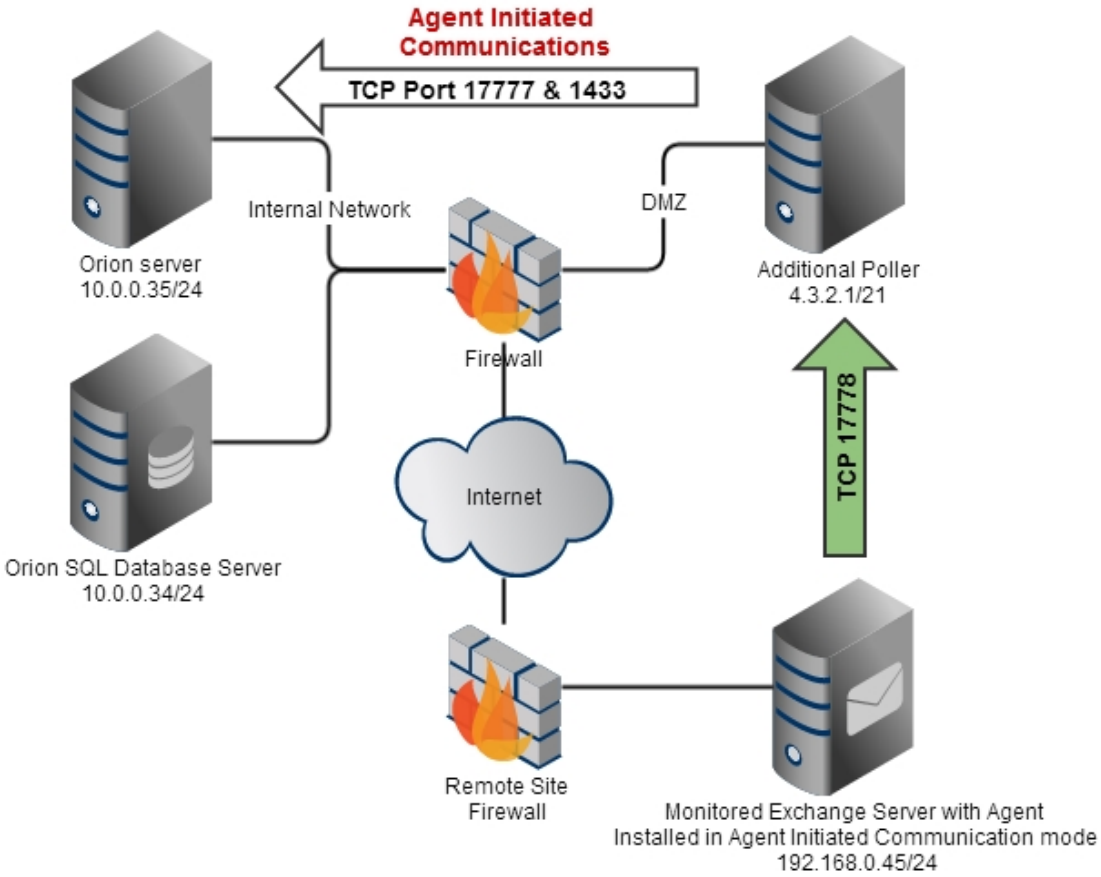
Server Initiated Communication

All communication between your SolarWinds Orion server or additional polling engine and the agent is initiated by the server, and the agent does not initiate communication to your SolarWinds Orion server. You do need to have a direct route from the server with the agent installed to your SolarWinds Orion server or additional polling engine. To use this communication method, port **17790** must be open on the remote host's firewall to retrieve information from the agent.

This communication method is also known as a passive agent.

Agent Initiated Communication

All communication between your Orion server or additional poller and the agent is initiated by the agent, and your SolarWinds Orion server does not initiate communication with your agent. You do not need to have a direct route from the server with the agent installed to your SolarWinds Orion server or additional poller. To use this communication method, port **17778** must be open on the SolarWinds Orion server firewall to receive information from the agent.



This communication method is most useful when the agent is installed on a network separated from your Orion server by one or more NAT devices, and you have no easy way to connect the two.

This communication method is also known as an active agent.

Deploying an Agent

Orion supports three methods of deploying an agent to a client computer running Windows.

1. Have the Orion Server push the agent software to one or more client computers
2. Mass deploy the agent software to multiple computers using a mass-deployment technology such as Group Policy
3. Manual installation of the agent on a client computer

For more information, see:

- Deploying Agent Software via Orion Server Push
- Mass Deploying an Agent
- Deploying the Agent Manually
- Packaging the Orion Agent for Deployment with SolarWinds Patch Manager
- Deploying with a Gold Master Image

Deploying Agent Software via Orion Server Push

Selecting this method of deployment allows you to perform a network-wide deployment from within Orion and does not require the downloading of additional files. In order for this deployment method to succeed, the Orion server must be able to communicate with the client computers.

Deploying Agent Software via Orion Server Push:

1. From the web console, click **Settings**, then click **Manage Agents**
2. On the *Manage Agents* page, click **Add Agent**
3. Select the method you would like to use to add the agent, and then click **Next**. Steps for both options follow.

   Deploying the Agent on my Network:

   Opting to deploy the agent on the network allows you to install the agent on multiple client computers. To do this, complete the following steps:

a. On the *Deploy Agent on Network* page, either enter the IP address or host name of the Windows computer where you want the agent to be installed, or select nodes from the list by checking their respective check boxes, and then click **Next**.
Note: This field does not accept ranges. It is used to add computers that are currently not nodes in the system.

b. On the *Agent Settings* page:

   i. Check the box of the computer you selected in the previous step, then click **Assign Credentials**

   ii. Choose a credential from the drop-down list, or enter new credentials, then click **Submit**.
   Note: You can assign credentials to multiple locations/nodes at one time by selecting multiple check boxes.

c. Click **Deploy Agent**. At this point, Orion is going to install the agent software

Connecting to a Previously Installed Agent:

If **Allow Automatic Agent Registration** is not enabled, use this method. To connect to a previously installed agent, complete the following steps:

a. On the *Add Agent* page, enter a name for the Agent, then select the agent from the Agent drop-down list.

b. Check **Allow automatic agent updates** to have the agent automatically upgraded when upgrading to new versions of Orion modules that support the agent. **Note:** Disabling this option will require you to manually upgrade agents after upgrading your Orion products and modules.

c. Click **Submit** to complete the process.

When the connection is successful, the agent will appear in the agent list on the *Manage Agents* page.

Troubleshooting Deployment

Following is a list of possible errors with their respective resolutions:

Credential test for deployment fails:

- Ensure that the used account can access the following folder: **\\<hostname_or_ip>\admin$\temp**. Also ensure that a folder can be created at that location.
- Ensure that *Remote Procedure Call* (RPC), a Windows service, is running
- Ensure the required ports are open
- If you are using a domain account, use the complete name when entering credentials. For example:
  Domain\Username

Agent deployment fails:

- Ensure there are no other installations in progress. For example, Windows updates and installations prevents other installations from finishing successfully. If this is the case, retry agent installation when other installations have completed.
- On the target machine, check if the *SolarWinds Agent* service is installed and running. If it is, the agent may be experiencing connectivity issues with the Orion server. Ping the Orion server from the client machine and ensure that port **17778** is open on the Orion server. Also check that the client machine can connect to the Orion server web interface.
- If possible, try to install the agent manually on the target machine, ensuring that permissions are set correctly.
  Note: Agent deployment failure can also occur if a previous installation or upgrade is awaiting a reboot. To resolve this issue you will need to reboot the server before the installation of the agent can proceed on that machine.

Deploying the Agent Manually

Selecting this method of deployment may be helpful in troubleshooting connectivity issues with another form of agent deployment.

Deploying the Agent Manually:

1. From the web console, navigate to: **Settings > Agent Settings > Download Agent Software**.

2. In the *Manual Installer* column, click **Download .MSI** to download the .MSI file on the source machine, as shown:

3. Download both the .MSI installer file and the .MST transform file.

   Note: If you prefer to install the agent silently, take the following optional two steps:

   a. Right-click `cmd.exe` and select **Run as Administrator**.
   b. Enter the following command and then press **Enter**:
   ```
   msiexec /i Solarwinds-Agent.msi /q
   TRANSFORMS=SolarWinds-Agent.mst
   ```

4. Enter the Orion server IP address or hostname and the Orion administrator account credentials during installation

When the installation is successful, the agent will appear in the agent list on the *Manage Agents* page.

Troubleshooting Deployment

Following is a list of possible errors with their respective resolutions:

Agent is not able to connect to the Orion server.

- Ensure that you can ping the Orion server from the client machine
- Ensure that port **17778** is open on the Orion server and that the client machine can connect to it
- Ensure that you are using the correct Orion administrator credentials

Mass Deploying an Agent

If you are already using a mass-deployment technology, this deployment method is an easy way to get agents on a large group of computers.

Note: Polling engine selection is important. When you click **Download .MST**, the MST file created includes the polling engine IP address and other vital information. When you deploy the agent using the MSI file, along with the MST file on the managed node, the agent will be installed and pointed to the correct polling engine.

Mass Deploying an Agent:

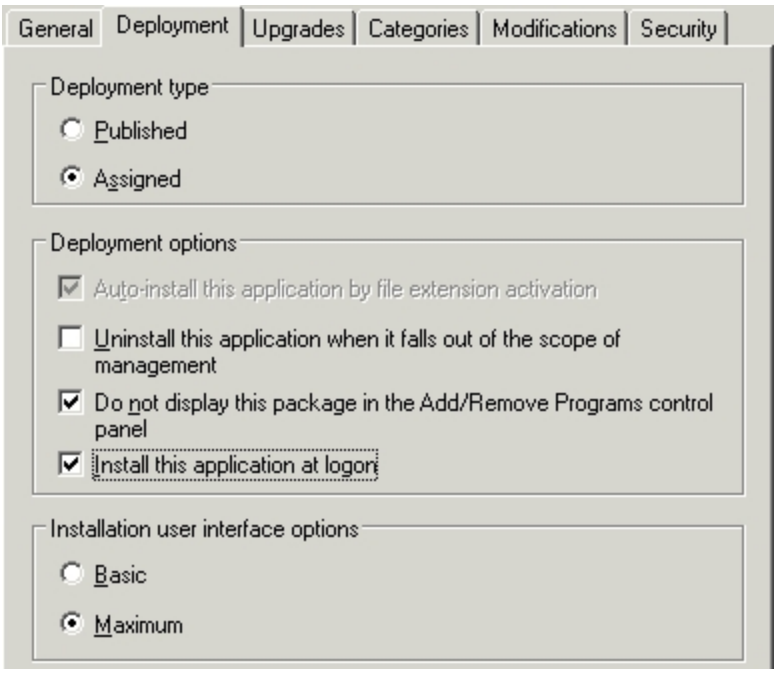
1. From the web console, navigate to **Settings > Agent Settings > Download Agent Software**.
2. In the **Mass Deployment Files** column, choose the agent communication mode. This information is included in the automatically generated .MST file.
    - For **Agent Initiated** communication, enter which polling engine you want the agent to use. You may need to manually enter the polling engine information if the IP address is different from what the SolarWinds Orion server reports.This happens when the monitored host is behind a NAT or proxy device. In these cases, enter the IP address of the SolarWinds Orion server or the additional polling engine as it is accessible from the host where the agent will be installed.
        a. To use a predefined polling engine, select **Use Connection Details from Polling Engine**, and then choose a polling engine from the drop-down menu.
        b. To manually enter the polling engine IP address, select **Enter Connection Details Manually**, and then enter both the host name and IP address. The IP address is required. Use the host name and IP address of the polling engine that the clients know.
    - For **Server Initiated** communications, enter your Agent Communication Port number. By default, this is port number 17790.
3. Select **Mass-Deployment (e.g. Group Policy)**.
4. Download *both* the **.MSI installer** file and the **.MST transform** file.

Adding the .MST file to a Group Policy:

1. Copy the software installation files (.msi, .mst) to a network share that is accessible to the hosts you where you wish to deploy the agent software.
2. Configure the permissions on the share to ensure that all required users and computers have Read access to the installation files.
3. Locate the container in Active Directory (a site, a domain, or an organizational unit (OU)) where you want to advertise the application and access the container properties.
4. Click the *Group Policy* tab.
5. Click **New** to create a new Group Policy (GPO).
6. Expand the **Computer Configuration\Software Settings** container in the **GPO** to reveal **Software Installation**, then right-click **Software Installation**.

7. Select **New**, and then select **Package**.
8. Select your MSI package, then select **Advanced** for the deployment method.

9. From the *Deployment* tab, check the **Deployment type/Deployment** options as shown.
   Note: Your deployment type/options may be different depending on your network.



10. From the *Modifications* tab, select your MST file from the network share.
11. Click **OK** to complete the setup. The agent is deployed and is registered by Orion (if auto-registration is enabled as defined in the Agent Settings page).

When the installation is successful, the agent will appear in the agent list on the *Manage Agents* page.

Troubleshooting Deployment

Following is a list of possible errors with their respective resolutions:

Agent deployment fails:

- On the target machine, check if the *SolarWinds Agent* service is installed and running. If it is, the agent may be experiencing connectivity issues with the Orion server. Ping the Orion server from the client machine and ensure that port **17778** is open on the Orion server. Also check that the client machine can connect to the Orion Server's web interface.

- If possible, try to install the agent manually on the target machine, ensuring that permissions are set correctly.
- If a host name or Fully Qualified Domain Name was used, ensure that it can be resolved from the client computer.
- If the Orion server or the additional poller is behind a NAT, ensure that the IP address specified in the creation of the MST file is the correctly routed IP address the client would use to access the Orion server.

Packaging the Orion Agent for Deployment with Patch Manager

The following guide assumes that you already have a working SolarWinds Patch Manager infrastructure.

Obtaining the Installer Files:

1. From the web console, log in using administrator credentials, then navigate to **Settings > Agent Settings > Download Agent.**
2. In the **Mass Deployment Files** column, select the appropriate **Polling Engine** and **Connection Details** from the drop-down list.
3. Download both the MSI and MST files and then save them to a known location on your Patch Manager Server.
   Note: Take note of the latest version listed under the .MSI File. This is needed for package creation in Patch Manager.
   Optional: Rename the *SolarWinds Agent* files to *SolarWinds Agent <version>* for easier tracking.

Building the Package:

1. Launch SolarWinds Patch Manager.
2. In the navigation pane, navigate to **Administration & Reporting\Software Publishing** and then click **SolarWinds, Inc. Packages**.

3. From the *SolarWinds, Inc. Packages Action Pane*, click **New Package**. This will launch the Patch Manager Package Wizard.

4. In the package information screen, enter the following general information for the package:

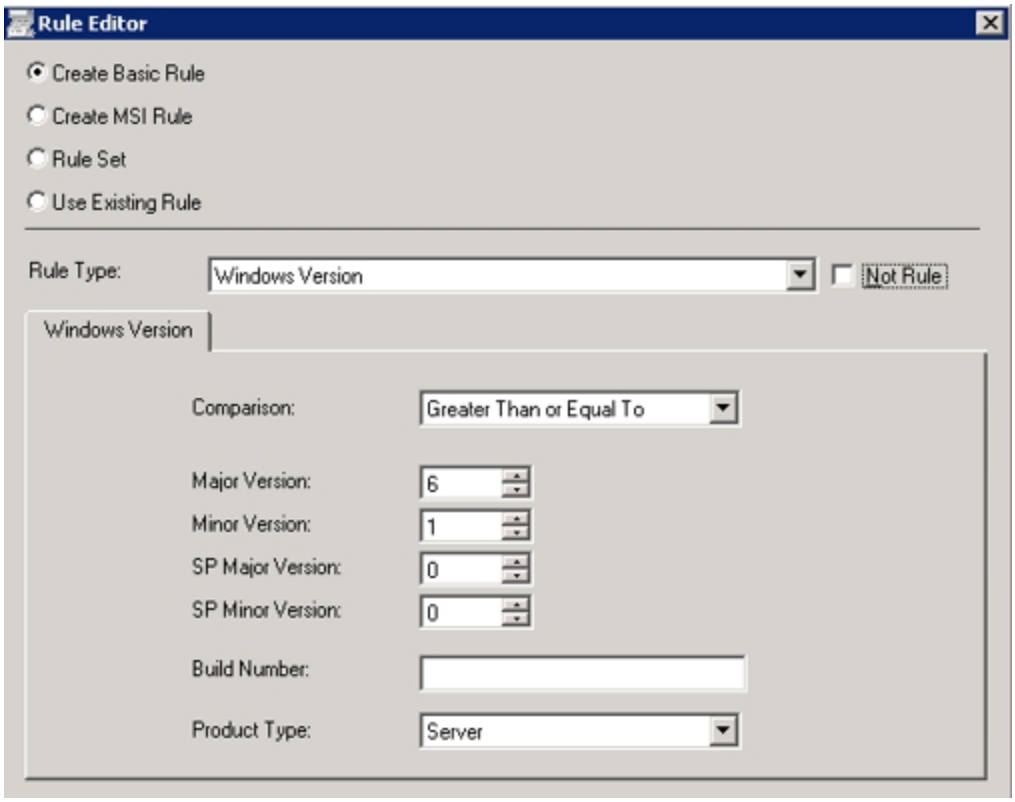
Field	Value	Comments
Package Title:	SolarWinds Orion Agent (Version Number) MSI	Replace “(Version Number)” with the actual version number of the agent software. See illustration.
Description:	SolarWinds Orion Agent	
Classification:	Tools	
Vendor:	SolarWinds, Inc.	
Product:	Orion Agent. (This must be entered manually the first time.)	
Severity:	None	
Impact:	Normal	
Reboot Behavior:	Can request reboot	

Note: All other fields can be left empty.

5. Click **Next**.

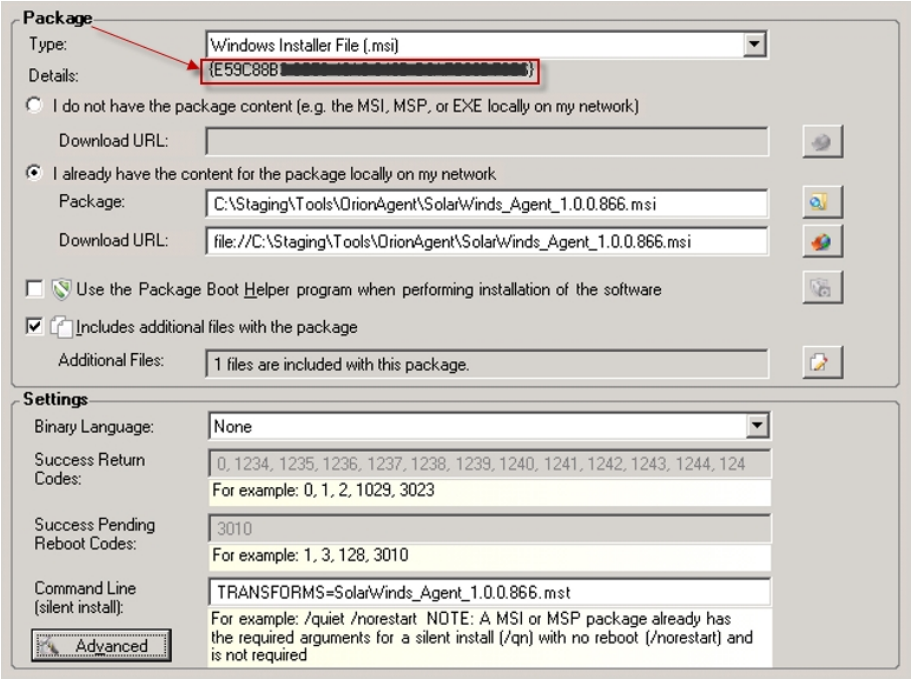
Add Deployment Rules:

1. On the *Prerequisite Rules* screen, click **Add Rule** then select *Windows Version* as the **Rule Type** and populate the remaining fields with the following information:



2. Click **OK** to save this rule, then click **Next**.
3. On the *Select Package* screen, select the **Package Type** as a *Microsoft Installer File (.msi)* and then select *I already have the content for the package locally on my network.*
4. Click the browse icon and locate the **MSI File for the Orion Agent**. The Download URL field will automatically populate.
5. The GUID product code is extracted from the MSI and displayed for review. Copy the GUID product code that will be used later.
   Note: The GUID is detected from the installer. Use the one displayed in your environment.

6. Check **Includes additional files with the package** and then click the button to the right to open the **Package Content Editor**.
7. Within the **Package Content Editor**, click **Add Files** and browse to the MST File for the Orion Agent.
8. Click **OK** to close the Package Content Editor. To confirm that you want to add these files to the cache, Click **Yes**.
9. Select **None** for the *Binary Language*.
10. In the *Command Line* field, enter: `TRASNFORMS=(MST FILE NAME)` (**Example:**"`TRANSFORMS=SolarWinds_Agent_1.0.0.866.mst`")

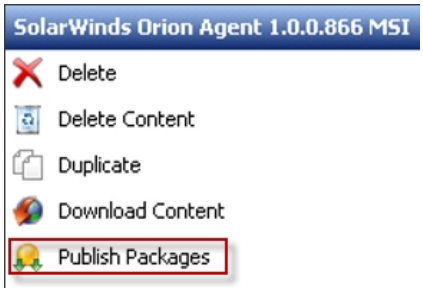


11. Click **Next**.
12. On the *Applicability Rules* screen, click **Add Rule**, then select **Create MSI Rule.**
13. Select **Rule Type:** *Product Installed* and then check **Not Rule**.
14. Enter the product code (without the braces) and leave all other fields empty.
15. On the *Installed Rules* screen, click **OK** to save the rule, and then click **Next**.
16. Click **Add Rule**, then select **Basic Rule.**

17. For the **Rule Type**, select *File Version with Registry Value.*
    a. For the **Registry Key,** enter: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SolarWinds\Agent`
    b. For the **Registry Value,** enter: `InstallDir`
    c. For the **Comparison,** select *Equal To.*
    d. For the **Version,** enter the version number for the agent. (For example: 1.0.0.866).
18. Click **OK** to save the rule, then click **Next.** Review the *Summary Page* and enter any notes at the bottom.
19. Click **Next** to save, then click **OK**.
    Note: You will be presented with a progress bar as the file is being packaged and uploaded. Upon completion, you will get a **Package Saved** dialog box.

Publishing the Package:

1. Within the *SolarWinds, Inc. Packages* view in Patch Manager, highlight the **SolarWinds Orion Agent** package that was created.
2. In the *SolarWinds Orion Agent Action Pane*, click **Publish Packages**.



3. Accept the default selections, or choose a specific WSUS server for publication.
4. Click **Next**.
5. You will be notified that the package has been published.
6. Click **Finish** to close the Publishing Wizard.

The Package for the SolarWinds Orion Agent has now been packaged and published to your WSUS server.

For more information on Approving and Deploying software, please see the *SolarWinds Patch Manager Administration Guide*.

Deploying with a Gold Master Image

A Gold Master Image is used when you want to maintain a master image that is copied when a new server is provisioned. This is useful for virtual machines, physical servers, and cloud instances. Whenever a new server is brought online using this image, the agent will already be installed.

To install the agent offline, take the following steps:

1. From the web console, navigate to **Settings > Agent Settings > Download Agent Software**.
2. In the **Mass Deployment Files** column, choose the agent communication mode. This information is included in the automatically generated files.
    - For **Agent Initiated** communication, enter which polling engine you want the agent to use. You may need to manually enter the polling engine information if the IP address is different from what the SolarWinds Orion server reports.This happens when the monitored host is behind a NAT or proxy device. In these cases, enter the IP address of the SolarWinds Orion server or the additional polling engine as it is accessible from the host where the agent will be installed.
        a. To use a predefined polling engine, select **Use Connection Details from Polling Engine**, and then choose a polling engine from the drop-down menu.
        b. To manually enter the polling engine IP address, select **Enter Connection Details Manually**, and then enter the host name and IP address. The IP address is required. Use the host name and IP address of the polling engine that the clients know.
    - For **Server Initiated** communications, enter your Agent Communication Port number. By default, this is port number 17790.
3. Select **Gold Master Image** and then click **Download Zip**.
4. Extract the contents of the .zip file.

5. Double click **Setup.bat.**
6. The installation wizard begins.
7. Click **Next.**
8. Select an installation folder by clicking **Change…**, or accept the default path, and then click **Next**.
9. When installation is complete, click **Finish**.

If you are deploying a Server initiated agent, take the following steps to enable agent communication with your SolarWinds Orion server.

To enable Server initiated communication on deployed agents:

1. From the web console, navigate to **Settings > Manage Agents**.
2. Click **Add Agent > Connect to a previously installed agent**.
3. Enter a name for the Agent
4. Select **Server Initiated Communication**.
5. Enter the IP address of the node where the agent is deployed as well as the port number for the agent (Default value is **17790**.)
6. Click **Submit**.

Deploying on Windows Core Servers

If installing the agent on a Windows Core Server, .Net 4.0 is required to be manually installed.

Important: Make sure that your computer has the latest Windows service pack and critical updates installed.

To Install the Agent on a Windows Core Server:

1. Right-click `cmd.exe` and click **Run as Administrator**.
2. Turn on WoW64 by entering the following command:

   ```
   Start /w ocsetup ServerCore-WOW64
   ```

3. Turn on the.NET 2.0 layer by entering the following command:

   ```
   Start /w ocsetup NetFx2-ServerCore
   ```

4. Turn on .NET 2.0 layer for WoW64 by entering the following command:

   ```
   Start /w ocsetup NetFx2-ServerCore-WOW64
   ```

5. Download the .NET Framework from the following location: http://www.microsoft.com/en-us/download/confirmation.aspx?id=22833

   Note: By default, no web browser is installed with Windows Core. Consider using FTP or a flash drive to import the necessary files.

6. Once the .NET Framework is installed, you may need to reboot the host server. The agent can then be deployed to the host server and operate normally.

Deploying Agents in the Cloud

Agents can be deployed in the cloud for use with Amazon Web Services, Microsoft Azure, and other third party cloud storage services. Use the following topics to learn about deploying an agent in common cloud storage services:

- Manually Deploy an Agent on Amazon Web Services
- Automatically Deploy an Agent on Amazon Web Services
- Automatically Deploy an Agent on Microsoft Azure

Manually Deploy an Agent on Amazon Web Services

You can manually deploy agents to a virtual machine using RDP and install both the **.MSI installer** file and the **.MST transform** file.

Requirements for manual agent deployment:

- **Agent Initiated Communication:** The poller must have a public IP address which is visible from the node that will have the agent installed. Port **17778** must be open on the poller.
- **Server Initiated Communication:** The node where the agent will be installed must have a public IP address. Port **17790** must be open.

You can manually deploy the agent in one of two ways:

- Silently via the Command Line Interface
- Manually using the Interactive Wizard

To manually install the .MSI and .MST files via the Command Line Interface:

1. From the Web Console, navigate to: **Settings > Agent Settings > Download Agent Software**.
2. In the *Mass Deployment Files* column, download both the .MSI installer file and the .MST transform file by clicking their respective buttons.
3. Open a command prompt in the administrator context. (Right-click `cmd.exe` and select, **Run as Administrator**.)
4. Enter the following command and then press **Enter**:
   ```
   msiexec /i "SolarWinds-Agent.msi"
   TRANSFORMS="SolarWinds-Agent.mst"
   ```

Deploying the Agent Manually using the Interactive Wizard:

1. From the Web Console, navigate to: **Settings > Agent Settings > Download Agent Software.**
2. In the Manual Installer column, click **Download .MSI** to download the .MSI file on the source computer.
3. Once download is complete, copy the .MSI file to the client machine and then install it by double clicking it and beginning the wizard.
4. During installation, select either **Agent Initiated Communication (Recommended)** or **Orion Server Initiated Communication**. When done, click **Next**.
5. Enter the **Orion server IP address** or **Hostname** and the Orion administrator account credentials (Username and Password) during installation.
6. When done, click **Next** and complete the wizard as needed.

Automatically Deploy an Agent on Amazon Web Services

You can automatically deploy an agent from Amazon Web Services.

To automatically deploy an agent on Amazon Web Services:

1. From the Web Console, navigate to: **Settings > Agent Settings > Download Agent Software**.

2. In the *Mass Deployment Files* column, download both the .MSI installer file and the .MST transform file by clicking their respective buttons.
3. Once download is complete, login to your AWS S3 account.
4. From the Amazon Web Services console, click **S3** under the *Storage & Content* category.
5. Click, **Create Bucket** to create a storage space for both the .MSI installer file and the .MST transform file.
6. Click on the newly created bucket in the list.
7. Click **Actions > Upload > Add Files** to upload both the .MSI installer file and the .MST transform file. When selected, click **Start Upload**.
8. On your virtual machines, create a custom PowerShell script to be used on each virtual machine where you want the agent installed. This script will run on the virtual machines when it is launched for the first time, downloading and executing the agent.
   Note: For information on creating a PowerShell script, refer to the following article:
   http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/UsingConfig_WinAMI.html#user-data-execution.
9. Login to your Amazon Web Services account:
   Note:Steps 10-11 can also be accomplished via the API or AWS Command Line Interface.

10. To create an instance, take the following steps:
    a. From the Amazon Web Services console, click **EC2** under the *Compute* header.
    b. Expand Instances from the *Navigation Bar*¸ and then click **Instances**.
    c. Click, **Launch Instance**.
    d. Select a Windows computer from the list by clicking, **Select**.
    e. Check the box of the desired Windows computer.
    f. Click **Next: Configure Instance Details**.
    g. Expand **Advanced Details**.
    h. Paste you PowerShell script in the **User Data** text box with the **As Text** option selected.
    i. Complete the wizard as needed, or click **Review and Launch**.
11. For instances that are already created, take the following steps:
    a. Stop the instance where you want to deploy the agent
    b. Right-click the instance and navigate to **Instance Settings > View/Change User Data**.
    c. Paste you PowerShell script in the text box as **Plain Text**.

Automatically Deploy an Agent on Microsoft Azure

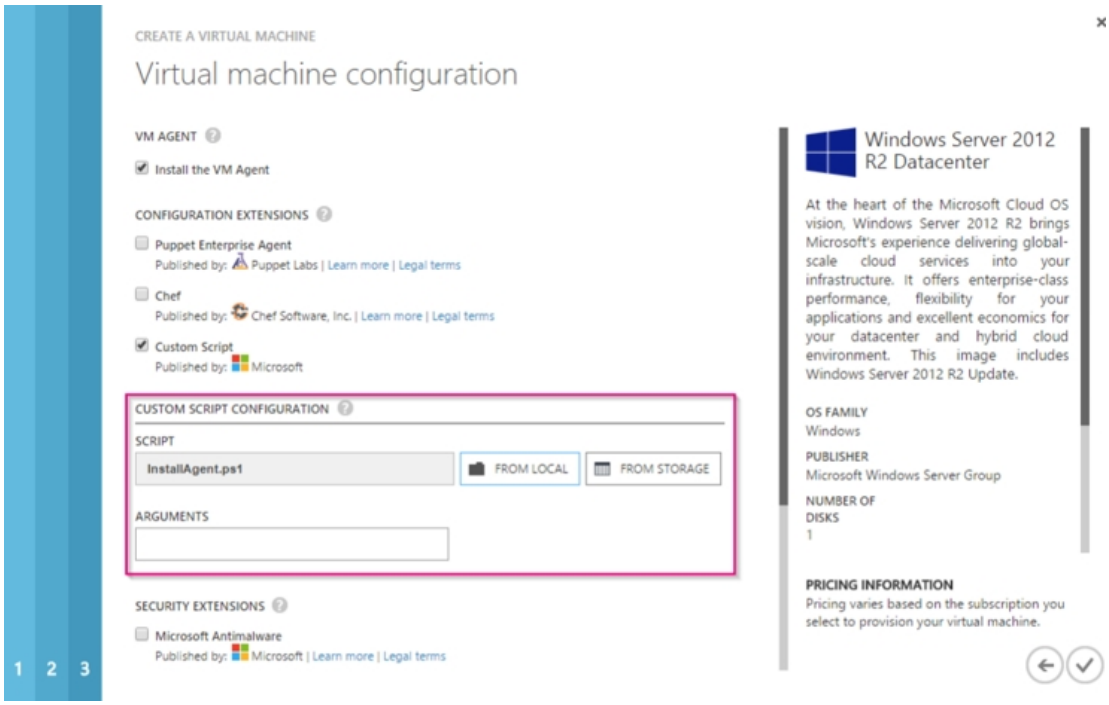
You can automatically deploy an agent from Microsoft Azure.

To Automatically Deploy Agents to Virtual Machines on Microsoft Azure:

1. From the web console, navigate to: **Settings > Agent Settings > Download Agent Software**.
2. In the *Mass Deployment Files* column, download both the .MSI installer file and the .MST transform file by clicking their respective buttons.
3. Upload both the .MSI installer file and the .MST transform file to your Azure Blob Storage. (You can use AzCopy to upload files to Azure Storage: http://azure.microsoft.com/en-us/documentation/articles/storage-use-azcopy/)

4. Create a custom PowerShell script to be used on each virtual machine where you want to install the agent. This script should be set to execute the downloading of the agent software to the virtual machine when the virtual machine is launched for the first time. For information on creating a PowerShell script, refer to section titled, **Use Case 1: Uploading files to a container in the default account** in the following article: http://azure.microsoft.com/blog/2014/04/24/automating-vm-customization-tasks-using-custom-script-extension/

5. Add your custom PowerShell script to virtual machines manually on last step of their creation in the Azure management portal, as shown:



Note: This step can also be accomplished via the API or AWS Command Line Interface.

Managing Agents

Most tasks related to managing agents can be done from the **Manage Agents** page, located on the **Settings** page. From this page, you can check agent connection and deployment status.

The following tools for the **Manage Agents** page are listed below:

Manage Agent Toolbar:

- **Add Agent:** Takes you to the **Add Agent** page, allowing you to choose to deploy the agent on a network, or connect to a previously installed agent.
- **Edit Settings:** Takes you to the **Edit Agent Settings** page, allowing you to adjust the agent name and automatic updating.
- **Delete:** Deletes the agent from the Orion server but does not uninstall it. Uninstalling the agent needs to be done manually
- **Choose Resources:** Displays a list of resources and statistics to monitor. This is only available for agents that are also nodes.
    - For a Single Agent: This will take you to the List Resources page, allowing you to choose items on the node you wish to monitor.
    - For Multiple Agents: From here, Orion will discover available resources on the agents you have selected using Network Sonar Discovery. From here, you can choose items on the nodes you wish to monitor
- **Manage as Node:** Manage the agent as a node. This button is active when one agent is selected that is not yet monitored as a node.

- **More actions:**
  - **View installed agent plug-ins:** Displays a list of plug-ins installed on the selected agent.
  - **View installed plug-ins report:** Displays a list of agent plug-in versions installed on all registered agents.
  - **Retry agent installation:** Will attempt to install the agent in the event of a file transfer timeout due to network connectivity issues.
  - **Reboot Agent Machine:** Reboots the server that hosts the selected agent.
    Note: This button is disabled by default. It becomes enabled when the installation of an agent requires a system reboot.
  - **Update:** Updates the agent software to the latest version available.
    Note: This button is disabled by default. It becomes enabled when:
    - Automatic updates for the agent is disabled.
    - The selected agent requires an update.
  - **Reconnect to passive agent:** If the connection to the agent management service is lost, for example, an agent was reinstalled manually, then this option allows you to manually trigger a connection to the agent rather than waiting for a regularly scheduled connection.

The available columns for the **Manage Agents** page are listed in the following table:

Agent/Node	Name or IP address of the listed node.
Agent Status	Current status of the listed agent. Agent Status can be as follows: • **Connected/OK:** Everything is working • **Unknown:** Agent is connected but no communication is received • **Update Available:** Agent version is older than the version on server and should be updated. • **Update in Progress:** Agent is currently being updated.

	• **Reboot Required:** Agent needs to be rebooted in order to finish the installation of plugins. • **Reboot in Progress:** Agent is currently being rebooted. Once reboot is complete, the agent should finish installation of plugins. • **Reboot Failed:** Agent cannot be rebooted. It may be temporarily offline or there may be some other issue. • **Plugin Update Pending:** A plugin on the agent has an older version than the one that is on the server and should be updated.
Connection Status	Current connection status of the listed agent. Connection status can be as follows: • **Connected/OK:** Connected • **Unknown:** The agent management service is not running • **Service not Responding:** The agent management service is running, but the agent is not connected • **Deployment Pending:** An agent deployment is going to start, but has not started • **Deployment In Progress:** The agent is being deployed to the target node • **Deployment Failed:** Agent deployment failed for various reasons • **Invalid Response:** The status displayed if the agent responds in an unexpected manner • **Waiting for Connection:** The agent was approved, but has yet to connect to the Orion Server
Registered On	Date when the agent was added to the agent management system.
Mode	Agent communication type:

	• **Agent initiated:** The agent initiates the connection to the agent management system. • **Server initiated:** The agent behaves as a web server and the agent management system initiates the connection.
Version	Version of the agent software. This is helpful in determining which agents should be updated.

For more information, see Agent Requirements.

Editing Agent Configuration

Editing an agent's configuration may be necessary if you experience problems and need to collect diagnostics.

To change these settings, take the following steps:

Editing Agent Configuration:

1. From the web console, navigate to **Settings > Agent Settings > Manage Agents**.
2. On the *Manage Agents* page, select an agent and then click **Edit Settings**.
3. Check **Allow automatic agent updates** to allow automatic updates to the agent.
4. Expand the **Troubleshooting** heading.
    a. **Optional:** Select a Log level. The default is *INFO*.
    b. Click **Download** to download the most recent troubleshooting files, or click **Collect new diagnostics** to generate current diagnostics.
5. When done, click **Submit**.

Tracking Your Polling Method

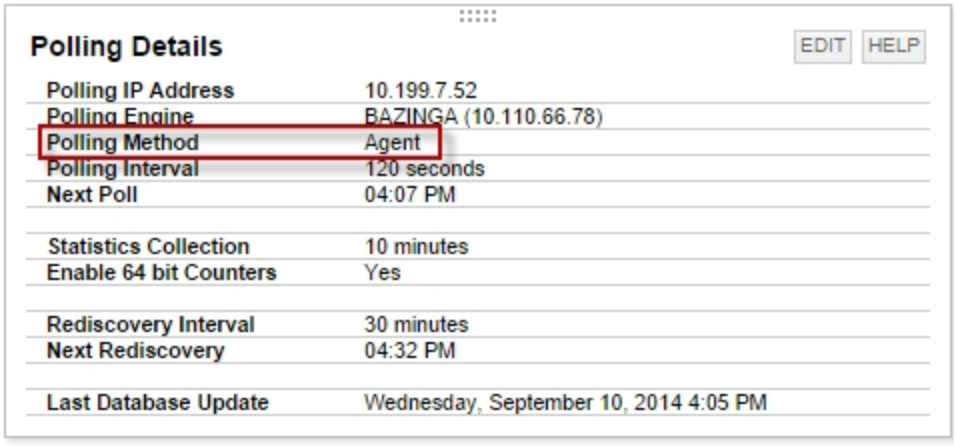
If different nodes are using different polling methods, you may want to keep track of which node is using which polling method for troubleshooting purposes. There are several methods you can use to identify the polling method of nodes:

- On the *Node Details* page (View individually)
- On the *Application Details* page (View individually)

- On the *Manage Nodes* page (View as a list)
- Creating a report to identify Agent usage

Identifying the polling method from the *Node Details* page:

1. From the web console, navigate to the *Home* tab.
2. In the **All Nodes** resource, expand a node tree and click a node to be taken to the *Node Details* page.
3. On the **Polling Details** resource, find the **Polling Method** field, as shown:

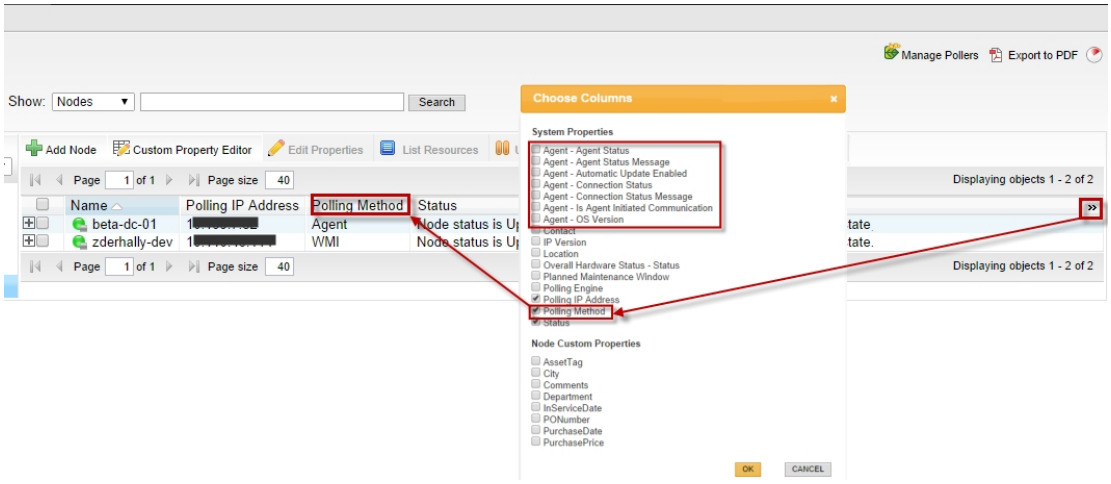


Identifying the polling method from the *Application Details* page:

1. From the web console, navigate to the *Application* tab.
2. In the **All Applications** resource, expand an application tree and click an application to be taken to the *Application Details* page.
3. In the **Management** resource, click **Edit Application Monitor**.
4. Expand the **Advanced** tree to reveal the polling method being used.

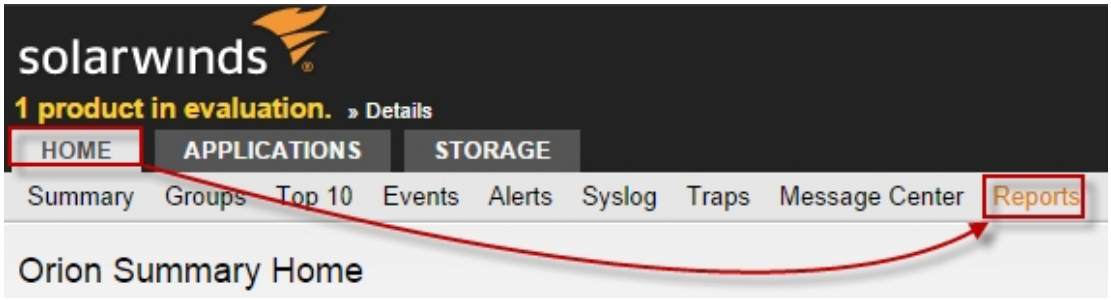
Identifying the polling method from the *Manage Nodes* page:

1. From the web console, navigate to **Settings > Manage Nodes**.
2. If not already visible, add the **Polling Method** field by clicking **>>** at the top-right of the table, as shown:
   Note: Once added, the fields can be sorted by clicking their respective column heads.



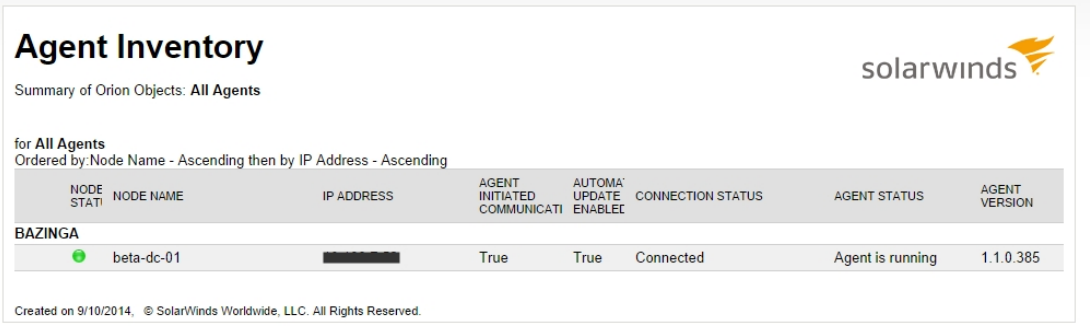
Creating a report to identify Agent usage:

1. From the web console, navigate to **Home > Reports**.



2. Search for *Agent* in the Search box.
3. Select the **Agent Inventory** report.
4. Click **View Report**, as shown above.

5. Your report should look similar to the following:



Agent Inventory

Summary of Orion Objects: **All Agents**

solarwinds

for **All Agents**
Ordered by:Node Name - Ascending then by IP Address - Ascending

NODE STATI	NODE NAME	IP ADDRESS	AGENT INITIATED COMMUNICATI	AUTOMA UPDATE ENABLEI	CONNECTION STATUS	AGENT STATUS	AGENT VERSION
BAZINGA							
	beta-dc-01	[redacted]	True	True	Connected	Agent is running	1.1.0.385

Created on 9/10/2014, © SolarWinds Worldwide, LLC. All Rights Reserved.

Installed Agent Plug-in Status

Use the following table to understand the agent plug-in status.

Status	Meaning
The plug-in is installed	The plug-in is installed, working correctly, and communicating with no problems.
Installation Pending	The plug-in is waiting to be deployed. It may be waiting for the computer it is installed on to reboot or because some other process on the remote host has interrupted the installation process.
Unknown	The status is unknown due to networking interruptions, communication problems with the agent, or because the plug-in is no longer installed.
Error	The plug-in may have installed incorrectly or failed to load.
In Progress	The plug-in is either being installed or uninstalled.

If you think a plug-in should be available and cannot find it in the list of installed plug-ins, you may need to check your purchased products or manually update your agent. New plug-ins and updates to existing plug-ins are installed when an agent is updated. It may take a few minutes before the status changes.

Editing Agent Settings in the Control Panel

If the agent loses connectivity to the Orion server, or is unable to connect after being manually installed, you can still configure the agent's settings via the Windows Control Panel that will allow the agent to re-connect to the Orion server.

Settings for the agent for the local computer can be found in the Windows Control Panel. This is installed on the server where the Agent is installed.

Editing Agent Settings with the Control Panel:

1. Navigate **to Start > Control Panel > Orion Agent Settings**.
2. Double-click the **Orion Agent Settings** icon.
3. Select and **Agent Communication Mode**:
   - **Agent initiated Communication**: Also known as an Active Agent.
   - **Server Initiated Communication**: Also known as a Passive Agent.
4. Complete the **Connection Settings** field as necessary to your environment.

   Note: A field for an Agent Passphrase (shared secret) is provided for security. When the agent is installed, you must set a passphrase. When the SolarWinds Orion server connects to that agent, it verifies the passphrase to successfully connect.

   - Both **Agent initiated Communication** and **Server Initiated Communication** offer the use of an optional proxy. To access the proxy settings, click **Proxy Settings**. Fill out the fields as needed and then click **OK**.
5. When done, Click **OK**.

Connecting to a Previously Installed Agent

You can connect to agents that you have installed previously or modify the agent's assigned polling engine. The steps are different depending on the agent communication mode. You should confirm the agent communication mode before you try to connect to it.

To connect to a agent using agent initiated communication:

1. On the *Add Agent* page, enter the name of the agent you want to connect to.
2. Select **Agent-initiated communication**.
3. Select the agent from the **Agent** drop-down list.
4. Expand **Advanced** to change the proxy.
5. Select **Allow automatic agent updates** to have the agent automatically upgraded when upgrading to new versions of SolarWinds modules that support the agent.
   Note: Disabling this option will require you to manually upgrade agents after upgrading your SolarWinds products and modules.
6. Click **Submit** to complete the process.

When the connection is successful, the agent will appear in the agent list on the *Manage Agents* page.

To connect to a agent using server initiated communication:

1. On the *Add Agent* page, enter the name of the agent you want to connect to.
2. Select **Server initiated communication**.
3. Enter the IP address or hostname of the remote computer on which the agent is installed.
4. Expand **Advanced** to change the default port number, assign the agent to a different poller, or use a proxy to connect to the agent.
5. To view the poller, click **Advanced**.
6. Select **Allow automatic agent updates** to have the agent automatically upgraded when upgrading to new versions of SolarWinds modules that support the agent.
   Note: Disabling this option will require you to manually upgrade agents after upgrading your SolarWinds products and modules.
7. Click **Submit** to complete the process.

When the connection is successful, the agent will appear in the agent list on the *Manage Agents* page.

Changing Agent Communication Modes

You can change how the SolarWinds agent communicates with the SolarWinds Orion server.

To switch between Server initiated mode and Agent initiated mode:

1. For nodes polled through the agent, from the web console, navigate to the *Node Details* page:
    a. **Home > Node**.
    b. From the **Management** resource, click **Edit Node**.
    c. Select the **WMI** option, enter your WMI credentials, and then click **Submit**.
2. Navigate to the **Agent Management** page and delete the Agent record:
    a. From the web console, navigate to **Settings > Manage Agents**.
    b. Check the box next to the **Agent** you want to uninstall, and then click **Delete** on the toolbar. Confirm deletion when prompted.
3. Install the Agent in the desired mode.
    a. From the web console, navigate to **Settings > Manage Agents > Add Agent > Deploy the agent on my network**.
    b. Select the desired node by checking its box, then click **Next**.
    c. Assign credentials then select the agent mode, **Active** or **Passive**.
        - **Active:** The Agent initiates communication with the server on port **17778**. This port must be opened on the server firewall so the Agent can connect. No change to the Agent firewall is required.
        - **Passive:** The Agent waits for requests from the server on a specified port. This port must be opened on the Agent computer's firewall so the server can connect. No change to the server firewall is required.
    d. Click **Deploy agent**.

4. Once the Agent is installed, navigate to the **Node Details** page:
    a. **Home > Node**.
    b. From the **Management** resource, click **Edit Node**.
    c. Change the polling method from **WMI** to **Agent**, then click **Submit**.

Changing the Agent Port

To change the default port for agent communication:

1. On the server with the agent, edit the following configuration file using a text editor:
   `c:\Program Files (x86)\SolarWinds\Orion\AgentManagement\SolarWinds.AgentManagement.ServiceCore.dll.config`
2. Change the port number in the following tag to the desired port number:
   `<agentManagementServiceConfiguration messagingPort="17778" />`
3. Save your changes. Once the port is changed, the agent can start using the new port number.
4. Restart the **SolarWinds Orion Module Engine** service.

Notes:

- If you installed the agent manually, you can change the port number during installation through the wizard in the web console.
- If you deployed the agent from the server, the port number is set automatically.
- If you used the .MST file for deployment for mass-deployment, you will need to download a new .MST file from the server after the port number was changed.

To change the default port on agents that have already been deployed:

1. The port number can be changed by navigating to **Start > Control Panel > Orion Agent Settings**.

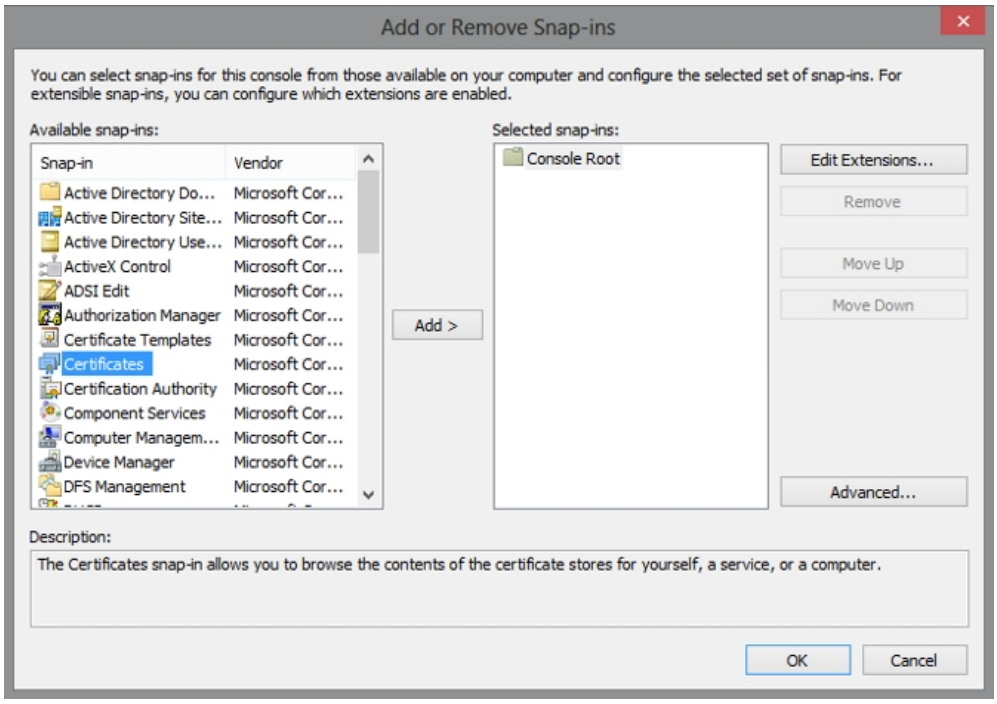
2. In **Orion Agent Settings**, enter a new port number in the field provided.
3. Click **OK**.

Certificates and the Agent

The Verisign Root Certificate Authority (CA) must be current. This is required because the agent software is signed using a Verisign certificate. If your certificate is not current, you will need to manually download the Root CA certificate and install it into the *Local Computer\Trusted Root Certification Authority* store on the server hosting the agent. The entire Verisign root certificate package can be downloaded from the following link.
http://www.verisign.com/support/roots.zip.

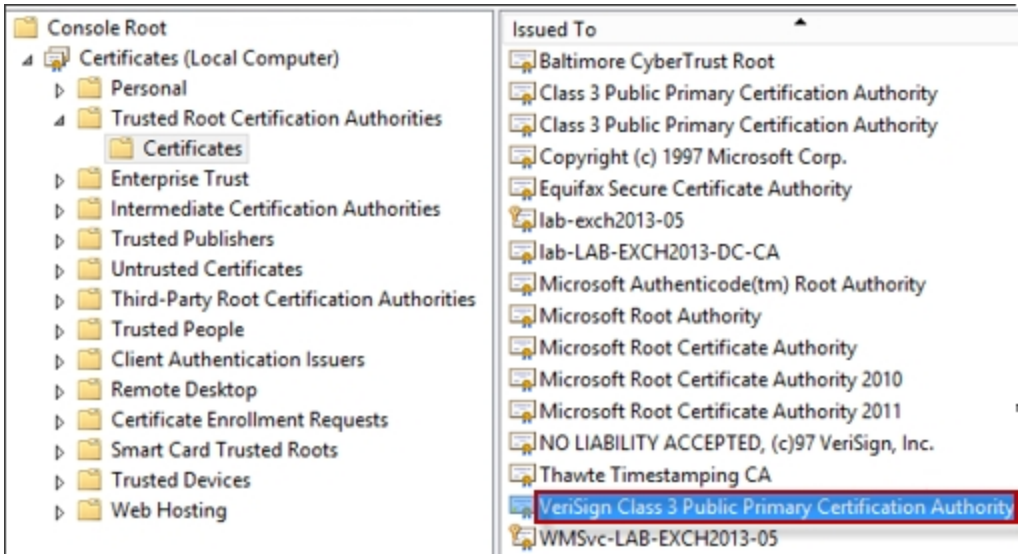
Installing a new Certificate:

1. Open a new Microsoft Management Console (MMC) by navigating to **Start**, then type *MMC* followed by **Enter.**
2. In the MMC, click **File > Add/Remove Snap-in…**
3. Add the Certificates Snap-in.



4. Select **Computer Account**, and then click **Next**.
5. Ensure **Local Computer** is selected. (The computer this console is running on).

6. Click **Finish**.
7. Click **OK** to add the snap-in into the MMC window.
8. Expand the certificate store tree.
9. Right click the **Trusted Root Certification Authorities** store.
10. Select **All Tasks/Import** to import the previously downloaded certificate(s).
11. Follow the prompts of the wizard to import the certificate(s).
12. Verify the **VeriSign Class 3 Public Primary Certification Authority – G5** certificate is present in the **Trusted Root Certification Authorities** store (It is recommended that you import all missing Root CA certificates).



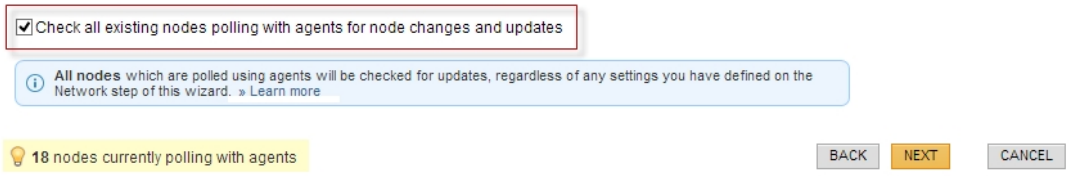
Using the Agent Polling Method

An agent is software that provides a communication channel between the SolarWinds Orion server and a Windows computer. Agents are used to communicate the information that SolarWinds plug-ins collect to the SolarWinds Orion server. For more information about the polling method, see Choosing Your Polling Method.

When the Agent Polling Method is selected, an agent is deployed to the node and installed using the credential you have selected. After the agent is installed, it operates under a local account.

Using the Network Sonar Wizard to Check Agent Polled Nodes

Agent discovery allows you to keep nodes that utilize the agent up to date. Checking this box allows the Orion server to find new volumes, interfaces, and other objects on nodes that use the agent.



While normal discovery finds new nodes and adds them to the Orion server, this is not true for nodes using the agent. Agent discovery is simply an extension to the standard discovery process.

A discovery profile may contain:

- Nodes using both the agent and non-agent nodes;
- Non-agent nodes
- Agent nodes

Agent Performance Counters

The following performance counters are associated with the agent:

SolarWinds: Agent Service

- **Messages Sent:** This counter displays the number of messages sent to the **Agent Management Service**.
- **Messages Received:** This counter displays the number of messages received from the **Agent Management Service**.
- **Exchange Received:** This displays the number of times the **Exchange Receive** method was called.
- **Exchange Sent:** This displays the number of times the **Exchange Send** method was called.

SolarWinds: Agent Management Service

- **Messages Sent to Agent Count:** Number of messages sent to the Agent.
- **Messages Received From Agent Count:** Number of messages received from the Agent.
- **Incoming Timed Out Messages Count:** Number of incoming messages that timed out before being processed by the recipient.
- **Outgoing Timed Out Messages Count:** Number of outgoing messages that timed out before they were sent to the target agent.
- **Incoming Failed Messages Count:** Number of incoming messages that failed to be processed.
- **Outgoing Failed Messages Count:** Number of outgoing messages that failed to be processed.
- **Total Agents Fully Connected:** Number of Total Agents Fully Connected.
- **Active Agents Fully Connected:** Number of Active Agents Fully Connected
- **Passive Agents Fully Connected:** Number of Passive Agents Fully Connected.
- **Passive Agents Disconnected:** Number of Passive Agents Disconnected.

- **Total Agents Connected To Messaging Hub:** Number of Agents Connected To the Messaging Hub.
- **Total Agents Connected To Files Hub:** Number of Agents Connected To the Files Hub.
- **Messages Processed Per Second:** Messages processed/sec.
- **Incoming Messages Processed Per Second:** Incoming messages processed/sec.
- **Outgoing Messages Processed Per Second:** Outgoing messages processed/sec.
- **Incoming Processing Queue Size:** Number of messages waiting in the incoming processing queue.
- **Outgoing Processing Queue Size:** Number of messages waiting in the outgoing processing queue.
- **Incoming Persistence Queue Size:** Number of messages waiting in the incoming persistence queue.
- **Outgoing Persistence Queue Size:** Number of messages waiting in the outgoing persistence queue.
- **Incoming SignalR Messages:** Number of messages received from SignalR.
- **Outgoing SignalR Messages:** Number of messages passed to SignalR for sending.
- **Incoming Exchange Queue Size:** Number of messages in the incoming queue with Exchange items.

Troubleshooting Agents

The most common issues with agents occur when they are installed or when you configure them. Agents may also be unable to connect to the SolarWinds Orion server or the server may not be able to connect to the agents.

For more troubleshooting information, use the following topics:

- Troubleshooting Your Agent Installation
- Troubleshooting Agent Configuration
- Troubleshooting Agent Connections

For information about what a plug-in status means, see Installed Agent Plug-in Status.

Troubleshooting Your Agent Installation

If your agent does not deploy correctly, use the following questions to help you troubleshoot the issue. You can also install the agent manually on the target computer.

Are you installing other software on the target computer?

Some software installations, such as Windows Updates, prevent other installations from finishing successfully.

Install the agent when the other installations have completed.

Is the target computer waiting to be restarted?

Deployment can fail when the computer is waiting to be restarted after installing software.

Restart the computer and try again.

Is the SolarWinds Agent server already installed and running on the target computer?

The agent may have connectivity issues.

Can you ping the SolarWinds Orion server or connect to the Web Console from the target computer?

The SolarWinds agent requires port 17778 to be open on the server.

Verify that the Orion server can ping the computer that has the agent is installed.

Note: This is not required for server initiated agents.

Do you use group policies in your organization?

You may have a network policy that interferes with deploying agents.

Troubleshooting Agent Configuration

The following sections will help you identify and correct Agent errors concerning configuration.

Passive Agent: Connection Refused

Error: *Connection refused.*

Resolution: Specify an Agent shared secret to connect to a passive Agent or specify a proxy. Also, verify that the agent port is accessible.

Passive Agent: Agent is not running in passive mode

Error: *Agent is not running in passive mode.*

Information: The agent is running in agent initiated communication mode and you cannot connect to it.

Resolution: Switch the communication mode to server initiated communication. You can uninstall and reinstall the agent from the server or manually re-install it. For more information, see Deploying an Agent.

You can also change the communication mode on the remote host by opening the Control Panel, and then opening the **Orion Agent Settings** item.

Invalid Agent Version

Error: *Agent is not running in passive mode.*

Information: Agent version is empty or zero. This indicates that something is wrong with the agent.

Resolution: Re-install the agent.

For more information, see Deploying an Agent.

Agent GUID is Different

Error: *Agent GUID is different than the requested ID.*

Information: That means that the agent is probably connected to another Orion server or is broken.

Resolution: Re-install the agent.

For more information, see Deploying an Agent.

Troubleshooting Agent Connections

If your agent and your SolarWinds Orion server cannot communicate, the agent cannot respond to queries or the SolarWinds Orion server cannot receive data from the agent.

Note: You need access to the remote host for most troubleshooting steps.

Use the following questions to help you troubleshoot the connection issue:

Is the agent service running?

You can check the Manage Agents page for the **Agent Status** or logon to the remote host with the agent installed on it to check the status.

If the agent is not running or has stopped, start the **SolarWinds Agent Service**.

Are all plug-ins installed correctly?

Select the agent in the Manage Agents page and click **More Actions > View installed agent plug-ins**.

If there is a problem with a plug-in, restart the agent. The agent checks for new plug-ins when it restarts.

Do the communication modes match between the agent and the server?

On the remote host, open the Control Panel, and then open the **Orion Agent Settings** item. The communication mode listed there must match the communication mode in the Manage Agents page on the SolarWinds Orion server.

If the modes do not match, change one to match the other.

Does the server initiate communication?

Logon to the server host and attempt to ping the remote host.

Server initiated communication requires port 17790 to be open on the remote host.

Does the agent initiate communication?

Logon to the remote host and attempt to ping the server.

Agent initiated communication requires port 17778 to be open on the server.

Installed Agent Plug-in Status

Use the following table to understand the agent plug-in status.

Status	Meaning
The plug-in is installed	The plug-in is installed, working correctly, and communicating with no problems.
Installation Pending	The plug-in is waiting to be deployed. It may be waiting for the computer it is installed on to reboot or because some other process on the remote host has interrupted the installation process.
Unknown	The status is unknown due to networking interruptions, communication problems with the agent, or because the plug-in is no longer installed.
Error	The plug-in may have installed incorrectly or failed to load.
In Progress	The plug-in is either being installed or uninstalled.

If you think a plug-in should be available and cannot find it in the list of installed plug-ins, you may need to check your purchased products or manually update your agent. New plug-ins and updates to existing plug-ins are installed when an agent is updated. It may take a few minutes before the status changes.

Chapter 15: Monitoring MIBs with Universal Device Pollers

Using Universal Device Pollers, SolarWinds Network Performance Monitor has the ability to monitor more than just network status, availability, bandwidth, and errors.

With Orion Universal Device Pollers, you can monitor virtually any statistic that your network devices can record, including:

- Interface traffic
- CPU temperature
- Addressing errors
- UPS battery status
- Current connections to a website

Universal Device Pollers collect both real-time and historical data associated with object IDs maintained in the extensive SolarWinds MIB database. As a result, Universal Device Pollers can retrieve data for nearly any conceivable network metric. Additionally, with Universal Device Poller transforms, you can mathematically manipulate the results of multiple pollers to create your own custom network performance metrics. All network information collected from Universal Device Pollers is accessible within the web console.

Warning: Universal Device Pollers do not collect information from either Orion Failover Engine or Hot Standby Engines. If a SolarWinds NPM server fails, data collection stops for any Universal Device Pollers on that server. Any Universal Device Pollers polling that server will be unable to report any information for the failed NPM server, even if it fails-over to an Orion Failover Engine. For more information, see Orion Failover and Disaster Recovery.

Note: Universal Device Pollers are tied directly to the individual SolarWinds NPM polling engines on which they are hosted. As a result, all Universal Device Pollers assigned to a monitored node that is moved from one SolarWinds NPM polling engine to another must be moved to the new polling engine as well.

The following sections provide instructions for defining and using Universal Device Pollers:

Downloading the SolarWinds MIB Database

SolarWinds maintains a MIB database that serves as a repository for the OIDs used to monitor a wide variety of network devices. This MIB database is updated regularly, and, due to its size, it is not included in the initial NPM installation package. If you are either updating your existing MIB database or using the Universal Device Poller for the first time, you will need to download the SolarWinds MIB database as detailed in the following procedure.

Note: You may need to restart the Universal Device Poller after installing the new MIB database.

To download and install the SolarWinds MIB database:

1. ***If you are responding to a prompt to download and install the SolarWinds MIB database,*** click **Yes**.
   Note: This prompt is typically only encountered by first-time users.
2. ***If you are downloading an update to your existing SolarWinds MIB database,*** complete the following procedure:
   a. Use your SolarWinds **Customer ID** and **Password**, to log in to the Customer Portal (http://www.solarwinds.com/customerportal/).
   b. On the left, under Helpful Links, click **Orion MIB Database**.
3. ***If you are using Internet Explorer and it prompts you to add the SolarWinds downloads site http://solarwinds.s3.amazonaws.com,*** complete the following steps to start the MIB database download:
   a. Click **Add** on the warning window.
   b. Click **Add** on the Trusted Sites window.
   c. Click **Close**, and then refresh your browser.
4. Click **Save** on the File Download window.
5. Navigate to an appropriate file location, and then click **Save**.
6. After the download completes, extract **MIBs.zip** to a temporary location.
7. Open the folder to which you extracted **MIBs.zip**, and then copy **MIBs.cfg** to the SolarWinds folder in either of the following locations on your default install volume, depending on your NPM server operating system:

- **\Documents and Settings\All Users\Application Data** on Windows Server 2003 and XP.
- **\Documents and Settings\All Users\ProgramData** on Windows Server 2008 and Vista.

Configuring Universal Device Poller Thresholds

Universal Device Poller critical and warning thresholds are configured in the web console. The following procedure configures Universal Device Poller thresholds.

To configure Universal Device Poller thresholds:

1. Log in to the Orion Web Console using an account with administrative privileges.
2. Click **Settings** in the top right corner of the web console.
3. Click **Custom Poller Thresholds** in the Settings grouping.
4. Either click a listed custom poller, or search for a custom poller using the search box on the left.
5. Confirm the **Poller Value Type**.

   Note: The Poller Value Type was set when you initially configured the Universal Device Poller, and it indicates how strings returned by the polled device are interpreted.

6. Build conditions to define both **Warning** and **Critical Thresholds**, as follows:

   a. Select whether **All child conditions must be satisfied (AND)** or if only **At least one child condition must be satisfied (OR)**.

   b. Select an appropriate comparison relation and then provide a threshold value on which the comparison is based.

   c. Click **+** to add additional conditions, as required, to define your poller threshold.

7. After configuring all thresholds, click **Submit**.

Creating Universal Device Pollers

The following procedure creates and defines a new Universal Device Poller.

To create and define a new universal device poller:

1. Click **Start > All Programs > SolarWinds Orion > Network Performance Monitor > Universal Device Poller**.
2. ***If you are prompted to download and install the MIB database,*** click **Yes**, and then download and install the MIB database. For more information, see Downloading the SolarWinds MIB Database.
3. Click **File > New Universal Device Poller**.
4. ***If you know the OID of the object you want to poll,*** type it in the **OID** field.
5. ***If you do not know the OID of the object you want to poll and you want to browse available MIB object definitions,*** complete the following steps:
    a. Click **Browse MIB Tree**.
    b. Expand the MIB tree in the left pane to navigate until you locate the object you want to poll.
    c. Select the object you want to poll, and then click **Select**.

    Note: Details describing the selected poller display in the right pane.
6. ***If you do not know the OID of the object you want to poll and you want to search available MIB object definitions,*** complete the following procedure:
    a. Click **Browse MIB Tree**.
    b. Click **Search MIBs** in the top right corner of the Browse MIBs window.
    c. Select a criterion to **Search By** (**Name**, **Description** keyword, or **OID**).
    d. Provide search strings in the Search field, and then click **Search**.
    e. Select the object you want to poll, and then click **Select**.

Note: The OID Details below the Search fields include a description of the corresponding object and indicate the MIB you are currently searching. If an existing OID exactly matches the OID string provided, details for the matching OID display below the Search field. Searching by name or description returns all OIDs with names or descriptions, respectively, containing the provided search string.

7. ***If you want to test the validity of a selected object for a specific node,*** select an appropriate test node in the right pane, and then click **Test**.

   Note: A green check icon indicates that the selected object was successfully polled for the selected node, returning the indicated value. A yellow warning icon indicates that the test poll was not successful for the reason indicated.

8. ***If you tested your poller and it failed,*** check the following:

   - Are you using the correct community string for the node that is being polled for the test? For more information about providing community strings, see Monitoring Devices in the Web Console.
   - Does the selected device support the polled MIB/OID? Refer to device documentation to confirm the MIBs supported by your device.
   - Can your NPM server access the device? Ping the device or use a SolarWinds Toolset application, such as IP Network Browser, to confirm that the device is responding to both ICMP and SNMP requests.

9. Click **Select** when you have located the OID you need.
10. If necessary, edit the provided **Name** and **Description** for your poller.

    Notes:

    - A poller name is required. SolarWinds NPM uses this name to refer to your poller throughout the Orion Web Console. Names must not contain spaces ( ) or dashes (-).
    - The description is optional, but it may be helpful in identifying the type of information collected by your poller.

11. ***If you want to change the advanced poller option defaults,*** click **+** next to **Show Advanced Options**, and then complete the following steps:

a. Select the **MIB Value Type** for the selected poller.
Note: Depending on the type of poller, the poller returns statistics formatted as a **Rate**, a **Counter**, or a **Raw Value**.

b. ***If you selected Rate or Counter as your MIB Value Type,*** provide an appropriate **Unit** and **Time Frame**.

c. ***If you selected Raw Value as your MIB Value Type,*** select the appropriate **Format** in which the polled raw values should appear.
Note: If you are using the **Enumerated** format, click **Map Values** to provide strings corresponding to the values returned by the poller.

d. Select the **SNMP Get Type** appropriate for the object you are polling, and then select **Node** or **Interface**, as appropriate for the polled object.

e. Confirm that the correct type of object is selected for the selected poller to poll (**Node** or **Interface**).

f. ***If you want to designate a specific Polling Interval for the selected poller,*** enter the desired interval, in minutes, between 1 and 600.

Notes:

- By default, the node or interface statistics polling interval is used as the **Polling Interval** for node and interface Universal Device Pollers, respectively. For more information about polling intervals, see Configuring Polling Engine Settings.
- All pollers defined as elements in a poller transform must use the same **Polling Interval**. If you are using the selected Universal Device Poller as one element in a poller transform, confirm that it is using the same **Polling Interval** as all other pollers in the transform.

g. ***If you want to maintain historical data collected by your poller,*** select **Yes** for the **Keep Historical Data** option.

Note: SolarWinds recommends that you keep historical data to take full advantage of the data display features present in SolarWinds NPM. Select **Yes** if you want to display collected poller data in charts and gauges within the Orion Web Console.

h. ***If you want the poller to begin polling immediately upon configuration,*** confirm that **Enabled** is selected as the poller **Status**.

   Note: If you select **Disabled**, the poller will not collect statistics until you enable the poller.

i. In the **Group** field, either select an existing group or provide a new group name to aid in organizing your pollers, and then click **Next**.

j. Click **+** to expand the node tree as necessary, and then check all the nodes to which you want to apply your new poller.

   Note: Available groups are listed in the **Group By:** field. Select a group to selectively limit number of nodes listed in the node tree.

k. ***If you want to see the current results for your poller on the nodes you have checked,*** click **Test**.

   Note: A green check icon indicates that the poller successfully polled the selected node, returning the indicated value. A yellow warning icon indicates that the test poll was not successful for the reason indicated.

l. ***If you tested your poller and it failed,*** check the following:

   - Are you using the correct community string for the node that is being polled for the test? For more information about providing community strings, see Monitoring Devices in the Web Console.
   - Does the device support the MIB/OID that is being polled? Refer to the documentation supplied by the device vendor to confirm the MIBs supported by your device.
   - Can you access the device from the Orion Network Performance Monitor server? Ping the device to see if it responds or use a SolarWinds Toolset application, such as IP Network Browser, to confirm that the device is responding to both ICMP and SNMP requests.

12. Click **Next**.
13. ***If you want to display poller results in Orion Web Console views,*** confirm that **Yes** is selected, and then, for each available NPM view, check the types of poller results resources, if any, that you want to display.

Note: Click **Preview** to see how your poller resource will display in the selected Orion Web Console view.

14. ***If you only want to display the poller results resource in the event that the poller returns valid results, check Do not show this poller if it is not assigned.***
15. Click **Finish**.

To check that your UnDP pollers are properly configured, run active diagnostics for UnDP using SolarWinds Diagnostics. For more information, see Running SolarWinds Diagnostics.

Assigning Pollers to Nodes or Interfaces

In addition to the Universal Device Pollers that you create, NPM is packaged with a few predefined example pollers. To use any of these pollers you need to assign the poller to a network device, and then enable the poller.

Note: For more information about creating your own Universal Device Pollers, see Creating Universal Device Pollers.

To enable and assign a poller to nodes or interfaces:

1. Click **Start > All Programs > SolarWinds Orion > Network Performance Monitor > Universal Device Poller**.
2. Click **File > Assign Pollers**.
3. Click **+**, as necessary, to expand the poller tree, and then check the pollers you want to assign.

   Notes:

   - By default, NPM provides two poller groups: Example and Default Group. The Example group contains all predefined NPM pollers, and Default Group is the group that contains all user-defined Universal Device Pollers if they are not assigned to any other group.
   - Checking a poller group automatically checks all pollers in the group. If you do not want to assign a specific poller in a checked group, click **+** next to the poller group name, and then uncheck the specific pollers that you do not want to assign.
   - If you need to assign multiple pollers either to a single node or to a group of nodes, check all the pollers you want to apply on this view. These pollers are assigned to nodes in the next step.
4. After you have checked all the pollers you want to assign, click **Next**.
5. Click **+** to expand the node tree down to the interface level, if necessary, and then check the elements to which you want to apply the selected pollers.

   Notes:

   - Available groups are listed in the **Group By:** field. Select a group to selectively limit the node tree.

- Interfaces are not displayed unless you are assigning an interface poller.
- When assigning an interface poller, checking a node automatically assigns the selected poller to all interfaces on the checked node. If you do not want to apply the poller to a specific interface on any parent node, click + next to the parent node, and then uncheck the specific interfaces to which the poller should not be assigned.

6. ***If you want to see the current results of the selected pollers on the nodes and interfaces you have checked,*** click **Test**.
   Note: A green check icon indicates that the poller successfully polled the selected node, returning the indicated value. A yellow warning icon indicates that the test poll was not successful for the reason indicated.
7. ***If you tested your poller and it failed,*** check the following:
   - Are you using the correct community string for the node that is being polled for the test? For more information about providing community strings, see Monitoring Devices in the Web Console.
   - Does the device support the MIB/OID that is being polled? Refer to the documentation supplied by the device vendor to confirm the MIBs supported by your device.
   - Can you access the device from the Orion Network Performance Monitor server? Ping the device to see if it responds or use a SolarWinds Toolset application, such as IP Network Browser, to confirm that the device is responding to both ICMP and SNMP requests.
8. Once you have completed your poller assignments, click **Finish**.

Disabling Assigned Pollers

By default, as soon as a poller is assigned, it collects statistics on the selected elements to which it is assigned. If you want to suspend data collection for a poller without deleting it, complete the following procedure to disable the poller. **Note:** To disable multiple pollers, repeat the following procedure for each poller you want to disable.

To temporarily disable a Universal Device Poller:

1. Click **Start > All Programs > SolarWinds Orion > Network Performance Monitor > Universal Device Poller**.
2. In the All Defined Pollers pane of the Orion Universal Device Poller window, click **+**, as necessary, to expand the poller tree, and then click the poller you want to disable.
3. Confirm you have selected the poller you want to disable by viewing the poller properties in the main Orion Universal Device Poller window. Click **Show all Properties** in the lower left of the main window to show more details, if necessary.
4. Click **Edit Properties** in the top right of the main window.
5. Set **Status** to **Disabled**, and then click **Finish**.

Duplicating an Existing Poller

Existing pollers are easily duplicated in SolarWinds NPM. The following procedure provides the required steps to duplicate an existing poller.

To duplicate an existing poller in SolarWinds NPM:

1. Click **Start > All Programs > SolarWinds Orion > Network Performance Monitor > Universal Device Poller**.
2. In the All Defined Pollers pane of the Orion Universal Device Poller window, click **+**, as necessary, to expand the poller tree, and then click the poller you want to duplicate.
3. Confirm that you have selected the poller you want to duplicate by viewing the poller properties in the main Orion Universal Device Poller window.
4. Click **Show all Properties** in the lower left of the main window to show more details, if necessary.
5. Right-click the name of the poller you want to duplicate, and then select **Duplicate Poller**.
6. Change the **Name** of the duplicate poller, and then edit the definition of the duplicate poller, as necessary, in the same way that you would create a new Universal Device Poller. For more information about creating a Universal Device Poller, see Creating Universal Device Pollers.

Importing MIB Pollers

SolarWinds NPM provides the ability to import custom pollers both from previous SolarWinds NPM versions and from Universal Device Pollers. Though you cannot import MIBs directly into the SolarWinds MIB Database, the import mechanism does allow you to import the association between a MIB and a Universal Device Poller. The poller can then be associated with a device in your environment. Use the following procedure to import a Universal Device Poller.

To import a Universal Device Poller:

1. Click **Start > All Programs > SolarWinds Orion > Network Performance Monitor > Universal Device Poller**.
2. Click File > Import Universal Device Pollers.
3. For each poller you want to import, complete the following steps:
    a. Click **Open**, and then navigate to the location of the poller to import.
    b. Select the poller to import, and then click **Open**.
4. Select the pollers to import from the list on the left, and then click **Import**.
5. ***If you want to remove a selected poller from the list of pollers to import,*** click the poller to remove, and then click **Remove**.

    Notes:

    - To select multiple pollers, hold down **SHIFT** or **CTRL**, and then click the pollers you want.
    - To collapse all folders and see just the group names, hold down **SHIFT**, and then click **-** next to any of the group names.
6. Click OK.
7. ***If you want the imported poller to begin polling immediately upon assigning network devices,*** complete the following steps:
    a. Select your new, imported poller in the All Defined Pollers pane on the left of the Orion Universal Device Poller window.
    b. Click **Edit Properties**.
    c. Confirm that the poller **Status** is **Enabled**, and then click **Finish**.

8. ***If you do not want the poller to begin polling immediately upon assigning network devices,*** complete the following steps:

    a. Select your new, imported poller in the All Defined Pollers pane on the left of the Orion Universal Device Poller window.

    b. Click **Edit Properties**.

    c. Select **Disabled** as the poller **Status**, and then click **Finish**.

    Note: If **Disabled**, the poller will not collect data until you enable the poller.

9. Assign nodes or interfaces to the imported poller. For more information, see Assigning Pollers to Nodes or Interfaces.

As soon as the imported poller has been enabled and assigned to appropriate network devices, the poller begins collecting statistics. To view these statistics, log in to the Orion Network Performance Monitor Web Console and browse to a node or interface that was just assigned to the poller. For more information, see Viewing Universal Device Poller Statistics.

Exporting Universal Device Pollers

SolarWinds NPM provides the ability to export Universal Device Pollers you have created using the following procedure.

To export a Universal Device Poller:

1. Click **Start > All Programs > SolarWinds Orion > Network Performance Monitor > Universal Device Poller**.
2. Click **File > Export Universal Device Pollers**.
3. In the Pollers pane on the left, click **+**, as necessary, to expand the poller tree, and then select the pollers you want to export.

   Note: Selecting a group name selects all pollers in the group, and multiple pollers may be selected using **Shift+Click** and **Ctrl+Click**.
4. ***If you have selected all the pollers you want to export,*** click **Export**.
5. ***If you want to remove a selected poller from the list of pollers to export,*** click the poller to remove, and then click **Remove**.

   Note: Selecting a group name selects all pollers in the group, and multiple pollers may be selected using **Shift+Click** and **Ctrl+Click**.
6. Click **Save**.
7. Navigate to the location where you want to export the selected pollers, provide a **File name**, and then click **Save**.

Setting Custom Poller Thresholds

Just as the default pollers that are packaged with your SolarWinds NPM have defined warning and critical thresholds, you are able to set the warning and critical thresholds for your configured Universal Device Pollers.

To set Universal Device Poller thresholds:

1. Log into the Orion Web Console using an account with administrative privileges.
2. Click **Settings** in the top right corner.
3. In the Settings grouping, click **Custom Poller Thresholds**.
4. In the left pane, click the poller for which you want to configure thresholds.
5. Confirm that the selected **Poller Value Type** is correct (**Text** or **Number**).
6. Configure both **Warning** and **Critical Thresholds** as follows:
    a. Select whether **All child conditions must be satisfied (AND)** or if only **At least one child condition must be satisfied (OR)**.
    b. Select an appropriate relation, and then provide a value.
    c. Add additional conditions, including additional condition blocks, as required, to define your poller threshold.
7. ***If you want to configure additional poller thresholds,*** click **Save and Continue**, and then configure additional poller thresholds, as above.
8. Click **Submit**.

Transforming Poller Results

Often, the results provided by a MIB poller are more easily understood after they have been manipulated with a simple mathematical calculation. For example, though a poller may return temperature values in Celsius, it may be easier to work with the poller results if they are presented in Fahrenheit. The following sections detail both currently available poller transformations and the creation of new poller transformations.

Available Poller Transformations

SolarWinds NPM provides a number of predefined transformation functions that may be applied to one or more pollers to generate mathematically manipulated poller results. The following table lists transformation functions that are currently available with the Universal Device Poller in SolarWinds NPM:

Poller Transformation	Definition
Average	Provides an average of the results of multiple pollers
Minimum	Provides the minimum of multiple poller results
Maximum	Provides the maximum of multiple poller results
Truncate	Truncates a polled value to a designated number of decimal places; e.g. **Truncate({HiPrecision},4)** truncates the result of the poller named HiPrecision to four decimal places.
ColumnAverage	Provides an average of the column values in a polled table
ColumnMinimum	Gives the minimum of a column of values in a polled table
ColumnMaximum	Gives the maximum of a column of values in a polled table
ColumnSum	Provides the sum of a column of values in a polled table

Poller Transformation	Definition
Temperature > Celsius to Fahrenheit	Provides the Fahrenheit equivalent of a poller result originally presented in Celsius
Temperature > Fahrenheit to Celsius	Provides the Celsius equivalent of a poller result originally presented in Fahrenheit
X to Kilobyte	Provides the number of Kilobytes equivalent to a poller result originally presented in Bytes
X to Megabyte	Provides the number of Megabytes equivalent to a poller result originally presented in Bytes
X to Gigabyte	Provides the number of Gigabytes equivalent to a poller result originally presented in Bytes
X to Terabyte	Provides the number of Terabyte s equivalent to a poller result originally presented in Bytes
Kilobyte to Megabyte	Provides the number of Megabytes equivalent to a poller result originally presented in Kilobytes
Kilobyte to Gigabyte	Provides the number of Gigabytes equivalent to a poller result originally presented in Kilobytes
Kilobyte to Terabyte	Provides the number of Terabytes equivalent to a poller result originally presented in Kilobytes
Megabyte to Gigabyte	Provides the number of Gigabytes equivalent to a poller result originally presented in Megabytes
Megabyte to Terabyte	Provides the number of Terabytes equivalent to a poller result originally presented in Megabytes
Gigabyte to Terabyte	Provides the number of Terabytes equivalent to a poller result originally presented in Gigabytes

Poller Transformation	Definition
Parse	Using C# regular expression syntax, retrieves the first match for a provided poller result in a string poller result, e.g. **parse((?<TempTell>)\d+), Current temperature is 55)** returns **55**. For more information about C# regular expressions, see Regular Expression Pattern Matching.

Creating a Poller Transformation

The following procedure provides the steps required to develop powerful poller transformations with Universal Device Pollers.

To transform poller results:

1. Click **Start > All Programs > SolarWinds Orion > Network Performance Monitor > Universal Device Poller**.
2. Click File > Transform Results.
3. Click **Next** on the page of example poller transformations.
4. Type a transformation **Name**, and then provide an optional **Description**.

   Notes:

   - A transformation name is required. SolarWinds NPM uses this name to refer to your defined poller transformation throughout the Orion Web Console.
   - Names are recorded without spaces, so any included spaces in the name are removed.
   - The description is optional, but it may be helpful in identifying the type of information generated by your poller transformation.
5. ***If you want to maintain historical data generated by your poller transformation,*** select **Yes** for the **Keep Historical Data** option.

Note: SolarWinds recommends that you keep historical data to take full advantage of the data display features present in SolarWinds NPM. Select **Yes** if you want to display transformed poller data in charts and gauges within the Orion Web Console.

6. ***If you want your poller transformation to begin calculating transformed results immediately upon configuration,*** confirm that **Enabled** is selected as the poller transformation **Status**.

   Note: If you select **Disabled**, the poller will not transform poller statistics until you enable the poller transformation.

7. In the **Group** field, either select an existing group or provide a new group name to aid in organizing your poller transformations.
8. Click **Next**.
9. Provide the mathematical definition of your poller transformation in the **Formula** field, as shown in the following steps:

   a. Click **Add Function**, and then select the function you want to apply to one or more pollers.

   b. Click within the function parentheses.

   c. Click **Add Poller**, and then select a poller to transform.

      Notes:

      - Repeat for each additional poller to add to the transformation formula.
      - Separate pollers with commas, as shown in the following example that averages the results of three pollers:

        avg({poller1**},{**poller2**},{**poller3**})**

      - Standard mathematical operations, as shown in the following example, are also valid as formulas:

        {poller1**}+{**poller2**}**

      - Mathematical constants e and π are also available, as **E()** and **PI ()**, respectively.

- Poller transformation formulas are also nestable, as shown in the following example that returns the average of two poller comparisons:

  avg(min({poller1**},{**poller2**}),max({**poller3**},{**poller4**}))**

10. ***If you want to test the validity of a selected poller transformation formula for a specific node,*** use the available criteria to select a device to test, and then click **Test**.
    Note: Test results for each poller in the formula display with the result of the defined poller transformation.
11. ***If you tested your poller transformation and it failed,*** check the following:
    - Is your transformation formula syntactically correct? Ensure that all braces and parentheses are balanced, that there are no unnecessary spaces, and that all pollers return the same type of values.
    - Are you using the correct community string for the node that is being polled for the test? For more information about providing community strings, see Monitoring Devices in the Web Console.
    - Does the device support the polled MIB/OID? Refer to documentation supplied by the device vendor to confirm supported MIBs for your device.
    - Can you access the device from the Orion Network Performance Monitor server? Ping the device to see if it responds or use a SolarWinds Toolset application such as IP Network Browser to confirm that the device is responding to both ICMP and SNMP requests.
12. Click **Next**.
13. Click **+** to expand the node tree down to the interface level, if necessary, and then check all the monitored devices to which you want to apply your defined poller transformation.

    Notes:

    - Available groups are listed in the **Group By:** field. Select a group to selectively limit the node tree.
    - Interfaces are not displayed unless your poller transformation operates on a defined interface poller.

When assigning an interface poller transformation, checking a node automatically assigns the selected transformation to all interfaces on the checked node. If you do not want to apply the poller transformation to a specific interface on any parent node, click **+** next to the parent node, and then uncheck the specific interfaces to which the transformation should not be assigned.

14. ***If you want to see the current results of the selected pollers on the nodes and interfaces you have checked,*** click **Test**.

    Notes:

    - A green check icon indicates a valid poller transformation, and the transformation result is displayed.
    - A yellow warning icon indicates that the poller transformation was not successful for the reason indicated.

15. ***If you tested your poller and it failed,*** check the following:

    - Is your transformation formula syntactically correct? Ensure that all braces and parentheses are balanced, that there are no unnecessary spaces, and that all pollers return the same type of values.
    - Are you using the correct community string for the node that is being polled for the test? For more information about providing community strings, see Monitoring Devices in the Web Console.
    - Does the device support the polled MIB/OID? Refer to documentation supplied by the device vendor to confirm supported MIBs for your device.
    - Can you access the device from the Orion Network Performance Monitor server? Ping the device to see if it responds or use a SolarWinds Toolset application such as IP Network Browser to confirm that the device is responding to both ICMP and SNMP requests.

16. Click **Next**.

17. ***If you want to display poller results in Orion Web Console views,*** confirm that **Yes** is selected, and then, for each available view, check the types of poller results resources, if any, that you want to display.

Note: Click **Preview** to see how your poller resource will display in the selected web console view.

18. ***If you only want to display the poller results resource in the event that the poller transformation returns valid results, check Do not show this poller if it is not assigned.***
19. Click **Finish**.

If your transformed UnDP poller combining data from other UnDP pollers does not work, make sure that it is assigned to the same node or interface as the UnDP poller used for the transformation and that it has the same polling interval.

Viewing Universal Device Poller Statistics

Once you have configured and enabled a Universal Device Poller, you can view the statistics that it records on any view within the Orion Web Console. The following procedure includes poller resources in Orion Web Console views.

To add poller resources to web console views:

1. Click **Start > All Programs > SolarWinds Orion > Network Performance Monitor > Universal Device Poller**.
2. In the All Defined Pollers pane of the Orion Universal Device Poller window, click **+**, as necessary, to expand the poller tree, and then click the poller you want to add as a web console resource.
3. Confirm that you have selected the poller you want to duplicate by viewing the poller properties in the main Orion Universal Device Poller window.
4. Right-click the poller to add as a resource, and then click **Web Display**.
5. Confirm that **Yes** is selected, and then, for each available NPM view, check the types of poller resources that you want to display.

   Note: Click **Preview** to see how your poller resource will display in the selected Orion Web Console view.

6. ***If you only want to display the poller resource when the poller returns valid results, check Do not show this poller if it is not assigned.***
7. Click **Finish**.

Mapping Universal Device Pollers with Network Atlas

With Network Atlas version 1.11, it is possible to include Universal Device Pollers as objects on custom maps. Universal Device Pollers are added to Network Atlas maps in the same way that nodes, interfaces, and other monitored network are included. For more information, see Adding Map Objects.

Chapter 16: Device Studio

Device Studio enables you to create your own Device Studio pollers to monitor specific technologies or unique devices that are not automatically detected for monitoring in your SolarWinds environment.

Use Device Studio to create Device Studio pollers for any and all of the unique devices on your network.

To open Device Studio:

1. Log in to the Orion Web Console using an account with administrative credentials.
2. Click **Settings** in the top right of the web console.
3. In the Node & Group management grouping, click **Manage Pollers**.

Managing Pollers

By creating Device Studio pollers, you can extend Orion to support new devices. This way you can poll arbitrary OIDs as native data fields.

For information about creating Device Studio pollers, see "Creating Device Studio Pollers".

You can perform the following actions with Device Studio pollers:

- Assign the poller to nodes.
- Edit, or duplicate and edit the poller.
- Scan new nodes with the poller.
- Export or import the poller.
- Delete unused pollers.

Customizing Pollers

By creating Device Studio pollers, you can define custom polling definitions in a way that allows Orion to view the defined set of pollers as fully integrated entities.

You can define a set of polled data, and then associate these data points with monitored nodes.

You can also override the values polled by SolarWinds pollers by the values polled by a Device Studio poller.

Device Studio pollers and the data polled by them appear as fully integrated entities in the Orion Web Console, including charts, alerts, and reports.

Managing Unique Devices

If you have devices on your network that SolarWinds does not immediately recognize for polling, you can either edit an existing poller to suit your device needs or create a completely new poller, specifically tailored to your unique device. By using the Create new poller wizard, you can create Device Studio pollers to add support for vendors and technologies that are not natively supported by Orion.

Device Studio technologies

Device Studio supports a number of different technologies. Each technology has a predefined set of properties that you can monitor on your devices. The technology you select defines how the polled data is processed, stored, and presented. Device Studio supports the following technologies:

- **CPU & Memory:** for collecting data about the CPU and memory load of single processor systems.
- **Multi CPU & Memory:** for collecting data about the CPU and memory load of multiprocessor systems.
- **Node Details:** for collecting data about the details of a node.

Additionally, pollers using other polling technologies, such as VLAN and VRF, are also displayed in the Manage Pollers view. However, it is not possible to create pollers using these technologies in Device Studio.

Creating Device Studio Pollers

You can create Device Studio pollers by using the Create New Poller wizard in the Orion Web Console.

To create a new Device Studio poller, complete the following steps:

1. On the Manage Pollers screen, click **Create New Poller**.
2. Select a technology you want to poll for. The options are CPU & Memory, Multi CPU & Memory, and Node Details. For more information about the technologies, see "Device Studio technologies".
3. Specify the Poller Package Name.
4. Select a test node on which to test the poller.
5. Optionally, specify the tags, description and author corresponding to the poller, and then click **Next**.
6. On the Specify Data Source tab, select a metric you want to define, and then click either **Edit Data Source** or **Define Data Source**.
7. If you do not need to read the metric from the Object Identifier (OID), provide a constant value for the metric in the Use a constant value window, click **Submit**, and then proceed with **Step 12**.
   Note: Define a constant value, for example, when you are creating a CPU and memory poller, and the device you want to poll only supports CPU values.
8. If you want to specify another value, click **Cancel** on the Use a constant value window, and then proceed with the next steps.
9. Specify the OID by browsing in the SolarWinds MIB database, or by defining the OID manually. For information about manually defining OIDs, see "Manually Defining Object Identifiers (OIDs)". After specifying the OID, click **Submit** on the Pick Object Identifier window.
10. If necessary, transform the multiple returned values into a single value, or select a different OID. For more information, see "What is a Formula?".
11. In the Create a calculated value window, select a function and an input from the lists, click **Test**, and then click **Submit**.
    For more information, see "Common Formulas".
12. If the value is as expected, click **Yes, the data source is reasonable**, and then click **Next**.

13. On the Discovery Settings tab, select the **Automatically poll nodes...** check box, and then click **Next**.
14. On the Summary tab, review the poller package settings, and then click **Submit**.

Testing Device Studio pollers

A Device Studio poller may not always be seamlessly supported by the device it is tested on. For example, errors occur if the OID the Device Studio poller polls for is not supported by the device, or if the returned value is not of the expected data type defined by the Device Studio poller.

To get the Device Studio poller working in a your environment, try the following methods:

- Try testing the Device Studio poller on a different, more suitable node.
- If the device you use for testing is not fully compatible with the Device Studio poller, upgrading the firmware of your test device might help.
- Try modifying the Device Studio poller to suit the devices you have. For example, you can modify the OID that is used to poll the device.
  Notes:
  - Modifying Device Studio pollers this way requires familiarity with the MIB database structure.
  - Some of the pollers provided by SolarWinds cannot be modified with Device Studio. You can only modify the poller definition of these pollers in a text editor.

Using thwack community pollers

Apart from creating your own Device Studio pollers, you can also import pollers provided by contributors of the thwack community.

The thwack community pollers are available in the Orion Web Console under **Manage Pollers > thwack Community Pollers**. The list is updated automatically every 30 minutes, and it contains the device pollers that have been made available on thwack, under **Network Performance Monitor > NPM Content Exchange > Device Pollers > Documents**.

You can group the available pollers according to tags, author, or technology. Click the name of a device poller to view the description of the poller.

To further verify whether the poller suits your specific device, you can test the poller before importing it.

To test a device poller:

1. Select the thwack community poller from the list, and then click **Test Device Poller**.
2. Provide your thwack credentials, and then click **Submit**.
3. Select an SNMP node for testing, and then click **Test Poller**.

After the test is finished, you can directly assign the device poller to the test node.

To import a device poller:

1. Select the thwack community poller from the list, and then click **Import device poller**.
2. Provide your thwack user credentials, and then click **Submit**.
3. After the import process is finished, the poller will be available in the Local Poller Library, and you can assign it to a device. For more information, see "Assigning Pollers".
   Note: If the poller already exists because of an earlier import, you can either overwrite the existing poller, or create a new one.

Importing thwack community pollers to an environment without internet connection

The thwack community pollers are only updated automatically if you have a working internet connection. To import thwack community pollers to an environment that does not have an internet connection, you must download the pollers from a computer which can access the internet, save them to a portable drive or a USB drive, and then import them manually.

Exporting pollers to the thwack community

Besides importing thwack community pollers, you can also export your own Device Studio pollers to share them with other users of the thwack community.

To export a Device Studio poller to thwack:

1. On the Manage Pollers screen, click the Local Poller Library tab.
2. Select the poller you want to export.
   Note: You can export Device Studio pollers that you created, but you cannot export pollers that are provided by SolarWinds.
3. Click **Export**, and then select **Export to thwack**.
4. Provide your thwack user credentials, and then click **Submit**.
   Note: If you already logged in to thwack from the Orion Web Console during the same session, you do not have to enter your credentials again, and the Device Studio poller will be exported immediately.

The Device Studio poller will be available on thwack, in the **Network Performance Monitor > NPM Content Exchange > Device Pollers > Documents** section.

Why is Orion unable to connect to thwack?

The Orion server must have internet connection to be able to connect to thwack. If the connection is blocked by a firewall or a proxy, the list of shared pollers cannot be retrieved from thwack, and any operation that relies on communication with thwack, such as the upload or download of a poller will fail.

Check your firewall and proxy settings to make sure that Orion can connect to the internet.

Manually Defining Object Identifiers (OIDs)

If the OID does not exist in the SolarWinds MIB database, you can manually define the OID you want to use.

To manually define an OID:

1. On the Data Source screen, click **Browse OIDs**.
2. On the Pick Object Identifier screen, select the check box under **Manually Define Object Identifier (OID)**.
3. Type the name and OID.
4. Select the SNMP get type. For information about SNMP get types, see "SNMP Get Type".
5. Click **Poll current value from test node**.

SNMP Get Type

The SNMP Get type defines the type of query you have to run to retrieve the appropriate information. You can retrieve scalar values by using either GET or GET NEXT, and you can retrieve values from a particular column in a table value by using GET TABLE.

Note: For table records, only the first five values are returned.

What is a Formula?

Often, the results provided by a MIB poller are more easily understood after they have been manipulated with a simple mathematical calculation. For example, though a poller may return temperature values in MB, it may be easier to work with the poller results if they are presented in GB. The calculations and transformations that are used to manipulate poller results are referred to as formulas within the Orion Web Console.

For a list of common formulas that are available in Device Studio, see "Common Formulas".

Common Formulas

The following table provides the list of common formulas that can be used to manipulate Device Studio poller results.

Formula	Description
KiloToByte	Multiplies input by 1024
MegaToByte	Multiplies input by 1024 x 1024
GigaToByte	Multiplies input by 1024 x 1024 x 1024
Average	Returns the average of values from the input columns
Sum	Returns the sum of values from the input columns
Count	Returns the total number of input columns
Condition	Creates an if/then statement
Truncate	Rounds the input decimal number up or down to an integer
Length	Returns the number of characters in the input string
Replace	Replaces the content in the string
IndexOf	Returns the position in the string
SubString	Defines the section of the string of interest

Assigning Pollers

After creating a new Device Studio poller, you can assign it to a monitored device.

To assign a Device Studio poller to a monitored node:

1. On the Manage Pollers page, select the poller you want to assign to a node, and then click **Assign**.
2. Select the node you want to assign the poller to.
3. If the node has not been scanned yet, click **Scan now**.
4. If the scan result is a match or a multiple match, click **Enable Poller** to assign the poller to the node.

Note: You can only scan SNMP nodes whose status is Up.

Scanning Monitored Objects

When a monitored node is scanned, it is verified whether the OIDs of the monitored node and the OIDs specified in the poller match.

The following scenarios are possible:

- If the OIDs do not match, the scan returns a result indicating the mismatch, and the poller will not be assigned to the monitored node.
- If the OIDs match, and there is no other poller polling for the specific technology, then the poller is automatically enabled on the node.
- If the OIDs match, but there is already another poller polling the node for the specific technology, the new poller is not enabled automatically. In this case, you can enable the poller manually.

Chapter 17: Monitoring Network Events in the Web Console

Orion automatically logs all events that occur to any monitored devices on your network. These events are then displayed in the Orion Web Console, so you can view and acknowledge them as your network management policies require.

Use the following topics to perform these actions:

- Viewing Event Details in the Web Console
- Acknowledging Events in the Web Console

Viewing Event Details in the Web Console

Orion logs network events and lists them in the readily customizable Events view of the Web Console. Events are shown in order of occurrence, and they may be viewed by device, date and time, and event or device type.

Note: The Network Event Log is maintained as part of the Nightly Database Maintenance plan defined within the Database Settings area of the Orion Polling Setting page in the Orion Web Console. Records are kept for the number of days specified in the Events Retention field (the default is 30 days). For more information, see Orion Polling Settings.

To view event details in the Web Console:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Log in to the Orion Web Console, and then click **Events** in the Views toolbar.
3. ***If you want to filter your events view by object,*** select the **Network Object** or **Type of Device** to which you want to limit your view in the **Filter Devices** area.
4. ***If you want to limit your events view to show only events of a specific type,*** select the appropriate **Event Type** in the Filter Events area.
5. ***If you only want to see events from a specific period of time,*** complete either of the following options:
   - Select a predefined period from the **Time Period** menu.
   - Select **Custom** from the **Time Period** menu, and then click the appropriate fields to provide **Begin** and **End** dates and times.
6. In the **Show** X **Events** field, provide the maximum number of events you want to view.
7. ***If you want to show all events, including events that have already been cleared,*** check **Show Cleared Events**.
8. Click **Refresh** to complete your events view configuration.

Acknowledging Events in the Web Console

Acknowledging network events is straightforward in the Web Console, as shown in the following procedure.

To acknowledge events in the Web Console:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Log in to the Orion Web Console, and then click **Events** in the Views toolbar.
3. Provide appropriate filter criteria for the displayed events. For more information, see Viewing Event Details in the Web Console.
4. Click **Refresh** to ensure that all selected view criteria take effect.
5. Check individual events to acknowledge or click **Select All**.
6. Click **Clear Selected Events**.

Chapter 18: Using Maps

In the Orion Web Console, you can display maps showing monitored nodes, interfaces and volumes, SAM applications and components, and network links.

Open Street Map

You can display your nodes on maps powered by Open Street Map. For more information, see Managing the Worldwide Map of Orion Nodes Resource.

Network Maps

You can also create customized maps in the Orion Network Atlas and display them in the Orion Web Console.

For more information about displaying maps in the Orion Web Console, see Displaying Maps in the Orion Web Console.

For more information about Network Atlas, see Introducing Network Atlas.

Wireless Heat Maps

The Network Atlas also allows you to visualize the signal strength provided by your wireless access points in wireless heat maps.

For more information about creating wireless heat maps, see Creating Wireless Heat Maps.

For more information about displaying wireless heat maps in the Orion Web Console, see Displaying Wireless Heat Maps in the Orion Web Console.

Managing the Worldwide Map of Orion Nodes Resource

In the Orion Web Console, you can display monitored nodes in the Worldwide Map of Orion Nodes resource. Nodes that contain information about their location in the OpenStreet format are displayed automatically. For more information, see Automatic Placement of Nodes.

You can manage nodes shown on the map in the Manage the Worldwide map view.

Note: To start managing the worldwide map, click **Manage Nodes** in the Worldwide Map resource.

Adding Nodes Manually

Nodes with the same position are displayed as one location. Adding nodes means adding a new location into the map and defining the nodes that are located in it.

To add nodes manually:

1. Click **Place nodes on the map manually**, and then click into the map where you want to place the new nodes.
2. Use the Grouping and Search tools to select nodes which you want to place on the map.
   Note: Click **>** next to a node group name to expand a list of all nodes in the selected node group.
3. Provide a name for the new location.
4. Click **Place on Map**.
5. To apply your changes in the resource, click **Submit** or **Save and Continue** if you want to further edit your worldwide map.

Editing the Position of Locations

You can either drag-and-drop the location on the map, or provide an exact location using longitude and latitude.

To edit a position of a location:

1. Click the map location you want to edit, and then click **Edit location**.
2. Provide the **Latitude** and **Longitude** of the new location, and then click **Save**.
3. To apply your changes in the resource, click **Submit** or **Save and Continue** if you want to further edit your worldwide map.

Editing Locations

You can add or remove nodes in a location, or rename your location.

To edit nodes in a location:

1. Click the map location you want to edit, and then click **Edit** at the top right of the list of nodes at the selected map location.
2. Add or remove nodes in the location.
   - To add nodes, use the Grouping and Search tools to select new nodes for the location.
   - To remove nodes, click x next to the appropriate node in the Selected nodes section.

     Note: In the Edit Selection pop-up, you can also rename the location.
3. Click **Save Changes** to apply your changes.
4. To apply your changes in the resource, click **Submit** or **Save and Continue** if you want to further edit your worldwide map.

Removing Locations

To delete a location shown on the worldwide map:

1. Select the map location to remove.
2. Click **Remove from map**, and then confirm the map location removal.
3. To apply your changes in the resource, click **Submit** or **Save and Continue** if you want to further edit your worldwide map.

Automatic Placement of Nodes

If your devices contain information about their location in the OpenStreetMap format, they can be added into the Worldwide Map resource automatically.

Nodes with the same address appear in the map as one location.

By default, the automatic placement of nodes is enabled.

To verify whether the automatic placement of nodes is enabled:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right corner, and then click **Web Console Settings**.
3. Scroll down to Worldwide Map Settings and make sure that the **Automatic Geolocation** box is selected.

   Note: Locations will display in the Worldwide Map resource within an hour after you select this option.
4. Click **Submit** to apply the current settings.

Introducing Network Atlas

Network Atlas is a powerful tool for creating custom maps and network diagrams. The maps created in Network Atlas enable users to view a graphical depiction of their network in the Orion Web Console. You can also use the maps to create network documentation, which can then be printed and exported as needed.

Map objects may include monitored NPM nodes, interfaces, and volumes; SAM applications and components; nested maps; and network links.

The numerous presentation options for your network maps include the following:

- A large set of predefined background colors, textures, and images is available for you to use in your maps. You can also provide your own custom background graphics, such as floor plans.
- Real-time weather or natural disaster maps may be projected directly onto your network maps using linked web graphics as a background.
- The shape, size, color, and style of map links may be customized to illustrate the status or the relative bandwidth of associated objects.
- Map objects may be presented in a unique set of graphical styles to portray network status.
- Wireless heat maps display the signal strength provided by your wireless access points.
- Maps may be nested to selectively reveal increasing levels of map detail, and the status of nested map child objects may be bubbled up to the parent map.

Network Atlas Features

Network Atlas gives you the ability to create multi-layered, fully customizable, web-based maps of your network to visually track the performance of network elements, applications, and operations monitored by any of the following Orion applications:

- Network Performance Monitor
- Server & Application Monitor
- VoIP & Network Quality Manager
- Enterprise Operations Console

The following features are currently available in Network Atlas:

ConnectNow

The ConnectNow tool in Orion Network Atlas allows you to instantly draw lines between mapped objects that are connected on either Layer 2 or Layer 3. For more information, see Connecting Objects Automatically with ConnectNow.

Utilization and Connection Speed Shown

Multi-colored links between mapped devices communicate most recently determined interface utilization and connection speed. Utilization data is available for links that are not automatically created.

Linked Backgrounds

The linked backgrounds feature allows you to create maps with backgrounds sourced directly from the Internet. Using a linked background, you can create maps that include dynamic weather information relevant to your distributed network sites. For more information, see Selecting a Background Image.

AutoArrange

AutoArrange options allow you to quickly structure or reorganize objects on your map. For more information, see Selecting Automatic Layout Styles.

Wireless Heat Maps

Wireless Heat Maps allow you to visualize the strength of wireless signal generated by your Wi-Fi access points. For more information, see Creating Wireless Heat Maps.

Installing Network Atlas

Network Atlas is pre-installed on Orion EOC and Orion NPM, and it can be run as a local application on those Orion servers. Users can also run Network Atlas as a standalone application on any remote computer meeting the stated minimum requirements.

Network Atlas Requirements

The following table provides the minimum requirements for a Network Atlas installation.

Note: To take full advantage of Network Atlas features, users of Network Atlas must either have node management rights in Orion NPM or be assigned the administrator role in Orion EOC. Network Atlas may fail to complete file synchronization with the Orion database if Network Atlas users do not have sufficient permissions to access the Network Atlas synchronization folder. Confirm that the user logged in to Network Atlas is able to access the Network Atlas synchronization folder.

Server Component	Requirements
Operating System	Microsoft Windows XP, Windows Vista, Windows 7, Windows Server 2003, or Windows Server 2008 R2.
Memory	1 GB
Hard Drive Space	150 MB
Ports	Remote instances of Network Atlas require TCP on port 17777 to either the Orion NPM or the Orion EOC server.

Installing Network Atlas on a Remote Computer

The following procedure installs Network Atlas on a remote computer.

To install Network Atlas on a remote computer:

1. Log on to your Orion NPM or Orion EOC server.
2. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
3. In the Network Map resource, click **Download Network Atlas**.

   Note: If you do not see a **Download Network Atlas** link in your Network Map resource, click **Edit**, and then check the **Show Network Atlas Download** link option on the Edit Network Map resource page (administrative access may be required).
4. Save the Network Atlas installer (**NetworkAtlas.exe**) to an appropriate location on your remote computer.
5. Run the Network Atlas installer on your remote computer.

6. Click **Next** on the Welcome window.
7. ***If you have previously installed Network Atlas,*** you may be prompted to change, repair or remove your installation. Click **Repair**, and then click **Repair** again on the Ready to repair window.
8. ***If you are installing Network Atlas for the first time,*** complete the following steps:
    a. Accept the terms in the license agreement, and then click **Next**.
    b. Provide an appropriate installation destination folder, and then click **Next**.
    c. Click **Install** on the Ready to Install window.
9. Click **Finish** when the Setup Wizard completes.

    For more information about starting Network Atlas and creating a new map, see Creating Basic Maps.

Starting Network Atlas

Starting Network Atlas requires launching the application, connecting to the appropriate server, and selecting the map which you want to open.

Note: To take full advantage of Network Atlas features, users must have either node management rights in Orion NPM or the administrator role in Orion EOC.

To start Network Atlas:

1. Log on to the computer hosting your Network Atlas installation.
2. Click **Start > SolarWinds > Network Atlas**.
3. Connect to your primary Orion server, as directed in the following procedure:
    a. Provide your Orion **Login** and **Password**.

        Note: Your Orion **Login** and **Password** correspond to your Orion Web Console **User Name** and **Password**.

    b. Provide the IP address or hostname of your primary Orion server in the **Address** field.
    c. ***If you are connecting to an Orion NPM server***, select **Orion** as the **Connect to** target.

d. ***If you are connecting to an Orion EOC server***, select **EOC** as the **Connect to** target.

e. Click **Connect**.

4. Now on the Network Atlas Welcome screen, select what map you want to open in the Network Atlas:
   - To open a recent map, select it in the **Open Recent** section.
   - To open a map available in a certain location, click **Browse** and navigate to the map.
   - To create a new network map, click **Network Map** in the **Create New** section. For more information, see Creating Basic Maps.
   - To create a wireless heat map, click **Wireless Heat Map** in the **Create New** section. For more information, see Creating Wireless Heat Maps.

Creating Basic Maps

Creating a map can be as simple as selecting a background image, dragging network resources onto the drawing area, and connecting the objects with lines.

To create a basic map:

1. Start the Network Atlas.
2. Click **Network Map** in the **Create New** section.

A new empty network map will open in the Network Atlas.

Decide what you want to have in the map and accomplish the appropriate tasks:

- Adding Map Objects
- Connecting Objects Automatically with ConnectNow
- Connecting Map Objects Manually
- Using Object Links to Represent Interface Status
- Interpreting Map Links
- Using Anchor Points to Reshape Map Links
- Adding a Background
- Saving Maps

- Opening Maps
- Displaying Maps in the Web Console

Adding Map Objects

Any objects monitored by SolarWinds NPM or SAM may be added to a Network Atlas map, including all of the following:

- NPM nodes, interfaces, volumes, and Universal Device Pollers (UnDPs)
- SAM applications and components
- VoIP & Network Quality Manager operations
- Network Atlas nested maps; and network links.

For more information about populating an Orion database with your network devices, see "Discovering and Adding Network Devices" in the *SolarWinds Orion Common Components Administrator Guide*.

For information about monitoring applications and application components with SAM, see the *SolarWinds Server & Application Monitor Administrator Guide*.

To add monitored objects to your map:

1. ***If you are creating a new map,*** click the Orion Network Atlas button (), and then click **New Map**.
2. ***If you are adding objects to an existing map,*** complete the following steps:
    a. Click the Network Atlas button ().
    b. Click **Open Map**.
    c. Navigate to your existing map, and then click **Open**.
3. Expand and navigate the node tree in the left pane to locate the network nodes and monitored objects you want to add to your map.

    Note: All monitored applications, application components, interfaces, volumes, and Universal Device Pollers, associated with monitored nodes, in addition to other maps listed in the left pane, are available as map objects. Click **+** to expand any listed node and object types and view associated interfaces, volumes, applications.

4. Drag selected objects onto the drawing area.

   Notes:

   - If you want to add all the objects of a selected type on a selected node to your map in a single operation, click **+** next to the node name to reveal all its associated monitored network objects, and then drag all objects in the desired object group onto the drawing area.
   - A checkmark (✔) next to a node or network resource indicates you have already added it to your map.
   - To view details about a map object, hover over it with the mouse pointer.
   - To locate a specific map object in your map, click its network resource in the left pane. This selects the map object.

Connecting Objects Automatically with ConnectNow

Using the ConnectNow tool, Network Atlas can automatically draw lines between directly connected nodes on your network.

ConnectNow displays connections based on data polled for nodes with enabled L2 and L3 topology pollers, as well as for unidentified nodes.

An unidentified node is a node that was found on the network but which is not managed by Orion. These devices might be switches, hubs, routers, or other devices without names or addresses. They can also be virtual, generated to signify an indirect connection within your map in cases when a topology calculation cannot find any direct connections between two nodes. In these cases, an unidentified node is generated between the two known nodes.

For more information about adding individual nodes in the Orion Web Console, see Adding Devices for Monitoring in the Web Console.

For more information about network discovery, see "Discovering and Adding Network Devices" in the *SolarWinds Orion Common Components Administrator Guide*.

Notes:

- The ConnectNow tool cannot draw indirect connections between nodes. For example, if nodes A and C are connected indirectly through node B, you

must manually add node B to the map to create the connections.

- Orion Enterprise Operations Console (EOC) does not support ConnectNow.

To automatically connect objects using ConnectNow:

1. Add appropriate nodes to an open network map.

   Note: For more information about adding objects to a network map, see Adding Map Objects.

2. Click **ConnectNow** () in the **Home** ribbon.

Updating the Topology

ConnectNow displays data stored in the TopologyConnections database table. By default, the data are re-calculated every 30 minutes. You can update the data manually.

To update your topology manually:

1. Log in the Orion Web Console using and account with administrative privileges.
2. Go to **Settings > Manage Nodes.**
3. In the **More Actions** drop-down list, select **Update Topology**.

The values in the TopologyConnections table will be re-calculated and your topologies will be updated.

Connecting Map Objects Manually

You can represent network links in your map by drawing lines between map objects. If a connected object is down, any connected links change color to red.

To manually connect map objects:

1. Make sure the **Home** ribbon is selected.
2. Click **Straight** () or **Curved Line** () in the **Lines** group, as appropriate.
3. Click an object with the line drawing tool to begin drawing the link
4. Click and drag as needed to set optional anchor points along the link path.
5. Click a second object to finish drawing the link.

6. ***If you want the links connecting your mapped objects to communicate the status of connected interfaces,*** complete the following steps:
    a. Right-click a link, and then select **Properties**.
    b. Select **Status** in the left pane of the Link Properties page.
    c. Drag the appropriate interface objects from the left pane of the Orion Network window to the link status assignment areas.

Using Object Links to Represent Interface Status

The following procedure configures an object link to represent the status of its connected interfaces.

To use object links to represent actual interface states:

1. Right-click a link, and then select **Properties**.
2. Select **Status** in the left pane of the Link Properties page.
3. Drag the appropriate interface objects from the left pane of the Orion Network window to the link status assignment areas.

Interpreting Map Links

Links created on Network Atlas maps are not merely connectors between network objects. Map links display the states and performance of the interfaces through which your linked objects are connected. Interface states and performance data are determined from Orion NPM polling data.

Interface performance information in maps can be communicated using the interface status or performance:

- Determining Interface Status
- Determining Interface Performance

Determining Interface Status

Connections are shown as either solid or dotted lines. A solid line indicates that the connection is UP. A dotted line indicates that the connection is DOWN.

The following table relates how interface states are reflected in the status of a link between NodeA, with InterfaceA, and NodeB, with InterfaceB.

Note: Link status is only shown as either UP or DOWN. To emphasize potential problem links, DOWN status is granted a higher priority.

		InterfaceB Status		
		UP	DOWN	UNKNOWN
InterfaceA Status	UP	UP	DOWN	UP
	DOWN	DOWN	DOWN	DOWN
	UNKNOWN	UP	DOWN	DOWN

Determining Interface Performance

In addition to interface status, map links can show either interface utilization or interface connection speed. A legend is available to interpret colors representing interface performance data.

To display interface performance data:

1. Click **Connection Display Options** in the bottom left pane.
2. Select any of the following options, as appropriate:
   - **Show Link Utilization** provides interface utilization information in colored links. This option is selected and is shown by default on new maps.

     Note: Utilization data is not shown for manually created links.
   - **Show Link Speed** provides interface connection speed information in colored links.
   - **Don't show additional info** provides only interface UP/DOWN status information on device links. This is the default option for previously created maps.
   - **Include Link Labels** enables or disables displaying connection labels.

Using Anchor Points to Reshape Map Links

You can use anchor points to change the shape of object links on your map, as shown in the following procedure.

Note: Use multiple anchor points to create more complex shapes and curves.

To use object link anchor points:

1. Click **Select** in the **Tools** group or click the middle mouse button.
2. Click and drag the link you want to reshape.

Adding a Background

You can select colors, textures, and locally-hosted or Internet-hosted images to serve as your map backgrounds.

- Selecting a Background Color
- Selecting a Background Texture
- Selecting a Background Image
- Clearing the Background

Selecting a Background Color

Network Atlas supports 24-bit color backgrounds.

To set a map background color:

1. Click **Home**.
2. Click **Background > Background Color** ().
3. Select a color from the palette, or click **More Colors** to select a custom color.

Selecting a Background Texture

Network Atlas also provides numerous colored textures that can serve as map backgrounds.

To set a map background textures:

1. Click **Home**.
2. Click **Background > Background Texture** ().
3. Enter appropriate values for the **Width** and **Height** of your map in the **Map Size in Pixels** area.

   Note: The default values are the smallest area bounding the existing map objects and labels.
4. Select a texture to apply as your map background, and then click **OK**.

Selecting a Background Image

Network Atlas allows you to use images as your map background. The source of the background image can be a graphics file on your hard drive or a URL link to a graphics file on the Internet in any of the following graphics formats:

- Graphics Interchange Format (.gif, non-animated)
- Tagged Image File Format (.tiff)
- Joint Photographic Experts Group (.jpg)
- Microsoft Windows Bitmap (.bmp)
- Portable Network Graphics (.png)

Linked backgrounds are updated when the map is accessed or when the browser page is refreshed. In a typical use case, a linked background is used to provide weather data from an Internet weather service on a network map.

Notes:

- Files used for linked backgrounds must be continuously accessible by URL reference.
- Files used for static backgrounds must be available within the local file system.
- Background images you supply display at their full size in the Orion Web Console, so consider their dimensions. You may rescale images within the application, but images displayed at full scale provide optimal quality.
- In determining map size and resolution, consider web page layouts and potential display screen resolutions.

- Example background images are in the **NetworkAtlas Backgrounds** folder located in your default shared documents folder. Clicking **Background Image** always starts you in this background images folder.

To select a background image:

1. Click **Home**.
2. ***If you want to use a background image from disk,*** click **Background > Background Image**, and then navigate to the image you want to use.
3. ***If you want to use a background image from the Internet,*** complete the following steps:

    a. Click **Background > Linked Background**.

    b. Type the URL of the image you want to use.

    c. Click **Validate**.

    d. Click **OK**.

    Notes:

    - In the web console, map background images linked from the Internet are refreshed with the Orion Web Console refresh.
    - If the SolarWinds NPM server is behind a web proxy, the proxy settings entered into Microsoft Internet Explorer are used to create the Internet connection. If the web proxy requires authentication, you cannot link directly to the background image. A workaround is to write a script that periodically downloads the Internet image and saves it to a folder on the web server. You can then specify the saved image as the linked background image.

Clearing the Background

To clear the current map background, click **Home**, and then click **Background > Clear Background** ().

Saving Maps

Network Atlas saves your maps directly to the server to which you are connected.

Note: To save a map to your hard drive instead of your Orion server, click > **Export** > **Export Map**.

To save a map:

1. Click the Network Atlas button (), and then click **Save**.
2. ***If you are saving the map for the first time***, name the map, and then click **OK**.
3. ***If you want to save your map to your hard drive,*** complete the following steps:
    a. Click > **Export** > **Export Map**.
    b. Navigate to an appropriate location on your hard drive.
    c. Provide a **File name**, and then click **Save**.

Opening Maps

Maps are loaded from the Orion server to which you are connected. They appear in the left pane of the Network Atlas window.

To open a map:

1. Click **+** to expand the Maps group in the left pane of the Network Atlas window.
2. Double-click the map you want to open.

Note: You can also click the Network Atlas button in the top right-hand corner and select Open Map.

Displaying Maps in the Web Console

You can display saved maps in the Orion web console Network Map resource. The procedure for selecting Network Maps is different between Orion EOC and Orion NPM, and maps created for one are not compatible with the other.

Select either of the following procedures, as appropriate:

- Map Resources in the Orion Web Console
- Displaying Maps in the Orion Web Console
- Displaying Maps in the Orion EOC Web Console

Displaying Maps in the Orion EOC Web Console

The following procedure opens a saved map in the Orion EOC Web Console.

Note: For more information about converting maps to display in an Orion EOC Web Console, see Importing Maps into Orion EOC.

To display a saved map in the Home view of the Orion EOC web console:

1. Log on to the Orion EOC web console with an Administrator account.
2. Click **Settings**.
3. Click **Manage Views**.
4. Select **Home**, and then click **Edit View**.
5. Click **Resource**.
6. Click **Network Map** in the Added list.
7. Select your map from the **Select Network Map** list, and then click **Save**.
8. Click **OK, Save Changes**.
9. ***If prompted to confirm your changes***, click **OK**.
10. Click the **Home** view to see your map.

Creating Wireless Heat Maps

Wireless heat maps help you visualize wireless signal coverage on a building floor plan.

Note: If you want to see the location of your clients on wireless heat maps in the Orion Web Console, you need to add at least 3 access points and 1 signal sample, or 4 access points into the map.

To create wireless heat maps:

1. Start **Network Atlas** in your SolarWinds program folder. For more information, see Starting Network Atlas.
2. On the Welcome to Orion Network Atlas Screen, select **Wireless Heat Map** in the **Create New** section.
3. Enter a name for the new map.
4. Set a floor plan image for the background. For more information, see Setting a Floor Plan as Background.

5. Set the map scale. For more information, see Setting the Wireless Heat Map Scale.
6. Add one or more managed wireless access points. For more information, see Adding Wireless Access Points.
7. Optional: Add signal samples to improve the map accuracy. For more information, see Taking Signal Samples.
8. Click **Generate** to display wireless signal coverage on the map.

Wireless Heat Map Poller

Wireless heat map poller collects information about the signal strength on monitored access points. By default, this poller is disabled on your devices because of performance issues.

However, to include an access point in a wireless heat map, Network Atlas needs information contained in this poller. Network Atlas thus automatically enables the wireless heat map poller on the appropriate wireless controller.

When do I need to disable the wireless heat map poller?

If you start experiencing performance issues when working with wireless heat maps, you might need to disable the wireless heat map poller on appropriate devices. Disabling the poller will resolve performance issues, but your wireless heat maps will not be updated any more. Appropriate resources in the Orion Web Console and the Network Atlas will both be able to display the last status that had been generated before you disabled the wireless heat map poller.

To disable the wireless heat map poller:

1. Log into the **Orion Web Console** using and account with administrator privileges.
2. Click **Settings** in the top right corner, and then click **Manage Pollers** in the Node & Group Management grouping.
3. Locate the wireless heat map poller in the pollers table, and click the appropriate item in the **Assignments** column, such as **1 Node**. Clicking the assignments link opens the **Assign Wireless Heat Map to Nodes** view.
4. Select all nodes for which you want to disable the poller, and then click **OFF: Disable Poller** button in the table title.

Note: Clicking the grey **OFF** icon for individual nodes in the **Poller Status** column disables the poller for the appropriate node. The icon will turn to green **ON** and the poller will be disabled.

Setting a Floor Plan as Background

The floor plan should reflect the real dispositions of the office or buildings on the map. Setting a floor plan as the background for your heat map allows you to correctly position the wireless access points and reflect the wireless signal coverage on your map.

Requirements:

The floor plan must be a graphic file in one of the following graphics formats:

- Graphics Interchange Format (.gif, non-animated)
- Tagged Image File Format (.tiff)
- Joint Photographic Experts Group (.jpg)
- Microsoft Windows Bitmap (.bmp)
- Portable Network Graphics (.png)

  Note: To ensure the best readability possible of the resulting wireless map, use black and white images.

To set a background for your heat map:

1. Click **Background Image** on the **Home** ribbon.
2. Navigate to the floor plan image that you want to use as the background for your heat map, select the appropriate image, and click **Open**.

   The floor plan will appear as the background for your heat map.

Setting the Wireless Heat Map Scale

For an accurate display of the wireless coverage provided by your wireless access points, you need to set the scale for your wireless heat map.

Requirements

- You have already inserted a background image for your wireless heat map (a floor plan).

- You need to know the distance of two objects displayed on the background image.

  Note: To minimize error, set scale for the longest distance possible, such as the building or floor length.

You can use online maps, such as Google Maps, to measure your office building. Locate the building on Google Maps, right-click it and measure the distance of the office building walls.

To set the map scale:

1. Click **Set Scale** in the **Home** ribbon. A blue line segment with squares as end points will appear in the plan.
2. Drag endpoints of the segment to the objects on the map whose distance you know.
3. Fill in the distance between the endpoints into the appropriate field, and select the units (feet or meters).

   Example: In floor plans, you usually know the dimensions of individual rooms. Drag and drop the line segment end points so that the end points are located on the opposite walls, and fill in the width of the room.
4. Click **Set Scale** to apply the scale to your wireless heat map.

Adding Wireless Access Points

Generating a wireless heat map requires that you insert wireless access points used by client devices into the map.

Requirements

- Appropriate wireless LAN controllers must already be managed in NPM.
- Currently, only Cisco controllers are supported.
- Wireless Heat Maps require that the Wireless Heat Map poller be enabled on the wireless LAN controllers that you intend to use in the map.

To add wireless access points to the map:

1. Go to the navigation tree in the left-hand part of Network Atlas main screen.
2. Locate the wireless access points that you want to add to the wireless heat map.

   Note: To find access points on a node, navigate to Orion Objects > vendor name, such as Cisco > appropriate node > Wireless Access Points.
3. Drag and drop one or more access points to their location on the map.

The selected access points will appear on the appropriate location in the map.

Taking Signal Samples

Wireless heat maps display the ideal wireless signal coverage, they do not count with physical obstacles, such as office walls. To make wireless heat maps more real, you can take signal samples - measure the wireless signal strength on devices within your office whose location you know. These devices may include cell phones, laptops, or tablets connected to your wireless network.

When you want to take a signal sample, you insert the device into its location on the map. Network Atlas measures the signal strength in the appropriate location, and includes the measured value into the map calculation.

Signal samples represent the signal strength measured in a specified location. They stay in the map and are designated by a wireless signal strength icon. The measured signal strength will influence the calculation of heat maps even after the client used for creating the sample moves from its position.

Note: If you move your access points, please keep in mind that your signal samples might not be accurate any more. Consider deleting obsolete signal samples and adding new ones.

Add simple or multiple signal samples into places where you expect the signal to be blocked by walls or other obstacles, or to places where the signal strength does not correspond with your heat map.

Polling the signal is usually faster for cell phones. Consider taking signal samples using a cell phone.

Simple Signal Samples

You can use one wireless device, walk it to a certain location and take a signal sample there. After you take the sample, you can walk the device to another location and take another signal sample. This procedure is also called "walking edition" because it requires you to walk through the office.

Multiple Signal Samples

If you have multiple wireless devices and want to measure the wireless signal strength on more of them, take multiple signal samples (also called "sitting edition" because you can do it sitting at your desk).

Requirements

- You need to have a wireless heat map created and open in the Network Atlas.
- You need to have wireless access points added into the map.
- You need to have clients, such as cellular phones, tablets, laptops, connected to the access points positioned in your wireless heat maps.

Taking Simple Signal Samples

Simple signal sample allows you to take your device connected to a wireless access point, walk it to the position where you want to take a signal sample, and measure the signal strength there. Network Atlas will create a signal sample and include the measured values into the heat map calculation. You can then walk the device to another location and use it to create another signal sample, using the same device.

To take a simple signal sample:

1. Click **Take Signal Sample** in the **Home** ribbon. The **Signal Sample** wizard will display in the right-hand part of Network Atlas as a tab.
2. Walk your device to the location where you want to measure the wireless signal strength and click **Next**.
3. Select the wireless client (cellular phone, laptop, or tablet) whose location you know in the drop-down list and click **Next**.

4. Drag and drop the selected client into its current location, and click **Next**. Network Atlas will start measuring the wireless signal strength in the appropriate spot, which can take a few minutes, depending on the particular device.
5. ***If you want to add another signal sample***, click **Repeat**, walk the device to a new location, and repeat steps 3-4.
6. ***If you want to apply the measured signal strength to the heat map***, click **Generate Map**.
7. Network Atlas will regenerate the map accordingly. Click **Close** to hide the Signal Sample wizard tab.

Taking Multiple Signal Samples at the Same Time

If there are more devices connected to your wireless access points, you can use these devices to create multiple signal samples at the same time.

To take multiple signal samples at the same time:

1. Click **Take Signal Sample** in the **Home** ribbon. The **Signal Sample** wizard will display in the right-hand part of Network Atlas as a tab.
2. Click **Use multiple devices to take signal samples**.
3. Drag and drop appropriate clients to their positions on the wireless heat map, and click **Next**.

   Notes:

   - If there are too many devices, use the search box to find the devices you want to use for creating signal samples.
   - Network Atlas will start measuring the wireless signal strength in the signal sample points, which can take a few minutes.
   - If the signal measuring fails, Network Atlas informs you about it, and you can either repeat the measurement for the device, or start the wizard anew.
4. Network Atlas will automatically regenerate the map according to the defined signal samples. Click **Close** to hide the Signal Sample wizard tab.

Troubleshooting Wireless Heat Maps

If your wireless signal coverage on your wireless heat maps is not as expected, you can take the following troubleshooting measures.

- Make sure that the map scale you have entered is precise.
- Make sure that your access points are located correctly.
- Verify that signal samples are up-to-date.
- The signal samples stay in the map even after the device you measured the signal strength on moves away. If you change the position of your access points, or the dispositions of your office, the signal samples might not be accurate and could affect the calculated wireless heat map.
- Delete obsolete signal samples.

  To delete a signal sample, open the wireless heat map in the Network Atlas, select the signal sample, and press the Delete key.

- Add new signal samples. For more information, see Taking Signal Samples.

Advanced Mapping Techniques

You can apply a number of advanced mapping techniques to enhance the usefulness of your maps, such as zooming in and out, creating nested maps, adding map objects, changing the appearance of objects, links, or labels, or linking objects to URLs or embedding maps in web pages.

This section discusses the following topics:

- Zooming In and Out of a Map
- Creating Nested Maps
- Displaying Map Object Metrics
- Adding Independent Map Objects and Floating Labels
- Changing the Appearance of Map Objects
- Changing the Appearance of Links
- Changing the Appearance of Labels
- Linking Map Objects to URLs
- Linking or Embedding Maps in Web Pages

Zooming In and Out of a Map

Network Atlas allows you to zoom into a map to enlarge details or to zoom out to reduce its size. Zoom level is a visual aid, and it is not saved with the map.

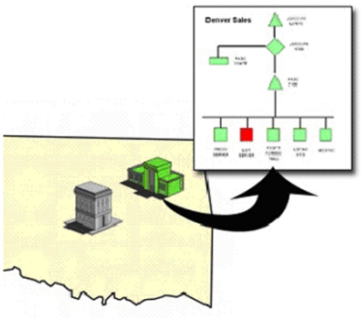
Use any of the following methods to zoom in or out on a displayed map:

- Press and hold CTRL while rotating the mouse wheel button.
- Click the **Zoom** slider on the status bar, and then slide the zoom control to the zoom level you want.
- Click **View**, and then select the type of zoom you want to use from the Zoom group.

Creating Nested Maps

Nested maps allow you to navigate through a map to see multiple levels of detail. For example, a map of the United States can include an icon for a child map of Oklahoma. You can then click the Oklahoma object to open the child map.

The map of Oklahoma can then become a parent map to a network diagram.



Each child map can include a view of the objects, either devices or other maps, deployed on it. Any nested objects can then be clicked to view the next level of map detail, until the level of the final network device is reached and all available network information is displayed.

Note: The total number of objects on a map, including those displayed on child maps, affects how fast the map loads in the Orion Web Console. If your maps load slowly, decrease the number of map objects.

To create a nested map:

1. Drag a map from the Maps group in the left pane onto the parent map, and then position the map icon appropriately.
2. ***If you want the status of a child map to also indicate the status of its child objects,*** complete the following steps:
    a. Right-click the child map icon on the map, and then select **Properties**.
    b. Check **Include child status** on the Status properties page, and then click **OK**. The object status icon now includes the secondary status indicator.

Displaying Map Object Metrics

The status of a map object icon reflects its current state, such as up or down. You can add a secondary status indicator to a map object to reflect metrics such as response time, CPU load, or the state of any child objects. This secondary status indicator appears at the bottom right corner of the status icon.

To add the secondary status indicator:

1. Right-click the map object, and then select **Properties**.
2. Check **Include child status** on the Status properties page, and then click **OK**.

To change the thresholds of the metrics:

1. Right-click the map object, and then select **Properties**.
2. Click **Metrics** to view the Metrics properties page.
3. ***If you want to change the warning or critical threshold for a metric,*** click the threshold value, and then type a new value.
4. ***If you want to ignore a metric,*** uncheck the metric.
5. Click **OK**.

Notes:

- The secondary status indicator respects the Orion web console Status Rollup Mode setting for displaying status.
- All child objects and selected metric thresholds are taken into account to determine secondary status.

Adding Independent Map Objects and Floating Labels

You can add independent map objects and labels that do not have associations to network nodes or resources.

To add an independent object:

1. Click **Home**.
2. Click **Add Object** in the Objects group to add a gray map object to the map.

Independent labels may also be placed anywhere on your map.

To add an independent label:

1. Click **Home**.
2. Click **Add Label** in the Labels group. A label is added to the map.

Changing the Appearance of Map Objects

Changing the graphics that represent map objects is an excellent way of increasing the information density of your map without increasing the map complexity.

You can set the default representation style for all map object of a certain type, or you can change the appearance of selected map objects.

To set the default representations of map objects:

1. Click the Orion Network Atlas button, and then click **Network Atlas Settings**.
2. Click **Graphic Styles** in the left column.
3. Select an appropriate default style for each available map object.

Changing the representation of selected map objects opens up another level of graphical information. For example, you can set an object icon to display a mainframe graphic, visually designating the type of device being monitored. You can then select a status style, such as 3D Pad Underneath, to illustrate the map object status.

To change the representation of selected map objects:

1. Right-click a map object, and then select **Properties**.
2. Click **Appearance** in the left column of the Properties page.
3. ***If you want the map object to appear as a fixed-size, LED-type graphic***, complete these steps:
    a. Select **Orion LED Status Icon**.
    b. Select a style from the Orion LED Status Icon **Style** list, and then click **OK**.
4. ***If you want the map object to appear as a scalable shape***, complete these steps:
    a. Select **Shape**
    b. Select a style from the Shape **Style** list, and then click **OK**.
    c. Drag a corner handle on the map object to resize the shape.
5. ***If you want the map object to appear as a scalable graphic***, complete these steps.
    a. Select **Graphic**.
    b. Click **Select Graphic**, select an appropriate graphic, and then click **OK**.
    c. Select a status style from the Graphic **Style** list, and then click **OK**.
    d. Drag a corner handle on the map object to resize the graphic.

Pasting Custom Icons from the Windows Clipboard

You can paste graphics from the Windows clipboard directly into your Network Atlas maps and then display an overlay behind them to depict the status.

Icons that you paste into Network Atlas are saved to the Orion database, and made available for reuse in other maps under the "Imported" icon grouping. Pasted icons saved to the Orion database can be accessed and used by remote instances of Network Atlas.

To paste a custom icon into Network Atlas:

1. Open the icon image in a graphics program such as Visio or Photoshop.
2. Copy the image to the Windows clipboard with the Copy command.
3. Open the appropriate map in Network Atlas.
4. Paste the image as a new object following these steps:
    a. Right-click on the map and then click **Paste**.
    b. Select **Paste the image from the Clipboard as a new object**.
    c. Enter a name for the new image in the **Please enter a name for the new image** field.
    d. Click **OK**.

Icons added in this manner are also saved on the Orion NPM server in the path **%APPDATA%\SolarWinds\NetworkAtlas\Maps\Orion\<orion server address>\NetObjects\Imported**.

%APPDATA% is typically located in **C:\Documents and Settings\<logged on user>\Application Data** for Windows XP, and **C:\Users\<logged on user>\AppData\Roaming** for Windows Server 2008.

To delete a custom icon:

1. Determine which file on the Orion NPM server contains the icon (for example, **mypicture.wmf**).
2. Add **.del** to the file name (for example, **mypicture.wmf.del**).
3. Start Network Atlas on the NPM server to delete the icons from the database.

Adding Custom Icons from Graphics Files

You can use any Windows Media File **(.wmf**) or Graphics Interchange Format (**.gif**) format graphic as a custom icon, but you must name the graphic files according to their roles. The file name must not contain any other dash (-) characters other than depicted in this table.

Role	File name
Critical status	iconName-**critical.gif**
Down status	iconName-**down.gif**
External status	iconName-**external.gif**
Icon with no status	iconName.**gif**
Unknown status	iconName-**unknown.gif**
Unmanaged status	iconName-**unmanaged.gif**
Unplugged status	iconName-**unplugged.gif**
Unreachable status	iconName-**unreachable.gif**
Up status	iconName-**up.gif**
Warning status	iconName-**warning.gif**

To add custom icons from graphics files:

1. On your Orion NPM server, create the folder:

   %APPDATA%
   \SolarWinds\NetworkAtlas\Maps\Orion\<orion server address>\NetObjects\User Graphics.

   Note: %APPDATA% is typically **C:\Documents and Settings\<logged on user>\Application Data** for both Windows XP and Windows Server 2003, and **C:\Users\<logged on user>\AppData\Roaming** for Windows Server 2008.

2. Copy the graphics files to this folder.
3. Start Network Atlas on the Orion server to finalize the additional icons.

After copying the graphics files to their location, you can assign them as an icon as you would any other graphic image.

To assign a custom icon to an object:

1. Right-click the object on the map, and then click **Select Graphic**.
2. Select **User Graphics** in the left pane.
3. Select the appropriate graphic image, and then click **OK**.

Changing the Appearance of Links

Orion Network Atlas allows you to change the appearance of network links by customizing their width, color, and line styles.

To change the appearance of a link:

1. Right-click a link, and then select **Properties**.
2. Select **Appearance** in the left column of the Properties page.
3. Select a line width in pixels from the **Width** list.
4. Select a line color from the **Color** list.
5. Select a line style from the **Style** list.
6. Click **OK**.

Note: The color setting only changes the color of links that have Up status.

Changing the Appearance of Labels

Orion Network Atlas allows you to change the appearance of labels by changing text attributes, borders, and background colors.

To move a label:

- Drag the label to the desired location.

To edit the text in a label:

1. Double-click the label.
2. Press **<SHIFT>+<ENTER>** to separate multiple lines within the same label.

To change the appearance of a label:

1. Right-click the label, and then select **Properties**.
2. Select **Appearance** in the left column of the Properties page.
3. ***If you want to change the font attributes***, click the **…** button, select appropriate font attributes, then click **OK**.
4. ***If you want to change the text alignment***, select an alignment from the **Text Alignment** list.
5. ***If you want to change the text color***, click the **Text Color** box, and then select a new color.
6. ***If you want to add a label border***, select the border width in pixels from the **Border Width** list.
7. ***If you want to change the label border color***, click the **Border Color** box, and then select a new color.
8. ***If you want to remove a label border***, select **0** from the **Border Width** list.
9. ***If you want to add a label background***, uncheck **Transparent Background**.
10. ***If you want to change the label background color***, click the **Background Color** box, and then select a new color.
11. ***If you want to remove a label background***, check **Transparent Background**.
12. Click **OK**.

Linking Map Objects to URLs

Orion Network Atlas allows users to click on map objects in the Orion web console to see more details. By default, map objects are linked to the most relevant Orion details page for the object. You can customize the URL hyperlink to link to external web sites and pages as necessary.

To link a map object to a URL:

1. Right-click the map object, and then select **Edit Hyperlink**.
2. ***If you want to link to the relevant Orion page for the map object***, select **Logical page in Orion**.
3. ***If you want to link to a custom URL***, select **Manually set address**, and then type the URL.
4. Click **OK**.

Linking or Embedding Maps in Web Pages

You can link or embed your maps in other web pages by referencing the URL for the map.

The map URL is in the form:

http://orionServer/Orion/NetPerfMon/MapView.aspx?Map=mapName

orionServer

This is the IP address or host name of your Orion NPM server.

mapName

This is the display name of the map. If the map display name contains space characters, substitute **%20** for the spaces when specifying the name.

Customizing Orion Web Console Tooltips

In the web console, hovering over map objects displays a tooltip providing current identification and status information about the object. Tooltips are customizable for all map object types, and you can customize the tooltips in the Orion Web Console to display additional information by inserting Orion alert variables, custom properties, and other text.

Notes:

- Tooltip customizations are global and affect all maps.
- Orion EOC does not support custom web console tooltips.
- For a complete list of variables available for use in Orion Network Atlas tooltips, see Network Atlas Tooltip Variables.
- Use **${CR}** to enter a carriage return.

To add additional information to map object tool tips:

1. Log on to Orion Web Console as an administrator.
2. Click **Edit** in the Map resource.
3. Click **Customize map tooltips**.
4. Type the variables and any text you want to add in the text field for the appropriate map object type.
5. Click **Submit**.

Importing Orion NPM Maps into Orion EOC

Maps created for use in Orion NPM must be converted before they may be used in Orion EOC. SolarWinds provides a utility for this conversion, as indicated in the following sections.

Map Import Requirements and Configuration

The Orion to EOC Map Converter utility imports maps into Orion EOC v1.5 from other SolarWinds Orion products. Before attempting to convert maps for use in Orion EOC, confirm that your environment meets the following requirements:

- Orion EOC must currently be managing at least one SolarWinds Orion server.
- If Orion EOC is configured to use Active Directory accounts to access Orion servers, confirm that you have entered the password for the AD account in the Orion Logins section of EOC. Additionally, only AD accounts that were individually added to the Orion Server may be used to import a map. Active Directory group accounts are not compatible with Map Converter.

The user running the Orion to EOC Map Converter utility must also meet the following specifications:

- The user must run the Map Converter using a Windows Administrator account that also has Orion EOC Administrator role permissions.
- The user must log into the Map Converter using an Orion EOC account that was individually added to Orion EOC. Active Directory group accounts are not compatible with Map Converter.

- The user must have Orion EOC access to at least one Orion server.
- The user must have Node Management rights on the remote Orion server

To configure your environment for map import:

1. Copy **SolarWinds-OrionToEOCMapConverter-1.5.exe** to your Orion EOC server.
   Note: Download **SolarWinds-OrionToEOCMapConverter-1.5.exe** from http://downloads.solarwinds.com/.
2. Execute **SolarWinds-OrionToEOCMapConverter-1.5.exe**, and then complete the installer.
3. Allow members of the **Users** group **Full Control** of files in the folder **<volume>:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files**, as follows:
   a. Using Windows Explorer, find the folder **<volume>:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files**.
   b. Right-click the folder, and then click **Properties**.
   c. Open the **Security** tab.
   d. ***If you are using Windows 2008,*** click **Edit**.
   e. Select **Users** in the **Group or User Names** list, select **Full Control**, and then click **OK**.
4. Allow the **Everyone** group **Full Control** to the folder **<volume>:\Windows\Temp\SolarWinds\NetworkAtlas\EOC\SolarWinds\NetworkAtlas\MapsWeb\EOC\localhost** and all of its child objects, as follows:
   a. Using Windows Explorer, find the folder **<volume>:\Windows\Temp\SolarWinds\NetworkAtlas\EOC\SolarWinds\NetworkAtlas\MapsWeb\EOC\localhost**.
   b. Right-click the folder, and then click **Properties**.
   c. Open the **Security** tab.
   d. ***If you are using Windows 2008,*** click **Edit**.
   e. Click **Add**.

f. Enter **Everyone** in the **Enter the object names to select** text box, and then click **OK**.

g. Click **Advanced**.

5. Select **Replace permission entries on all child objects with entries shown here that apply to child objects**, and then click **OK**.
6. Click **Yes** when prompted to continue.
7. Select **Everyone** in the **Group or User Names** list.
8. Select **Full Control**, and then click **OK**.

Importing Maps into Orion EOC

The following procedure imports maps into your Orion EOC environment.

To import maps into Orion EOC:

1. Log on to the Orion EOC server with a Windows Administrator account that also has Orion EOC Administrator role permissions.
2. ***If you are using Windows Server 2008,*** right-click **Start > All Programs > SolarWinds > Convert Orion maps to EOC**, and then click **Run as Administrator**.
3. ***If using Windows Server 2003,*** click **Start > All Programs > SolarWinds > Convert Orion maps to EOC**.
4. Select the Orion server hosting your maps from the **Orion** list.
5. Select the maps you want to import into Orion EOC.
6. ***If you want to edit the name of an Orion EOC map you are importing,*** click the map name in the **New Name** column and then edit the name.
7. Click **Import**.

Troubleshooting

The following issues may arise as you import Orion maps into Orion EOC:

- Maps you import from different Orion servers may share the same name. You must rename these maps so that each has a unique name in Orion EOC. Any pre-existing child/parent relationships for any renamed map will

break. You must manually reconfigure parent/child relationships after importing.

- Windows 2008 customers may encounter problems either after manually clicking the Refresh button or after selecting a different Orion server. If the utility crashes, restart it and resume importing.
- If using an operating system such as Windows Server 2008 that has UAC, you must run the program using **Run as Administrator**.

Advanced Map Layouts

You can improve the visual layout and organization of your maps by using the advanced layout tools to help you align and distribute your objects and links.

This section discusses the following topics:

- Positioning Map Objects
- Displaying Grid Guides
- Aligning Map Objects
- Distributing Map Objects
- Selecting Automatic Layout Styles

Positioning Map Objects

Using drag-and-drop from the objects tree on the left, you can place and move map objects anywhere on your map. More precise movement and positioning are also possible, using the nudge and position features.

To nudge a map object, select the object, and then press **<Ctrl> + <arrow>**.

To reposition a map object:

1. Click the map object to reposition.
2. Click the **Edit** ribbon.
3. In the Size & Position area, enter appropriate **X** and **Y** coordinates.

   Note: Map center is designated as (**X**,**Y**) = (**0**,**0**).

Displaying Grid Guides

A grid guide helps you maintain structural and spatial relationships as you arrange your map objects. Network Atlas allows you to select two kinds of grids and to change the grid spacing. Grids are not map objects, and are neither saved with a map nor displayed in the Orion Web Console.

To display a grid:

1. Click the **View** ribbon.
2. Click **Show Grid**  in the Grid group.

To customize the grid:

1. Click **View**.
2. ***If you want grid lines***, click **Grid Option > Grid Lines**.
3. ***If you want grid points***, click **Grid Options >Grid Points**.
4. ***If you want to change the grid size***, click **Grid Options > Grid Size**, and then select a grid size.

Aligning Map Objects

You can change the relative alignment of your map objects using the alignment tools.

To change the alignment of objects in the map:

1. Click the **Edit** ribbon.
2. Select the map objects you want to align.
3. Click the appropriate button in the Align group to arrange your selected objects

Button	Function	Description
	Align Left	Aligns all selected objects on the left edge of the group

Button	Function	Description
	Align Right	Aligns all selected objects on the right edge of the group
	Align Bottom	Aligns all selected objects on the bottom edge of the group
	Align Top	Aligns all selected objects on the top edge of the group
	Center Vertically	Centers all selected objects vertically
	Center Horizontally	Centers all selected objects horizontally

Distributing Map Objects

You can distribute your map objects evenly across the selection area using the distribution tools.

To distribute map objects:

1. Click **Edit**.
2. Select the map objects you want to distribute.
3. Click the appropriate button in the Distribute group to arrange your selected objects.

Button	Function	Description
	Distribute Horizontally	Distributes all objects so that they are equidistant from the left edge of the leftmost object to the right edge of the rightmost object
	Distribute Vertically	Distributes all objects so that they are equidistant from the top edge of the topmost object to the bottom edge of the bottommost object

Selecting Automatic Layout Styles

You can select from the following styles to automatically change the relative positioning of objects your map.

Circular

Emphasizes the clusters inherent in the topology of a map. It emphasizes prominent links between main objects and its peripherals. Object groups have radial placements. Use circular layouts for maps containing ring and star network topologies.

Symmetrical

Emphasizes the symmetrical patterns inherent in the map topology. It emphasizes an even distribution of objects, and minimizes edge crossings. Object groups have star spiral placements. Use symmetrical layouts for maps that have fairly homogenous or uniform clusters.

Hierarchical

Emphasizes mapped dependency relationships by placing objects at different levels. Use hierarchical layouts to depict data dependencies.

Orthogonal

Emphasizes compact drawings and uses only horizontal and vertical edges. Objects are enlarged if necessary to provide enough space for edge connections. Use orthogonal layouts for maps that need to depict multiple clusters in a space-efficient manner.

Tree

Emphasizes parent and child relationships. Child objects are arranged farther from the root object than their parent objects. Use tree layouts for maps that have a central control object.

Reorganize

Moves all mapped objects back to the center of the map view.

Arrange Labels

Restores the default relative position of all object labels.

To arrange map objects according to a layout style:

1. Click **Edit**.
2. Click an appropriate layout style from the AutoArrange group.

Map Properties

The Map Properties window allows you to configure options regarding the following aspects of your map:

- Setting the Map Up Status Threshold
- Overriding Account Limitations

Setting the Map Up Status Threshold

The UP status threshold is the percentage of map objects that must be in an up state on a given map for the map to be represented as up on the parent map.

To set the percentage of map objects that determine Up status of a map:

1. Right-click any empty portion of the map, and then select **Map Properties**.
2. Slide the **Map status will be UP** slider to configure an appropriate up state threshold on the Map Properties page.

Overriding Account Limitations

For security reasons, you may wish to prevent web console users who have account limitations from seeing network nodes on the map they are not allowed to see. By hiding the restricted nodes and links, users with account limitations remain unaware that the nodes even exist.

To hide nodes from users who have account limitations:

1. Right-click any empty portion of the map, and then select **Map Properties**.
2. Select **Remove nodes that users do not have permission to view**.

If you choose to reveal restricted nodes to all users, all web console users can see the restricted nodes, but users with account limitations cannot retrieve any additional information about the restricted node.

To reveal nodes to all users:

1. Right-click any empty portion of the map, and then select **Map Properties**.
2. Select **Allow all users to view all nodes on this map**.

Note: An Orion NPM user with account limitations, but who has permission to run and use the Network Atlas application, can change this setting in the map and see the presence of restricted nodes. Although the user cannot retrieve any information regarding the restricted nodes, this can still be considered a security risk. If this is a concern, do not give node management permissions to Orion NPM users who have account limitations.

Network Atlas Settings

You can customize the default icon styles, map defaults, and node tree specifications from the Network Atlas Settings window.

To open the Network Atlas Settings window, click the Network Atlas button (), and then click **Network Atlas Settings**.

The following sections describe the options available in the Network Atlas Settings window.

Connection Settings

The options in this section allow you to select the default Orion server details.

Map Defaults

The options in this section allow you to set a device threshold for the overall map status. The status indicator reflects the state of many objects at once; therefore, SolarWinds recommends that the map status be set at 100%. At this setting, when any device on a map or sub-map is down, the problem status will be indicated.

Node Tree

The options in this section allow you to customize the view of the node tree located on the left pane of the Network Atlas main window. Some users find it helpful to display the status icons of each node and interface, while others find the vendor network node and interface icons more useful. You may also specify that node names and/or IP addresses be included in the display.

Graphic Styles

The options in this section allow you to select the default graphical styles for Network Atlas. You can change the default style types for network objects, and you can select a color scheme for Network Atlas itself.

Displaying Maps in the Orion Web Console

The following procedure opens a saved map in the Orion Web Console.

To display a saved map in the Home view of the Orion Web Console:

1. Log on to the Orion Web Console using an account with administrative privileges.
2. Click **Edit** in the Map resource.
3. Select your map from the **Select Map** list.
4. Click **Submit**.

Map Resources in the Orion Web Console

The following map-related resources are available in the Orion Web Console:

Map

The Map resource displays a selected map within the Orion Web Console. Objects on the map a user is not permitted to see are hidden from the user, as are any connections to those objects. For more information about including Network Atlas maps in the Orion Web Console, see Displaying Maps in the Orion Web Console.

All Maps

This resource provides a list of all available network maps. Clicking any map name opens a view containing the selected map with a list of the objects included in the map. Clicking an object name or its description opens the corresponding Orion NPM device Details page, providing extensive diagnostic information about the selected map object.

All Wireless Heat Maps

This resource provides a list of all available wireless heat maps. Clicking any map name opens a wireless heat map view containing the selected map, and a list of wireless access points on the map. You can also display clients connected to access points on the map.

Custom List of All Maps

This resource is a customizable version of the All Maps resource.

List of Objects on Network Map

This resource lists all objects displayed on the map shown in the Network Map resource. Clicking an object name or its description opens the corresponding Orion NPM device Details page, providing extensive diagnostic information about the selected map object.

Displaying Wireless Heat Maps in the Orion Web Console

In the Orion Web Console, you can display your wireless heat maps created in the Network Atlas, in the Wireless Heat Map resource.

You can also display the location of your wireless clients connected to access points available in the wireless heat map. For more information, see Viewing the Location of Clients in Wireless Heat Maps.

To display wireless heat maps in the Orion Web Console:

1. Create the appropriate wireless heat map in the Network Atlas. For more information, see Creating Wireless Heat Maps.
2. Log in to the Orion Web Console.
3. To open a wireless heat map, use one of the following options:
   - Go to the All Wireless Heat Maps resource and click the thumbnail for the appropriate map. The map will open in the Wireless Heat Map view that includes all resources specific for wireless heat maps.

     Note: By default, the All Wireless Heat Maps resource is available on the NPM Summary view.
   - Add the Map resource on the appropriate view, click **Edit**, select the appropriate map in the list, and click **Submit**. For more information, see Editing Views.

Updating the Map

By default, the map is regenerated once a day and the information about clients connected to wireless access points is collected every 5 minutes.

To change the polling settings:

1. Go to Polling Settings, for example via **Settings > Polling Settings**.
2. Scroll down to the **Wireless Heat Map** area.
3. Adjust the **Map Generation Start Time** or **Default Client Signal Strength Poll Interval**, as appropriate.

Viewing the Location of Clients in Wireless Heat Maps

The Wireless Heat Map resource allows you to see the location of clients connected to access points available on a wireless heat map.

To be able to view clients in a wireless heat map, you must add at least 3 access points and 1 signal sample, or 4 access points into the map.

To display wireless clients in the Orion Web Console:

1. Create the appropriate wireless heat map in the Network Atlas. For more information, see Creating Wireless Heat Maps.
2. Log in to the Orion Web Console and open the appropriate wireless heat map in the Wireless Heat Map resources. For more information, see Displaying Wireless Heat Maps in the Orion Web Console.
3. Make sure the **Show connected wireless clients** option is selected.

   You should now be able to see clients currently connected to access points available on the map.

   Note: If you cannot see a client on the map, its position might be calculated outside the selected map. To verify this, consult the **Displaying** item in the legend. If the map shows less clients than are actually connected, such as 1 out of 3, it means that the remaining clients are either outside of the map, or filtered out.

Limiting the Number of Displayed Clients

Displaying too many clients on the map might make the map too crowded, and could also cause performance issues. A wireless heat map can show maximum of 100 clients.

To limit the number of clients on the map:

1. Go to the Map resource.
2. Click **Select which clients to show**.

   Note: You can also click the **Edit** button in the resource instead.

3. Click **+** next to **Select Wireless Clients To Be Specified**.
4. Define how the displayed clients should be selected:

Random Selection of All Clients

To limit the number of all clients, Select **Show every client connected to any AP on the map**.

If you want to limit the number of clients, select the **Limit the number of clients to** box, and fill in the number of clients to be shown on the map (1-100).

Clients Connected to an AP

To limit the number of clients connected to a specified access point:

a. Select **Only Show clients connected to a specific AP**.

b. Select the appropriate Wireless AP in the list.

c. If you want to limit the number of clients, select the **Limit the number of clients to** box, and fill in the number of clients to be shown on the map (1-100).

Select which clients to show

To select specific clients to be displayed on the map:

a. Select **Let me pick specific clients to show**.

b. Use the Group and Search by filters and select appropriate clients to be displayed in the view.

5. Click **Submit** to apply your settings.

Chapter 19: Creating and Viewing Reports

SolarWinds provides you with a wide array of predefined reports for each Orion module, and a web-based interface that enables you to customize these predefined reports and create your own reports, which can be printed or exported in a variety of formats.

In addition to using the Orion Web Console to view and create reports, you can also use the Orion Report Writer to maintain legacy reports created prior to the introduction of the Web Console Report Interface.

The following sections provide detailed information related to creating, viewing, and managing SolarWinds reports:

Predefined Orion Reports

Your SolarWinds installation comes with many predefined reports that can be used as soon as there is data to be reported on.

To view the list of available reports in the Web Console:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. On the **Home** tab, click **Reports**.

To view the list of predefined reports in the Report Writer:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Report Writer**.

These predefined reports are sufficient for most needs, but for specialized requirements, these can be easily customized. You can also create entirely new report layouts. For more information, see Viewing, Creating, Exporting, Importing, Editing and Scheduling Reports in the Orion Web Console.

Note: Legacy reports created prior to the introduction of the Web Console report interface can only be edited using the Report Writer. For more information, see Using Report Writer.

Viewing, Creating, Exporting, Importing, Editing and Scheduling Reports in the Orion Web Console

The **Reports** tab in the Orion Web Console enables you to view, edit, create, export, print and schedule reports for your SolarWinds Orion installation.

Note: The Orion Web Console does not allow you to edit legacy reports created with the Orion Report Writer. Use the Report Writer to edit these. For more information, see Using Report Writer.

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 > Orion Web Console**.
2. Log in to the Orion Web Console, and then click **Home > Reports**.
3. Select an appropriate report grouping in the Group by: field.
4. Check the report you want to view, and then click **View Report**.

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.

Creating Reports in the Web Console

Highly customizable reports, featuring the same charts, tables, gauges and resources available in web console views, can be created directly from the web console.

There are two ways to create a new report in the web console:

- ***Modify an existing web-based report.*** Add new content to and/or edit the existing content of an existing report. This is the recommended approach for new users. See Modifying an Existing Web-Based Report.
- ***Create a completely new report.*** Select the layout and contents for the report. See Creating a New Web-Based Report.

Modifying an Existing Web-Based Report

Modifying an existing web-based report is often the simplest way to generate a new report. This can be as easy as adding a new resource (a table or chart) to the report. You can also edit information about each resource, such as its title. Advanced users can create their own tables and charts.

To modify an existing web-based report:

1. Log in to the Orion Web Console.
2. Click **Home > Reports**.
3. Click **Manage Reports** in the upper right.
4. Select **Report Origin** in the **Group by** dropdown in the left pane, and select **Web-based** from the list below.
5. Select the report to use as the basis for your new report, and click **Edit Report** to display the Layout Builder view.
6. ***To change the size of your report,*** either click **Fit to window width** to fit the modified report to the current browser window, or enter a new value, in pixels (px), in the **Report width** field.
7. In the Header area:
   - Edit the **Title** and **Subtitle**, if required.
   - ***To replace the current logo,*** confirm that **Logo** is checked, and then click **Browse for logo** to select your new logo.
8. In the Content area:
   a. If you want to change the layout, either select the **Page Layout** from the drop-down list on the left, or select the required number of **Layout columns**.
   Note: If you already have content in the report you should be careful when removing columns.
   b. Click **Add Content** to add appropriate elements to columns. You can also delete or edit existing content.
   Note: For more information, see Adding Content to a Web-Based Report Column.

9. ***To change the footer in your report,*** confirm that **Footer** is checked, and complete the following steps.
    a. ***To include the report creation date in the footer,*** confirm **Creation date** is checked.
    b. ***To provide custom text in the footer,*** confirm **Custom text** is checked, and enter the text.
10. Click **Next** to display the Preview view.
11. ***If the preview is how you want the report to be,*** click **Next** to display the Properties view.
12. ***If not,*** click **Back**, and make the required edits, as covered in previous steps.
13. ***To mark this report as one of your Favorite Reports,*** check **My Favorite Reports**. Marking a report as a favorite promotes it to the top of any reports list in which it appears.
14. Enter an appropriate **Report Description**.
15. Select an appropriate **Report Category**.
    Note: This report will be included in the selected **Group by** category on the Manage Reports view.
16. ***If there are any defined custom properties that may apply to this report,*** they are listed in the Custom Properties area. Provide appropriate values for all listed custom properties.
17. Enter any comments appropriate for this report in the **Comments** box. In addition to providing information, you can use this to group reports on the Manage Report page.
18. ***To apply or change limitations for this report,*** expand **Report Limitation**, and then select an appropriate **Report limitation category**.
    Note: Access to web-based reports can be restricted. Users can be assigned specific report limitation categories, and may only view reports that are in these categories.
19. Click **Next** to display the Schedule Report view.

20. ***To schedule this report to be generated, emailed, saved and/or printed at set times:***
    a. Select **Schedule this report to run regularly.**
    b. ***If you have already set up report schedules***, click **Assign Schedule**, and select from the list.
    c. ***If you need to set up a new schedule***, click **Create new schedule**. For more information, see Creating a Report Schedule While Creating or Editing a Report.
21. ***If you do not want to schedule this report***, check **No schedule needed**.
22. Click **Next** to display the Summary view.
23. ***To preview the report***, click **Preview Report**.
24. ***To change any of the settings***, click **Edit** to return to the appropriate page.
25. ***To create and display the report after saving***, click **Show created report after saving**.
26. Click **Submit**.

Creating a New Web-Based Report

While modifying an existing web-based report is often the simplest and the most direct way to create a new report, you can easily create an entirely new web-based report.

To create a new web-based report:

1. Log in to the Orion Web Console.
2. Click **Home > Reports**.
3. Click **Manage Reports**.
4. Click **Create New Report**.
5. Select and add the first resource to be added to the first column of your report. For more information, see Adding Content to a Web-Based Report Column.
6. Click **Select and Continue**. The Layout Builder view is displayed with the selected resource added. You can edit this and add further content later.

7. ***To change the size of your new report,*** either click **Fit to window width** to fit the new report to the current browser window, or enter a new value, in pixels (px), in the **Report width** field.
8. In the Header area, configure your new report as follows:
    a. Enter a **Title** and **Subtitle**.
    b. ***To replace the default logo,*** confirm that **Logo** is checked, and click **Browse for logo** to select your new logo.
9. In the Content area, configure your new report as follows:
    a. Either select the required **Page Layout** from the selector on the right or provide the number of **Layout columns**.
    b. For each column, click **Add Content** to add resources to your report. For more information, see Adding Content to a Web-Based Report Column.
    c. Click **Add section** to add further rows of content to this report.
10. ***To include a footer in your report,*** confirm that **Footer** is checked, and complete the following steps:
    - ***To include the report creation date in the footer,*** confirm that **Creation date** is checked.
    - ***To provide custom text in the footer,*** confirm that **Custom text** is checked, and then provide the custom text you want to include.
11. Click **Next** to display the Preview view.
12. ***If the preview is not how you want your report to be,*** click **Back**, and make the required edits.
13. ***If the report preview is acceptable,*** click **Next** to display the Properties view.
14. ***To store this report as one of your Favorite Reports,*** check **My Favorite Reports**. Marking a report as a favorite promotes it to the top of any reports list in which it appears.
15. Provide an appropriate **Report Description**.
16. Select the appropriate **Report Category**.
    Note: This report will be included in the selected Group by category on the Manage Reports view.

17. ***If there are any defined custom properties that may apply to this report,*** they are listed in the Custom Properties area. Provide appropriate values for all listed custom properties.
    Note: You may leave any custom property field blank, but your SQL database will record the field as 'empty' because SQL does not recognize `NULL` as a valid entry.
18. Enter any comments appropriate for this report in the **Comments** box. In addition to providing information about your report, you can use this to group reports on the initial Report page.
19. ***To apply or change limitations for this report,*** expand **Report Limitation**, and then select an appropriate **Report limitation category**.
    Note: Web-based reports can be restricted to specific users. Users may be assigned specific report limitation categories, and they may only view reports that are in the same report limitation category.
20. Click **Next** to display the Schedule Report view.
21. ***To schedule this report to be generated, emailed, saved and/or printed at set times:***
    a. Select **Schedule this report to run regularly.**
    b. ***If you have already set up report schedules***, click **Assign Schedule**, and select from the list.
    c. ***To set up a new schedule***, click **Create new schedule**. For more information, see Creating a Report Schedule While Creating or Editing a Report.
22. Click **Next** to display the Summary view.
23. ***If you do not want to schedule this report***, check **No schedule needed**.
24. Review the report configuration. Click **Edit** to return to any sections you want to amend or click **Submit** to save the report.

Adding Content to a Web-Based Report Column

You can include any web console resource in your new report, as described below.

Note: The following procedure assumes you are already creating or editing a report in the web console report Layout Builder. For more information, see Creating Reports in the Web Console.

To add content to a web-based report column:

1. On the Layout Builder view, click **Add Content** in the column to which you want to add a new report resource.
2. Select a criterion in the **Group by:** field.

   Note: The **Classic category** grouping provides the most comprehensive list of available resources.

3. Select the resource group from the list in the left pane.
4. Select the resource from the list in the main pane.
5. Click **Select and Continue**.
6. ***If the resource is designated to work only with a specific object or objects***:

   a. Select the required object(s) from the left pane.

   b. To give a specific name to this data source, rather than accepting the default, enter it in the **Selection Name** field.

   c. Click **Add to Layout**.

7. ***If you are an advanced user and want to add a Custom Chart or Table,*** see Adding a Custom Chart or Table to a Web-Based Report Column.
8. Once you have added content to a column, it is displayed with an **Edit Resource** button. Depending on the selected resource, clicking this button will enable you to change the title, subtitle and various other fields and settings.

   Note: For resources and charts that report on a specific object or objects, you can select the object(s) from a drop-down list.

9. If you want to add a further row to your report, click **Add section**. You can now add content to this row as described above.

   Note: Resources can be dragged between columns and sections.

10. Click **Next** to preview the report.

Adding a Custom Chart or Table to a Web-Based Report Column

Advanced users can create custom charts or tables for inclusion in their web-based reports, as described in the following procedure. Because the Orion platform generates such a wealth of data, you need to ensure that you know exactly what data you are using, from which instances it originates from, and what you do with them to ensure that your custom charts and tables show meaningful results.

To add a custom chart or table to a web-based report column:

1. Click **Add Content** in the column to which you want to add a custom chart.
2. Select **Type** in the **Group by:** field.
3. Select **Reports** from the list in the left pane.
4. Select **Custom Chart** or **Custom Table** as required from the list in the main pane, and click **Select and Continue**.
5. Select:
   - **Specific Objects (static selection)** if you know precisely which objects you want to include in your chart or table.
     Note: This is the most straightforward selection method, and recommended for new users. It is also the preferred method for relatively permanent network objects.
   - Select **Dynamic Query Builder** to select objects based on object properties.
     Note: This is the preferred selection method for groups of objects of a specified type that may change over time. "All Cisco nodes in Austin" is an example of a group best defined using the Dynamic Query Builder.
   - Select **Advanced DataBase Query (SQL, SWQL)** only if you are comfortable querying your SolarWinds database directly, using SQL or SWQL.
6. ***If you selected the Specific Objects (static selection) method,*** select objects as shown in the following steps:
   a. Select the object type to chart from the **Show** drop-down.
   b. Select the grouping criterion from the **Group by** drop-down.

c. Expand the groups displayed, if necessary, then check the object(s) to use.

7. ***If you selected the Dynamic Query Builder method,*** define objects as shown in the following steps:

   a. Select the type of selector query you want to use (**Basic** or **Advanced**).

      Note: Though the **Advanced Selector** provides access to all network object characteristics, the **Basic Selector** provides access to a smaller subset of the most frequently used network object characteristics.

   b. ***To use the Basic selector***:

      i. Select the type of objects to report on from the **I want to report on** drop-down.

      ii. Select whether **All child conditions must be satisfied (AND)** or if only **At least one child condition must be satisfied (OR)**.

      iii. Select a property of the monitored object, a conditional relation, and provide a value.

      iv. Click **Add Simple Condition** if you want to add another condition.

   c. ***To use the Advanced Selector***:

      i. Select the type of objects to report on from the **I want to report on** drop-down.

      ii. Select whether **All child conditions must be satisfied (AND)** or if only **At least one child condition must be satisfied (OR)**.

      iii. For each condition you want to add, select the condition type by clicking on the green plus symbol (**+**). You can add a ***Simple Condition*** where you specify a monitored object property, a conditional relationship and a value, an **Advanced Condition** where you select two monitored object properties and a conditional relationship, or a nested **And/Or block**.

8. ***If you selected the Advanced Database Query (SQL. SWQL),*** provide a selection query, as follows:

    a. Select the **Query Type** (**SWQL** or **SQL**).

    Note: For more information about SWQL and SQL queries, click **How to use SWQL / SQL**.

    b. Enter a query, and then click **Preview Results** to confirm that your query provides expected results.

9. In each case enter a name for this selection in the **Selection Name** field if you don't want to use the default name and click **Add to Layout**.
10. You now need to edit the chart or table to specify the data series or columns you want to use and other settings. This is covered in Editing a custom chart and Editing a custom table.

To add additional custom charts or tables:

1. If you add further custom charts or tables, you will be asked if you want to use objects you selected previously or make a new object selection.
    - Click **Use previously specified objects** and select the objects from the drop-down to use the previously selected objects.
    - Click **Create new object selection** and continue from Step 5 above to specify new objects.

To edit a custom chart:

Once you have specified the objects to be reported on for a chart, you need to select the data series to be used.

1. For the custom chart you want to edit, select the time period to be reported on from the **From** drop-down.
2. Click **Edit Chart**.
3. Enter a **Title** and **Subtitle** as required.
4. Click **Add Data Series**.
5. Select the **Object** to report on, then how you to group data pertaining to this object.

Note: The groups available and the data series within these groups will depend on the object selected.

6. Select the **Data Series Name** from the list in the right pane, and click **Add Data Series**.
7. For additional settings for each data series, click **More**. Here you can:
   - Edit the **Display name** for this data series
   - Select a custom **Color** for this data series
   - **Show the 95th percentile line** for this data series
   - **Show Trend** for this data series
8. Repeat steps 4 to 7 to add further data series.
9. Enter a **Custom label** for the Left axis.
10. Select the **Units displayed**, and **Chart** type, and check the **Show the sum of all data series**, if required.
11. Select the **Sample Interval**. This can be from once a minute to once a week. Data within each sample interval is summarized so that a single point or bar is plotted for each of these periods. **Note:** It is possible to select a sample interval that is longer than the reporting period.
12. ***To filter the data used in the chart:***
    a. Either:
       - Select **Show only limited number of top records** and enter how many of the top records to be used.
       - Select **Show only limited % of top records** and enter the top percentage of the top records to be used.
    b. Select how you want to sort this selection of records from the **Sort records by** drop-down. The choices shown here will depend on the data series selected.
    c. Select either **Ascending** or **Descending** from the **Sort order** drop-down.
    d. Select the **Data aggregation** method required.
    e. Click **Advanced** if you want to sort records using a secondary field.

13. You can set up additional data series using the right axis. This allows you to superimpose two charts using different labels, units, and chart type.

    Note: You cannot use a separate time period or filter results settings for the right axis series.

14. Click **Submit** to return to the Add Report page.

To edit a custom table:

Once you have specified the objects to be reported on for a table, you need to select the data series to be used.

1. For the custom table you want to edit, select the time period to be reported on from the **From** drop-down.
2. Click **Edit Table**.
3. Enter a **Title** and **Subtitle** as required.
4. Click **Add Column**.
5. Select the **Object** to report on, then how you want to group data pertaining to this object.

   Note: The groups available and the data series within these groups will depend on the object selected.

6. Select the **Database column names** from the list in the right pane, and click **Add Column**.
7. For additional settings for a column, click **Advanced**. Here you can:
   - Edit the **Display name** for this column.
   - Check **Hide this column in the resulting table**, if you want to use this column when querying the database but do not want to show it. For example, you may want to use this column's data in the time-based settings but not show the data in the table.
   - Check **Allow HTML tags**, if you want to use any HTML tags retrieved from the database for this column.

- Select the **Display settings** to be used for this column. This applies the selected formatting to the data in this column. The applicability of the formatting depends on the data. For example, if the column is Last Boot, you can show the date of the last boot or how many days ago it was. Similarly, if the column is Vendor and the display setting is Vendor icon, the vendor name will be replaced by the vendor logo, if available.
- Select the **Data aggregation** method to use for this column, if you want to summarize your data by time period.
- Select the **Alignment** for this data. This can be left, right or center.

8. To add further columns, click on the green plus sign in the table layout section, and repeat steps 5 to 7.
9. ***To restrict data in your table to a specific time period***, select **Yes** from the **Time-based settings** drop-down.

   Note: You can only do this if your table contains a column with historical data.

   a. Select the column to use to specify the time period from the **Date/Time column in this table is** drop-down.
   b. Select the **Sample Interval**. This is used to summarize your data by time period.
10. To sort results in your table:

    a. Select the column you want to sort by from the **Sort results by** drop-down.
    b. Select how you want to sort the column. This can be **Ascending** or **Descending**.

       Note: You can sort further, using the remaining columns in the same way.
11. To group results in your table:

    a. Select the column you want to sort by from the **Group results by** drop-down.

Note: You can group further, using the remaining columns in the same way.

12. To filter the results in your table, either:
13. Select **Show only the top __ records** and enter the number of records to show
14. Select **Show only the top __ % of records** and add the percentage of records to show
15. Click **Submit** to return to the Add Report page.

Scheduling Reports

Schedules enable you to set up report actions to occur at specific times. These actions let you generate reports and print them, save them to disk or email them to selected recipients. You can create schedules for single or multiple reports or assign reports to existing schedules. In addition, you can add URLs to the schedules, so that screen captures of specific websites at the time the reports were generated are included.

- Reports can be assigned to schedules either when they are being edited or created, or in the Schedule Manager.
- Schedules can be created from the Report Manager, the Schedule Manager or from within the creation or editing of a report.

Creating a Report Schedule While Creating or Editing a Report

You can directly assign a report to a schedule while editing the report.

To create a new schedule while creating or editing a report:

1. Click on the **Schedule Report** tab to display the Schedule Report view.
2. Click **Schedule this report to run regularly**.
3. Click **Create new schedule** in the dropdown.
4. Enter an appropriate **Schedule Name** and **Description**.

5. Click **Add Frequency** and then complete the following steps:
    a. Enter a name for this frequency.
    b. Select:
        - **Specific Date(s)** to select specific dates and times
        - **Daily** to schedule the report actions to run every day
        - **Weekly** to schedule the report actions to run once or more a week
        - **Monthly** to select the month and the day of the month to run the report actions.
    c. ***If you selected Specific Date(s),*** select the date(s) and time(s) when you want the scheduled report actions to occur and then click **Add Frequency**.

        Note: Click **Add Time** to select additional dates and times.
    d. ***If you selected Daily,*** complete the following steps:
        i. Select the number of days between scheduled report actions.

            Note: to run the report on work days, select **Business Day (Mon - Fri)**.
        ii. Select the time(s) to run your report actions.

            Note: Click **Add Time** to add additional dates and times.
        iii. ***If you do not want the schedule to start immediately upon completion,*** select **Specific Date(s)** in the **Starting On** field, and then select the date and time when you want the schedule to start.
        iv. ***If you want the schedule to end at some point,*** check **Ending On**, and then select the date and time when you want the schedule to end.
        v. Click **Add Frequency**.
    e. ***If you selected Weekly,*** complete the following steps:

i. Check the days of the week to run the report actions.

ii. Select the time(s). You can click **Add Time** to add additional dates and times.

iii. ***If you do not want the schedule to start immediately upon completion,*** select **Specific Date(s)** in the **Starting On** field, and then select the date and time to start.

iv. ***If you want the schedule to end at some point,*** check **Ending On**, and then select the date and time for it to end.

v. Click **Add Frequency**. You can add multiple frequencies, if required.

f. ***If you selected Monthly,*** complete the following steps:

i. Select the months, days and times when you want to run your report actions.

Note: Click **Add Time** to add additional dates and times.

ii. ***If you do not want the schedule to start immediately upon completion,*** select **Specific Date(s)** in the **Starting On** field, and then select the date and time when you want the report schedule to start.

iii. ***If you want the schedule to end at some point,*** check **Ending On**, and then select the date and time when you want the report schedule to end.

iv. Click **Add Frequency**.

6. Click **Add Action**, and select the action (**Email**, **Print**, or **Save** to **Disk**) to be executed on the configured schedule, and then click **Configure Action**.
7. Enter a **Name** for the action.
8. ***If you selected Email:***

a. In the **To** field, enter the email addresses of all recipients, separated by semicolons.

b. If you need to add CC or BCC addresses, click **CC** and/or **BCC**, and enter the email addresses of these recipients.

c. ***To change the default name and address of the sender***, click "-" and enter the appropriate **Name of Sender** and **Reply Address**.

d. Click **Message**, and enter the **Subject** and **Message** for the email. You can compose the message as **HTML** or **Plain Text**.

e. ***If you also want a printable version of your emailed reports***, check **Retrieve a Printable Version of Reports**.

f. Check the format(s) in which you want to provide the emailed report: **PDF**, **CSV**, **Excel**, or **HTML**.

g. ***To include the URL of the emailed report so recipients can access it remotely***, check **Include Report's URL**

h. Click **SMTP Server**.

i. If you have already configured an SMTP server, select the **Name of SMTP Server**, and then click **Save**.

j. ***If you have not already configured an SMTP server***, select **Add New Server**, and then complete the following steps:

   i. Provide the **Hostname or IP Address** of your SMTP Server and the designated **SMTP Port Number**.

      Note: The SMTP server hostname or IP address field is required. You cannot send an email without identifying the SMTP server.

   ii. ***If you want to use SSL encryption for your emailed report,*** check **Use SSL**. This changes the SMTP port number to 465.

   iii. ***If your SMTP server requires authentication***, check **This SMTP Server requires Authentication**, and then provide requested credentials.

k. Click **Add Action**.

9. ***If you selected Print:***

   a. Provide a Windows User name, using `domain\username` format, and **Password** for a user with access to the printer on which you want to print your report.

   b. Click **Printer Settings**.

c. Click **Select**, and then select the printer to which you want to send the report.

d. Click **Select.**

e. Enter the number of **Copies**, the **Layout**, whether you want **Color** or **Black and white** printing, and the **Margins** to be applied.

f. Click **Add Action**.

10. ***If you selected Save to Disk***:

a. Enter the **Network Share Location** where you want to save the report.

b. If you also want a printable version of your saved report, check **Retrieve a Printable Version of Reports**.

c. Enter the Windows **User name**, using `domain\username` format, and **Password** for a user with access to the Network Share Location.

d. Select the format(s) in which you want to provide the saved report (**PDF**, **CSV**, or **Excel**).

e. Click **Add Action**. You can add multiple actions.

Creating, Assigning and Editing Report Schedules in Report Manager

The section contains procedures for the following scheduling tasks:

- Creating a new schedule
- Editing a schedule
- Assigning a report to a schedule
- Unassigning a report from a schedule

To create a new schedule from the Manage Report page:

1. Select the report for which you want to set up a schedule.
2. Click on **Schedule Report > Create New Schedule** to display the Properties view.
3. Enter an appropriate **Schedule Name** and **Description of Report Schedule**.

4. ***To add addition reports to this schedule,*** click **Assign another Report**, select the report(s) to be included in this schedule, and click **Assign Report (s)**.
5. ***To assign webpages to this schedule***, so that a snapshot of the selected website is included with the reports, click **Assign Webpage** and enter the URL in the field displayed. You can assign multiple webpages. Remember to start each with `http://` or `https://` as appropriate.
6. ***To specify a user account so that its limitations are applied to this schedule***, expand **Advanced Settings**, click **Another User** and enter the **User name or Account ID** and **Password**.
7. Click **Next** to display the **Frequency** view.
8. Click **Add Frequency** and then complete the following steps:
    a. Enter a name for this frequency.
    b. Select:
        - **Specific Date(s)** to select specific dates and times
        - **Daily** to schedule the report actions every day
        - **Weekly** to schedule the report actions once or more a week
        - **Monthly** if you want to select the month and the day of the month to schedule the report actions.
    c. ***If you selected Specific Date(s),*** select the date(s) and time(s) when you want the scheduled report actions to occur and click **Add Frequency**.

        Note: Click **Add Time** to select additional dates and times.

    d. ***If you selected Daily,*** complete the following steps:
        i. Select the number of days between scheduled report actions.

            Note: To run the report on work days, select **Business Day (Mon - Fri)**.

        ii. Select the time(s) to run your report actions.

            Note: Click **Add Time** to add additional dates and times.

iii. ***If you do not want the schedule to start immediately upon completion,*** select **Specific Date(s)** in the **Starting On** field, and select the date and time when you want the schedule to start.

iv. ***If you want the schedule to end at some point,*** check **Ending On**, and select the date and time when you want the schedule to end.

v. Click **Add Frequency**.

e. ***If you selected Weekly,*** complete the following steps:

i. Check the days of the week to run the report actions.

ii. Select the time(s). You can click **Add Time** to add additional dates and times.

iii. ***If you do not want the schedule to start immediately upon completion,*** select **Specific Date(s)** in the **Starting On** field, and then select the date and time to start.

iv. ***If you want the schedule to end at some point,*** check **Ending On**, and then select the date and time for it to end.

v. Click **Add Frequency**. You can add multiple frequencies, if required.

f. ***If you selected Monthly,*** complete the following steps:

i. Select the months, days of the month and times at which you want to run this schedule.

Note: Click **Add Time** to add additional dates and times.

ii. ***If you do not want the schedule to start immediately,*** select **Specific Date(s)** in the **Starting On** field, and then select the date and time when you want the report schedule to start.

iii. ***To set an end date and time for the schedule,*** check **Ending On**, and then select the date and time when you want the report schedule to end.

iv. Click **Add Frequency**.

9. Click **Next** to display the Actions view.

10. Click **Add Action**, and select the action (**Email**, **Print,** or **Save to Disk**) to be executed on the configured schedule, and then click **Configure Action**.
11. Enter a **Name** for the action.
12. ***If you selected Email:***
    a. In the **To** field, enter the email addresses of all recipients, separated by semicolons.
    b. ***To add CC or BCC addresses***, click **CC** and/or **BCC**, and enter the email addresses of these recipients.
    c. ***To change the default name and address of the sender***, click "-" and enter the appropriate **Name of Sender** and **Reply Address**.
    d. Click **Message**, and enter the **Subject** and **Message** for the email. You can compose the message as **HTML** or **Plain Text**.
    e. ***If you also want a printable version of your emailed reports***, check **Retrieve a Printable Version of Reports**.
    f. Check the format(s) in which you want to provide the emailed report: **PDF**, **CSV**, **Excel**, or **HTML**.
    g. ***To include the URL of the emailed report so the recipients can access it remotely***, check **Include Report's URL**.
    h. Click **SMTP Server**.
    i. ***If you have already configured an SMTP server***, select the **Name of SMTP Server**, and click **Save**.

j. ***If you have not already configured an SMTP server***, select **Add New Server**, and complete the following steps:

i. Provide the **Hostname or IP Address** of your SMTP Server and the designated **SMTP Port Number**.

Note: The SMTP server hostname or IP address field is required. You cannot send an email without identifying the SMTP server.

ii. ***To use SSL encryption for your emailed report,*** check **Use SSL**. This changes the SMTP port number to 465.

iii. ***If your SMTP server requires authentication***, check **This SMTP Server requires Authentication**, and provide requested credentials.

k. Click **Add Action**.

13. ***If you selected Print:***

a. Provide a **Windows User** name, using `domain\username` format, and **Password** for a user with access to the printer on which you want to print your report.

b. Click **Printer Settings**.

c. Click **Select**, and then select the printer to which you want to send the report.

d. Click **Select.**

e. Enter the number of **Copies**, the **Layout**, whether you want **Color** or **Black and white** printing, and the **Margins** to be applied.

f. Click **Add Action**.

14. ***If you selected Save to Disk***:

a. Enter the **Network Share Location** where you want to save the report.

b. If you also want a printable version of your saved report, check **Retrieve a Printable Version of Reports**.

c. Enter the Windows **User name**, using `domain\username` format, and **Password** for a user with access to the Network Share Location.

d. Select the format(s) in which you want to provide the saved report (**PDF**, **CSV**, or **Excel**).

e. Click **Add Action**. You can add multiple actions.

15. Click **Next** to display the Summary view.
16. ***If the schedule summary is correct***, click **Create Schedule**.
17. The schedule is display in the Schedule Manager.

To edit a schedule

1. Click the **Schedule Manager** tab.
2. Select the schedule you want to edit and click **Edit Schedule**.
3. The Properties view for the schedule is displayed.

To assign a report to a schedule or multiple schedules

1. Select the report you want to assign.
2. Click **Schedule Report > Assign Existing Schedule.**
3. Confirm that you want to assign the report by selecting the schedule or schedules in the **Assign existing schedule** list and clicking **Assign Schedule(s)**.

To unassign a report from a schedule or multiple schedules

1. Select the report you want to unassign.
2. Click **Schedule Report > Unassign Schedule.**
3. Confirm that you want to remove the report by selecting the schedule or schedules in the **Unassign schedule from report** list and clicking **Unassign Schedule(s)**.

The Report Scheduler

The Report Scheduler provides a list of all report schedules that have been set up for your Orion web-based reports. You can create, edit, run and delete schedules from this page, and assign reports to schedules.

1. Log in to the Orion Web Console.
2. Click **Home > Reports**.
3. Click **Manage Reports** in the upper right.
4. Click the **Schedule Manager** tab.
5. ***To create a schedule***, click **Create New Schedule**. The Add Report Schedule page is displayed. For more information, see Creating, Assigning and Editing Report Schedules in Report Manager.
6. ***To edit a schedule***, select the schedule and click **Edit Schedule**. The Edit Report Schedule page is displayed. For more information, see Creating, Assigning and Editing Report Schedules in Report Manager.
7. ***To run a schedule immediately***, select the schedule and click **Run Now**. The selected schedule is run.
8. ***To delete a schedule***, select the schedule and click **Delete**. You are asked to confirm that you want to delete the schedule.
9. ***To assign a report or reports to a schedule***, select the schedule and click **Assign to a Report**. Select the report(s) to be assigned to this schedule and click **Assign Report(s).**

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.

Important: This functionality is replaced by web-based reports, though legacy reports must be edited in 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:
   Note: You can toggle between Preview and Report Designer modes at any time by clicking **Preview** or **Design**, respectively, on the toolbar.
   - **Preview** displays the report as it will appear in printed form. For more information, see Preview Mode.
   - **Report Designer** is the report creation and editing interface. For more information, see Design Mode.
4. ***If you want to separate the data for individual network objects with horizontal lines,*** click **Report Style**, and then check **Display horizontal lines between each row.**
5. Click **OK** to exit Report Writer Settings.

For more information about creating reports in Report Writer, see Creating and Modifying Reports in Report Writer.

Viewing Reports in the Report Writer

The following procedure opens reports for viewing in the Orion Report Writer.

To view reports with Orion Report Writer:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Report Writer**.
2. 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**.

Design Mode

Use Design mode to create new reports and modify or rename existing reports. The options available for 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. The options available depend on the type of report being designed, but all reports require that you select the data to include and decide how that data will be sorted, ordered, filtered, and presented.

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

Creating and Modifying Reports in Report Writer

Use the following procedure to modify or create reports in Report Writer.

To open a report with Report Writer:

1. ***To modify an existing report,*** click an existing report from the inventory in the left pane of the main Report Writer window.
2. ***To create a new report,*** click **File > New Report**.
3. 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.

See the following documents for more information about configuring reports in Report Writer:

- General Options Tab
- Select Fields Options Tab

- Filter Results Options Tab
- Top XX Records Options Tab
- Time Frame Options Tab
- Summarization Options Tab

General Options Tab

The General tab is displayed by default, showing 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. Customizing Views.

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: Unchecked 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. Filters are configured as follows.

To configure filters:

1. Click **Browse** (**…**), and then select from the following options:
   - Select **Add a new elementary condition** to generate a condition 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.
2. Check or clear individual filter conditions to enable or disable their application, respectively, to your report.

Top XX Records Options Tab

You can limit the number of records shown in your report to either a top number or a top percentage of all results. Top XX options are configured as shown below.

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

You can 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

You can generate summaries of your results over specific periods of time using the Summarization tab.

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.
    - Check **Transparent Background** for better results when publishing your report to the Web.
4. ***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.
- Check **Hidden Field** to hide any field in your report.
- To view your changes at any time, click **Preview**.

Creating a Scheduled Report Job

The following procedure creates a scheduled report job for regularly printed or emailed reports.

To schedule a report:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Click **Reports**, and then lick **+** as required to locate the report you want to schedule.
3. Click the name of the report you want to schedule, and then copy the URL of the report you want to schedule.
4. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Orion Report Scheduler**.
5. Click **Edit > Add New Job**.
6. Provide a job name for this scheduled report, and then click **Continue**.
7. Paste the URL of the report you want to schedule into the link field.
8. ***If you need to provide Windows login credentials to view the report you are scheduling,*** click the NT Account login tab, and then provide the user account details needed to log in.
9. ***If you want to create a printable report that excludes the Orion Web Console banner and menu bar,*** on the Orion Web Login tab, check **Retrieve a Printable Version of this Page**.
10. ***If the report you are scheduling requires an Orion user account,*** on the Orion Web Login tab, check **Send Orion Username / Password in URL**, and then provide the required user credentials to view the Orion report.
11. Click **Continue**.
12. Configure the scheduling for your report job, and then click **Continue**.

13. ***If you want to email the report,*** complete the following procedure:
    a. Confirm that either **Email the Web Page (as HTML)** or **Email the Web Page (as PDF)** are selected, and then click **Continue**.
    b. Provide required email addresses and a subject in the appropriate fields on the Email To tab.
    c. Provide a name and reply address on the Email From tab.
    d. On the SMTP Server tab, type the hostname or IP address and confirm the port number of the server used to send email from the Orion server.
    e. Click **Continue**.
14. ***If you want to print the report,*** complete the following steps:
    a. Select **Print the Web Page**, and then click **Continue**.
    b. Select the Printer, Orientation, and number of Copies you want to print.
    c. Click **Continue**.
15. Enter the user name and password for the Windows account that will email the report.
16. Click **Continue**.
17. Add any additional comments or notes about this job, and then click **Finish**.

Reports and Account Limitations

SolarWinds reports respect Orion Web Console account limitations. For security, by default, reports are not available to users with limited accounts unless an Orion administrator specifically provides access. The following procedure creates a reports folder for an account-limited user and configures the account-limited user to access Orion reports from it.

Note: For more information about creating user accounts, Creating New Accounts. For more information about applying account limitations to user accounts, Setting Account Limitations.

To allow account-limited users access to reports:

1. Open the Orion Reports folder.

   Note: All reports created or predefined in Orion Report Writer are, by default, stored, in **C:\Program Files\Solarwinds\Orion\Reports**.

2. Create a new folder using the name of the account-limited user.
3. Copy the reports you want the account-limited user to see from the Orion Reports folder into the new, account-limited user folder.
4. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
5. Log in to the Orion Web Console as an administrator.
6. Click **Settings** in the top right of the web console.
7. Click **Manage Accounts** in the Accounts grouping of the Orion Website Administration page.
8. Select the account-limited user, and then click **Edit**.
9. In the Default Menu Bar and Views section, select the **Report Folder** you created in the Orion Reports folder for the account-limited user.
10. Click **Submit**.

Exporting and Importing Reports

You can export reports in several formats from both the Orion Web Console and the Orion Report Writer. You can also import reports, previously exported as XML files, back into the Orion Web Console.

Exporting Reports

The most appropriate format for exporting a report depends on how you want to use the exported file. The different formats, in which Orion reports can be exported, are shown below.

	Orion Web Console	Orion Report Writer
XML	✔	
Excel	✔	✔
PDF	✔	✔
HTML and MHTML		✔
Image (BMP, GIF, JPG, PNG, etc.)		✔

Exporting Reports as Excel and PDF from the Orion Web Console

The most common formats for exporting reports have their own icons on the Orion Web Console's report page. You can view and edit Excel files as spreadsheets. You can create read-only files using the PDF export that retain the exact formatting used in the original report.

To export a report as Excel or PDF:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. On the **Home** tab, click **Reports**.
3. Click on **Manage Reports** in the upper right corner.
4. Click on the required report.
5. Click on either **Export as Excel** or **Export as PDF**, as appropriate.

Note: The **Export to Excel** button is only displayed if the report contains only custom table resources. Other resources cannot be converted to the Excel format.

Exporting Reports from the Orion Report Writer

The Orion Report Writer provides an export menu that enables you to save you report in all formats listed above except XML. To export to XML, you need to use the Solarwinds Orion Web Console.

To export a report from the Orion Report Writer:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting and Mapping > Orion Report Writer**.
2. Click on the report you want to export.
3. Click **File > Export**.
4. Click on the required file format.
5. Type a name for the exported file.
6. Click **Save**.

Exporting and Importing Reports as XML

You can save reports from the Orion Web Console in XML form and import them back if needed.

To export a report as XML:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. On the **Home** tab, click **Reports**.
3. Click on **Manage Reports** in the upper right corner.
4. Click on the **Type** column header, to display the web-based reports first.
5. Click on the required report, then click on **Export/Import**, and then click **Export Report**.
6. Click **Open** or **Save**, depending whether you want to view or save the report.

Note: You may be asked to supply the name of the program you want to use to view XML files.

To import an XML file using the Orion Web Console Writer:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. On the **Home** tab, click **Reports**.
3. Click on **Manage Reports** in the upper right corner.
4. Click on the **Type** column header, to display the web-based reports first.
5. Click on **Export/Import**, and then click **Import Report**.
6. Navigate to the required XML file, and then click **Open**.
7. The file will be imported and its name displayed at the top of the list of reports.
8. Note that if you import a report with the same name as an existing report, it will be prefixed with “Copy of”.

Chapter 20: Monitoring Syslog Messages

Syslog messages are one type of real-time notification that network devices can send in response to designated network events. Orion provides the SolarWinds Syslog Service, allowing Orion to receive Syslog messages from any monitored network device. The SolarWinds Syslog Service also has the ability to open multiple connections to your SQL server, so it can handle large numbers of simultaneously incoming Syslog messages from all your monitored devices.

Orion uses the SolarWinds Syslog Service to listen on UDP port 514 for incoming Syslog messages. Received messages are then decoded and stored in the Orion database. Until they are acknowledged, Syslog messages are available for viewing either in the web console Syslog view or in the Syslog Viewer application. The Syslog view in the Orion Web Console provides quick access to current messages, filtered by any or all of the following criteria:

- Name or type of network object sending the message.
- Message Severity, Facility, Type, or Pattern
- Time Period in which the message was sent.

The Syslog Viewer application also allows you to tailor your view of Syslog messages using fully customizable rules. Additionally, the Syslog Viewer gives you the ability both to search your Orion database and to configure Syslog-specific alerts for received Syslog messages.

Notes:

- When configuring your network devices to send Syslog messages, confirm that messages are sent to the IP address assigned to your Orion server. To ensure the proper configuration of a network device for Syslog messaging, refer to the documentation supplied by the device vendor.

- As a benchmark, a typical SolarWinds installation can process approximately 1 million Syslog messages per hour, which is equivalent to about 300 Syslog messages per second. Higher capacity can only be achieved with significant hardware improvements over minimum SolarWinds requirements.

Configuring the Orion Syslog Port

Orion listens for Syslog messages on port 514 (UDP). You can configure this port in the **SyslogService.exe.config** file, as indicated in the following procedure.
Note: Running the Configuration Wizard will revert any and all changes made to the **SyslogService.exe.config** file. If you run the Configuration Wizard, you must repeat this procedure to restore your required port setting.

To configure the Syslog port:

1. Log on to your Orion server using an account with administrative privileges.
2. Open **SyslogService.exe.config** in a text editor.
   Note: By default, **SyslogService.exe.config** is located in **C:\Program Files\SolarWinds\Orion\Orion\SyslogService**.
3. Locate the following line:

   <add key="UDPListenPort" value="514">
4. Edit **value="514"** as required to indicate the port on which your monitored devices are configured to send Syslog messages to your Orion server.
5. Save **SyslogService.exe.config**.

Syslog Messages in the Web Console

The Orion Web Console provides both Syslog-specific resources and a Syslog view that provides a table of Syslog messages received by your Orion server. The following sections provide an overview of available Syslog resources and procedures for viewing and acknowledging Syslog messages within the Orion Web Console.

Syslog Resources

NPM provides the following Syslog-related resources for inclusion within web console views.

Advanced Syslog Counts

Every Syslog message has a designated severity. For more information about Syslog severities, see Syslog Severities. The Advanced Syslog Counts resource groups by severity all Syslog messages received by the currently viewed node. For each severity, this resource provides the number of received Syslog messages.

Advanced Syslog Parser

The Advanced Syslog Parser resource provides a comprehensive view of the Syslog messages most recently received by the viewed node. The most recent messages of each severity are listed. For more information about Syslog severities, see Syslog Severities.

Advanced Syslog Summary

The Advanced Syslog Summary resource groups by message type all Syslog messages received by the currently viewed node, where the message type is encoded in the Syslog message packet. For each message type, this resource provides the severity, the hostname or IP address of the message originator, and the total number of Syslog messages received.

Last 25 Syslog Messages

The Last 25 Syslog Messages resource provides a list of the last 25 Syslog messages that have been sent by monitored network devices to the viewed node. For each message, this resource presents the date and time the message was sent, the hostname and IP address of the device sending the message, and the message text.

Clicking the hostname, IP address, or message text opens the corresponding Object Details page, providing extensive diagnostic information about the monitored network object sending the message.

Clicking **Edit** opens the Edit Last 25 Syslog Messages page where you can set the maximum number of displayed messages, select the time period for viewing messages, and establish filters to limit the messages this resource displays. For more information, see Using Node Filters.

Syslog Summary

The Syslog Summary resource lists the number of Syslog messages received by the viewed node from monitored network devices over a specified period of time.

Viewing Syslog Messages in the Web Console

You can customize the list view by using the following procedure to select your preferred message grouping criteria.

To view Syslog messages in the Web Console:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Log in to the Orion Web Console, and then click **Syslog** in the Views toolbar.
3. ***If you want to view Syslog messages for a specific Syslog enabled network object,*** specify the selected object in the Network Object field.
   Note: Only objects that have sent a Syslog message to the Orion server will be listed in this field.
4. ***If you want to filter your Syslog messages table by device type,*** select the type to which you want to limit your view in the **Type of Device** field.
5. ***If you want to filter your Syslog messages table by severity,*** select the severity level to which you want to limit your view in the **Select Severity** field.
   Note: For more information, see Syslog Severities.
6. ***If you want to filter your Syslog messages table by facility,*** select the facility to which you want to limit your view in the **Select Facility** field.
   Note: For more information, see Syslog Facilities.

7. ***If you want to limit your Syslog messages table to show only messages of a designated type,*** type the appropriate string in the **Message Type** field.
8. ***If you want to limit your Syslog messages table to show only messages containing a designated pattern,*** provide the appropriate string in the **Message Pattern** field.
   Note: An asterisk (*) is required as a wildcard character, both before and after the pattern string, unless the provided pattern is the beginning of the message, the end of the message, or the full message.
9. ***If you only want to see Syslog messages from a specific period of time,*** select a time period from the **Time Period** menu.
10. Confirm the number of messages displayed in the **Show Messages** field.
11. ***If you want cleared or acknowledged messages to remain in the Syslog view,*** check **Show Cleared Messages**.
12. Click **Refresh** to update the Syslog messages list with your new settings.

Acknowledging Syslog Messages in the Web Console

Acknowledging Syslog messages is straightforward in the Orion Web Console, as shown in the following procedure.

To acknowledge Syslog messages in the Orion Web Console:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Log in to the Orion Web Console.
3. Click **Syslog** in the Views toolbar.
4. Provide filter criteria for the Syslog messages table. For more information, see Viewing Syslog Messages in the Web Console.
5. Click **Refresh** to ensure that all selected view criteria take effect.
6. Check the messages you want to acknowledge, and then click **Clear Selected Messages**.

Using the Syslog Viewer

Orion also provides the standalone Syslog Viewer application for viewing and acknowledging Syslog messages on your network. Syslog Viewer 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 using the Syslog Viewer application for viewing, acknowledging, and triggering alerts in response to Syslog messages on your network.

To open the Syslog Viewer, click **Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Syslog Viewer**.

Viewing and Acknowledging Current Messages

The 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 using either of the following methods:
    - Right-click any message, and then select **Acknowledge Selected**.
    - Add an **Acknowledged** column to the Syslog Viewer, and then check each message that you want to acknowledge. For more information, see Syslog Server Settings.

Searching for Syslog Messages

Collected Syslog messages may be searched within Syslog Viewer. The following steps both search for Syslog messages and format search results.

To search the Syslog message list:

1. Click **View > Search Messages**.
2. Enter appropriate search criteria.
3. Click **Search Database**.

4. ***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 Syslog Server Settings.
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**.

Syslog Server Settings

Use the following procedure as a guide to starting and configuring the Syslog Viewer.

To start and configure the Syslog Viewer:

1. Click **Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Syslog Viewer**.
2. Click **File > Settings**.
3. Click the General tab in the Syslog Server Settings window.
4. Adjust the **Maximum number of messages to display in Current Messages view** slider to set the number of messages you want to display.
5. ***If you want to Automatically Refresh the Current Messages View,*** check the option accordingly, and then set the refresh rate with the middle slider.
6. Adjust **Retain Syslog messages for how many days?** to set the length of time Syslog messages should stay in the database.
7. Click the Displayed Columns tab.
8. Use the arrow keys to select and order the fields of information you want to see in the Current Messages view.
   Note: You can make it easier to acknowledge Syslog messages by selecting the **Acknowledged** column to add to your view.

9. ***If you want to wrap Syslog message text in the Current Messages view,*** check **Word wrap long messages**.
10. ***If you do not expect to use Syslog Server as your primary viewer for Syslog messages,*** select the Message Parsing tab, and then check the following options:
    - **Remove embedded Date/Time from Syslog Messages**
    - **Remove Message Type from Syslog Messages**
    - **Remove Domain Name from DNS Lookups**.

    Note: The following data points are saved within the Syslog tables in your Orion database. Removing the added data from each record helps you to proactively reduce the size of your database.

Configuring Syslog Viewer Filters and Alerts

The Syslog Viewer can be configured to signal Orion 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.
Note: Syslog rules may not be applied to nodes in an unmanaged state.

To configure Syslog Viewer filters and alerts:

1. Click **Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Syslog Viewer**.
2. Click **File > Settings**.
3. Click **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 Selected Rule**.
6. On the General tab, complete the following steps:
    a. Provide or edit the **Rule Name**.
    b. Check **Enabled**.
    c. Select appropriate servers from the **Apply this Rule to** list.

d. Enter the IP addresses or subnets to which this rule applies in the Source IP Addresses area.
Note: Use the examples provided on this tab to ensure that the list of source IP addresses is properly formatted.

7. ***If you want to limit the rule to only messages from specific hosts, domains, or hostname patterns,*** on the DNS Hostname tab enter a DNS Hostname Pattern.

   Notes:

   - The DNS Hostname Pattern rule is case-sensitive.
   - When **Use Regular Expressions in this Rule** is checked, you may use regular expressions in place of "like" statements. For more information about using regular expressions in NPM, see Regular Expression Pattern Matching.

8. ***If you want to limit the rule to only specific message types or text within a Syslog message,*** on the Message tab enter rules as appropriate for **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 checked, regular expressions can be used in place of "like" statements. For more information about using regular expressions in NPM, see Regular Expression Pattern Matching.

9. ***If you want to apply specific severity or facility types,*** on the Severity / Facility tab check the severity and facility types you want to apply.
Note: By default, all message severities and facilities are selected. For more information about Syslog severities and facilities, see Syslog Message Priorities.

10. ***If you want to limit rule application to within a specific period of time,*** select the Time of Day tab, check **Enable Time of Day checking**, enter the time period, and then check the 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.

11. ***If you want to suppress alert actions until a specified number of messages arrive that match the rule,*** complete the following procedure:
    Note: When **Suspend further Alert Actions for** is checked, 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.

    a. Select the Trigger Threshold tab, and then check **Define a Trigger Threshold for this Rule**.

    b. Enter option values as appropriate.

12. Configure Syslog alert actions on the Alert Actions tab, as shown in the following steps:

    a. ***If you are associating a new action to the rule,*** click **Add New Action**. For more information about available actions, see Available Syslog Alert Actions.

    b. ***If you want to edit an existing action for the rule,*** select an action from the list, and then click **Edit Selected Action**.

    c. Configure the action as appropriate. For more information about available actions, see Available Syslog Alert Actions.
    Note: Syslog alerts use a unique set of variables. For more information about available Syslog variables, see Syslog Alert Variables.

    d. ***If you need to delete an action,*** select the action, and then click **Delete Action**.

    e. Use the arrow buttons to set the order in which actions are performed.
    Note: Actions are processed in the order listed, from top to bottom.

    f. Click **OK** to save all changes and return to Syslog Viewer Settings.

13. 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.

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

Modify the severity, facility, type, or 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

Write a message to local or remote Windows Event Logs.

Forward the Syslog message

Specify the IP address or hostname and the port to forward a Syslog event.

Send a new Syslog message

Trigger a new Syslog message, sent to a specific IP address or hostname, on a specific port, with a customizable severity, facility, and message.

Send an SNMP Trap

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

Define the speech engine, speed, pitch, volume, and message to read.

Execute an external program

Allows you to specify an external program to launch using a batch file. This action is used when creating realtime change notifications in Orion.

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 either to a specific computer or to an entire domain or workgroup.

Note: The only operating systems supporting Windows Net Messaging on which SolarWinds supports Orion installations are Windows Server 2003 and Windows XP. SolarWinds only supports evaluation installations of Orion on Windows XP.

Send an E-mail / Page

Send an email from a specified account to a specified address, using a specific SMTP server, and containing a customizable subject and message.

Stop Processing Syslog Rules

Stops the processing of Syslog rules for the matching Syslog message.

Forwarding Syslog Messages

The Syslog message forwarding action allows you to forward received Syslog messages. Additionally, if you have WinPCap version 3.0 or higher installed on your NPM server, you can forward Syslog messages as spoofed network packets.

The following procedure configures available options for forwarded Syslog messages.

Note: The following procedure assumes you are editing a Forward the Syslog Message alert action. For more information about Syslog alert actions, see Configuring Syslog Viewer Filters and Alerts.

To configure the forward syslog message action:

1. Provide the hostname or IP address of the destination to which you want to forward the received Syslog message.

2. Provide the **UDP Port** you are using for Syslog messaging.
   Note: The default is UDP port **514**.
3. ***If you want to retain the IP address of the source device,*** complete the following steps:
   a. Check **Retain the original source address of the message**.
   b. ***If you want to designate a specific IP address or hostname as the Syslog source,*** check **Use a fixed source IP address (or hostname)**, and then provide the source IP address or hostname.
   c. ***If you want to spoof a network packet,*** check **Spoof Network Packet**, and then select an appropriate **Network Adapter**.
4. Click **OK** to complete the configuration of your Syslog forwarding action.

Syslog Alert Variables

The following variables can be used in Syslog alert messages. Each variable must begin with a dollar sign and be enclosed in curly braces as, for example, **${**VariableName**}**. Syslog alerts also support the use of Node alert variables. For more information on the use of variables, see Orion Variables and Examples.

Syslog Date/Time Variables

Syslog Date/Time Variable	Description
${AbbreviatedDOW}	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 â€œShort Dateâ€ and â€œShort Timeâ€ 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.

Syslog Date/Time Variable	Description
${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
${Hostname}	Host name of the device triggering the alert
${IP_Address}	IP address of device triggering alert

Syslog Variable	Description
${Message}	Status of device triggering alert
${MessageType}	The name of the triggered alert

${Severity}	A network health score indicating node states as follows:
	`INTERFACE_UNKNOWN = 1`
	`INTERFACE_WARNING = 1`
	`INTERFACE_DOWN = 1000`
	`NODE_UNKNOWN = 1000000`
	`NODE_WARNING = 1000000`
	`NODE_DOWN = 100000000`
	
	The `Up` score for Nodes and Interfaces is zero.

${Version}	Version of the SolarWinds software package

Syslog Message Priorities

Included at the beginning of each Syslog message is a priority value. The priority value is calculated using the following formula:

Priority = Facility * 8 + Severity

Syslog Facilities

The facility value indicates which machine process created the message. The Syslog protocol was originally written on BSD Unix, so Facilities reflect the names of UNIX processes and daemons, as shown in the following table.

Note: If you are receiving messages from a UNIX system, consider using the **User** Facility as your first choice. Local0 through Local7 are not used by UNIX and are traditionally used by networking equipment. Cisco routers, for example, use Local6 or Local7.

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 subsystem	18	local use 2 (local2)
7	network news subsystem	19	local use 2 (local3)
8	UUCP subsystem	20	local use 2 (local4)

Number	Source	Number	Source
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)

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 issues before ALERT-level problems.
3	Error	Non-urgent failures. Notify developers or administrators as errors 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.

Number	Severity	Suggested Actions
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.

Chapter 21: 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 162 and then decodes, displays, and stores the messages in the Orion database. The SolarWinds Trap Service allows Orion 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. As a benchmark, a typical SolarWinds installation can process approximately 500 traps per second.

Note: Higher capacity can only be achieved with significant hardware improvements over minimum SolarWinds requirements.

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 Orion 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), SNMPv2c, and SNPMv3, 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. Each managed device can notify the Orion 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. 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.

Note: When using SNMPv3 for polling a device and receiving traps from it, confirm that the same authentication type (auth, noauth, or priv) is configured for both polling and traps.

Viewing SNMP Traps in the Web Console

Customize the Traps view as shown in the following procedure.

To view SNMP traps in the Web Console:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Click **Traps** in the Views toolbar.
3. ***If you want to filter your traps table view by device,*** select the device to which you want to limit your view in the **Network Object** field.
4. ***If you want to filter your traps table by device type,*** select the device types you want to view in the **Type of Device** field.
5. ***If you want to limit your traps table to show only traps of a designated type,*** select the appropriate type in the **Trap Type** field.
6. ***If you want to limit your traps table to show only traps originating from a specific IP address,*** type the IP Address in the **Source IP Address** field.
7. ***If you want to limit your traps table to show only traps with a designated community string,*** select the appropriate community string in the **Community String** field.
8. ***If you only want to see traps from a specific period of time,*** select the time period from the **Time Period** menu.
9. Confirm the number of traps displayed in the **Show Traps** field.
10. Click **Refresh** to update the Traps view with your new settings.

Using the Trap Viewer

After the monitored devices on your network are configured to send traps to the Orion server, configure the Orion Trap Viewer to display received trap information, as shown in the following sections.

Notes:

- To ensure proper configuration of your network devices, refer to the documentation supplied by the vendor of your network devices.
- The Orion Trap Viewer receives traps on UDP port 162.

Viewing Current Traps

Trap Viewer makes it easy to view trap messages, as shown in the following steps.

To view current trap messages:

1. Click **Start > All Programs > SolarWindsOrion > Syslog and SNMP Traps > Trap Viewer**.
2. Click **View > Current Traps**.
3. Click a column header to order listed traps by the selected trap characteristic.
4. Configure the Trap Viewer by clicking and dragging columns to order the presentation of trap characteristics.

Searching for Traps

Collected trap messages may be searched within Trap Viewer. The following steps both search for trap messages and format the search results list.

To search the trap message list:

1. Click **Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer**.
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**.
7. ***If you want to hide the search criteria pane,*** toggle the pane open and closed by clicking the double up arrows in the top right of the page.

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 Orion > Syslog and SNMP Traps > Trap Viewer**.
2. Click **File > Settings**.
3. On the General tab, configure the following Trap server settings:
   a. Position the top slider to set the **Maximum number of traps to display in Current Traps view**.
   b. ***If you want SolarWinds NPM to Automatically Refresh the Current Traps View,*** check the option accordingly, and then position the middle slider to set the refresh rate.
   c. Position the **Retain Trap messages for how many days?** slider to set the length of time that traps remain in the database.
4. On the Displayed Columns tab, use the arrow keys to select and order the fields of information you want to see in the Current Traps view.
5. ***If you do not need the domain name from your trap messages,*** check **Remove Domain Name from DNS Lookups** on the Message Parsing tab.

   Note: Checking this option will remove the domain name from your trap messages, and this will help to reduce the size of your database.

Configuring Trap Viewer Filters and Alerts

The Trap Viewer can be configured to trigger SolarWinds NPM alert actions when received trap messages match defined rules. The following steps establish rules to filter trap messages and initiate alert actions as you determine.

Notes:

- With the exception of the asterisk (*) wildcard, SolarWinds recommends against using non-alphanumeric characters in filter definitions.
- Trap rules are not applied to unmanaged nodes.

To configure Trap Viewer filters and alerts:

1. Click **Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer**.
2. Click **File > Settings**, and then click the Alerts / Filter Rules tab.
3. ***If you are creating a new rule,*** click **Add Rule**.
4. ***If you are editing an existing rule,*** click **Edit Rule**.
5. Click the General tab.
6. Enter a **Rule Name**, and then check **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 limited to messages from specific hosts, domains, or hostname patterns,*** click DNS Hostname, and then enter a DNS Hostname Pattern.

   Notes:

   - The DNS Hostname Pattern rule is case-sensitive.
   - When **Use Regular Expressions in this Rule** is checked, regular expressions can be used in place of "like" statements. For more information about using regular expressions in NPM, see Regular Expression Pattern Matching.

   When **Use Regular Expressions in this Rule** is checked, regular expressions can be used in place of "like" statements. For more information about using regular expressions in NPM, see Regular Expression Pattern Matching.

10. ***If you want the rule limited on the basis of content within the Trap Details field,*** click Trap Details, and then enter a Trap Details Pattern.
    Note: When **Use Regular Expressions in this Rule** is checked, regular expressions can be used in place of "like" statements. For more information about using regular expressions in NPM, see Regular Expression Pattern Matching.
11. ***If you want the rule limited to specific community strings,*** click Community String, and then enter appropriate patterns in the **Community String Pattern** field.
    Note: When **Use Regular Expressions in this Rule** is checked, regular expressions can be used in place of "like" statements. For more information about using regular expressions in NPM, see Regular Expression Pattern Matching.
12. Click Conditions, and then generate trigger conditions 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** as necessary.

13. ***If you want to limit rule application to within a specific period of time,*** click Time of Day, check **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 traps arrive that match the rule,*** click Trigger Threshold, check **Define a Trigger Threshold for this Rule**, and then enter option values as appropriate.

    Note: When **Suspend further Alert Actions for** is checked, 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 will never be sent.

15. Click **Alert Actions**.
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.
17. ***If you are editing an existing action for the rule,*** select an action from the list, click **Edit Action**, and then configure the action.
18. Use the arrow buttons to set the order in which actions are performed.

    Note: Actions are processed in the order they appear, from top to bottom.

19. ***If you need to delete an action,*** select the action, and then click **Delete Action**.
20. Click **OK** to save all changes and return to Trap 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 Trap Alert Actions

The following actions are available for trap alerts.

Discard the Trap

Allows you to delete unwanted traps sent to the SNMP Trap server.

Tag the Trap

Allows you to add a custom tag to received traps. Ensure you include the Tag column in the viewer when assigning a tag.

Flag the Trap with a specific color

Allows you to assign a specific color for display in the Orion Web Console and the Trap Viewer 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 a local or 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. Specify the IP address or hostname of the trap destination and the port on which the trap should be sent. Check **Include Source Address** to include the IP address of the trap source.

Play a sound

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 using a batch file. This action is used when creating realtime change notifications in NPM.

Execute an external VB Script

Allows you to launch a VB Script using the selected script interpreter engine and a saved script file.

Send a Windows Net Message

Allows you to send a Windows Net message either to a specific computer or to an entire domain or workgroup.

Note: The only operating systems supporting Windows Net Messaging on which SolarWinds supports Orion installations are Windows Server 2003 and Windows XP. SolarWinds only supports Orion evaluations on Windows XP.

Send an E-mail / Page

Allows you to send an email from a specified account to an address, using a specific SMTP server, and containing a customizable subject and message.

Stop Processing Trap Rules

Stops the processing of SNMP trap rules for the matching trap.

Change the status of an interface

SolarWinds NPM can change the status of an interface from which a trap is received. Designate the status to which .the interface should change.

Trap Alert Variables

The following variables can be used in trap alert messages with the Orion Trap Server. Each variable must begin with a dollar sign and be enclosed in curly braces as, for example, **${**VariableName**}**.

Note: Trap alerts may also use any valid node variables. For more information about node alert variables, see Orion Variables and Examples.

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

Trap Date/Time Variable	Description
${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

Other Trap Variables

Trap Variable	Description
${Application}	SolarWinds application information
${Community}	Node community string

Trap Variable	Description
${Copyright}	Copyright information
${DNS}	Fully qualified node name
${Hostname}	Host name of the device triggering the trap
${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}.
${vbData1}	Trap variable binding value
${vbName1}	Trap variable binding name

Chapter 22: Creating Custom Properties

Custom properties are user-defined fields such as country, building, asset tag, or serial number, that you can define, associate with monitored network objects, and store in your SolarWinds database. After properties are added, they are available for use throughout the Orion Web Console.

Note: Custom properties must use the Latin1 character set.

A few examples of how custom properties may be used are as follows:

- Add information to nodes, such as contact, owner, or support contract
- Add a custom property that is used as an account limitation on nodes
- Add a custom property to nodes for grouping them on the web or in a report
- Add a custom property and display it as an annotation on a chart

A collection of the most commonly used properties is provided with your SolarWinds Orion installation, but it is easy to create additional custom properties to meet your precise requirements. For more information, see Creating a Custom Property.

Once a custom property is defined, the Import Wizard allows you to populate it from either a text- or comma-delimited file. For more information, see Importing Custom Property Data.

Alternatively, if you want to apply a property to only a few objects, you may choose to do this using the Edit view. For more information, see Editing Custom Properties.

You may also create external records by exporting custom properties from selected objects as a spreadsheet. For more information, see Exporting Custom Property Data.

Creating a Custom Property

The following procedure shows how to create a custom property in SolarWinds Orion products using Orion Platform 2012.2 and higher.

Note: Older versions of SolarWinds Orion Platform Services used the Custom Property Editor application to create and manage custom properties. The Custom Property Editor is not accessible through the Orion Web Console..

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.
3. Click **Manage Custom Properties** in the Node & Group Management grouping.
4. Click **Add Custom Property**.
5. Select the object type for the property you are creating, and click **Next**.

   Note: The object types available depend on the SolarWinds Orion products installed, but all installations will allow you to create **Node** and **Volume** custom properties.

6. ***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**.

7. Edit the **Property Name** and **Description** fields, as appropriate.

   Note 1: Property names must be unique for an object type. For example, you can have separate **Comment** properties for Nodes, Volumes, and other object types.

   Note 2: Property names are not case-sensitive. You cannot, for example, have properties called **Comment** and **comment** for the same object type.

8. Select the **Format** for the property. If Text is selected, you can click **Edit** to specify a maximum length.
9. Check the **Required** property box if this property must be provided for all objects.

10. ***To restrict the values that other, non-administrative users can select for the property,*** check **Restrict values**, and enter values, as follows:
    a. Enter an appropriate **Value**.
    b. Click **Add Value**.
    c. Repeat until you have entered all valid property values.
    d. ***To delete a provided property value,*** click **X** next to the property to delete.
11. If creating a custom property for Nodes, select the **Usage** for the property.
12. Click **Next**.
13. Click **Select <Objects>**, then, using one of the following methods, sort the objects to which the property can be applied:
    - Select an appropriate **Group by:** criterion, and click the group that includes the objects to which you want to apply this property
    - Use the search tool to search for the objects to which you want to apply the selected property
14. Check the objects to which you want the selected custom property to apply.

    Note: Click **>** to expand listed objects to view available child objects.
15. Click **Add** to add the checked objects to the **Selected <Objects>** list.
16. In the **Selected <Objects>** list, check the objects to which you want the selected property to apply, and click **Select <Objects>**.
17. For the selected objects, enter or select the required value.
18. ***If you are editing a property with restricted values, and want to add a new property value***, select **Add new value** from the drop-down menu, and enter the **New value**.
19. ***To apply the selected property to a different group of objects,*** click **Add more**, select objects as indicated above, and click **Submit**.

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.
3. Click **Manage Custom Properties** in the Node & Group Management grouping.
4. Check each property you want to remove, and click **Delete**.
5. Confirm your selection by clicking **Delete** when prompted.

Importing Custom Property Data

Once you have defined custom properties, you can import corresponding values from a formatted external document. For example, you may already possess a spreadsheet listing the asset tags of all your network nodes, and you may 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.

Note: Your data should be formatted as a table and at least one column title should match an existing object property (for example, IP Address).

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.
3. Click **Manage Custom Properties** in the Node & Group Management grouping.
4. Click **Import Values**.
5. Click **Browse**, navigate to your custom property data file, and click **Open**.
6. Select the object type for which you are importing values from the **Import values for** drop-down.
7. Click **Next**.

8. For each detected **Spreadsheet Column** in your data, select the corresponding **Orion Database Column**, and then select the appropriate **Relationship** between the indicated columns. This can be either **matches** or **imports to**.
    - Select **matches** to indicate columns in the spreadsheet that corresponds to existing columns in the Orion database (e.g. IP Address, MAC address).
    - Select **imports to** to import the data in the spreadsheet column to the selected Orion database column.

      Note: This option overwrites any existing data in the corresponding in the custom properties.
    - Select **imports to** and select **<No match found, ignore>** for any spreadsheet column you don't want imported.
    - Select **Create this custom property now** to open the Add Custom Property in a new browser tab if you need to create a custom property for this spreadsheet column.
9. Click **Import**.

Exporting Custom Property Data

Once you have defined custom properties, you may export your custom property data for selected monitored objects as a spreadsheet. For example, you may want to create a single spreadsheet that lists the asset tags of all your network nodes. The following steps outline the process for exporting custom property data.

To export custom property data:

1. Log in to the Orion Web Console using an account with administrative privileges.
2. Click **Settings** in the top right corner of your web console.
3. Click **Manage Custom Properties** in the Node & Group Management group.
4. Check the custom properties you want to export, and click **Export values**.

   Note: You can only select custom properties for a single object type.
5. ***If you want to export custom property data for specific objects of the type previously selected,*** click **Select <Objects>**, and select the desired objects.
6. Check the database columns you want to export. You can also change which custom properties you want to export here.
7. Select the file type to use for your exported data. This can be .csv, .txt, .html. or xls.
8. Click **Export**.

Custom Property Editor Settings

The Custom Property Editor Settings window allows you to customize the display for nodes and volumes.
Note: Orion Network Performance Monitor users may also customize the display for interfaces.

To configure Custom Property Editor settings:

1. Click **Start > All Programs > SolarWinds Orion > Grouping and Access Control > Custom Property Editor**.
2. Click **File > Settings**.
3. Click Node Editing and check the system properties you want to see in the Edit Node Properties window. Repeat for Volume Editing.
4. ***If you want to enable Auto-Search,*** click Auto-Search, and then check **Enable Auto-Search. Note:** With Auto-Search enabled, the current column is searched as you type. Select a cell, and then press **Enter** to edit its contents. With Auto-Search disabled, typing will begin editing the cell.

Editing Custom Properties

The Custom Property Editor allows you to easily enter or modify custom properties. If you are entering a large amount of data it can be easier to import the values from a spreadsheet using the Import feature. For more information, see Importing Custom Property Data.

To edit 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 the check boxes for the properties to be edited. You can only edit properties of one object type at a time.
4. Click in cells in the table that you want to edit, and then enter or modify the cell contents, as required.
5. ***To filter data displayed by column***, click the filter symbol before the column name, and enter the text to be filtered on in the pop-up box.
6. When you have added or edited the values, click **Save Changes**.

Using Filters in the Custom Property Editor Edit View

Filtering is available in the Edit Custom Properties windows for all devices, and you can apply filters to manipulate available data views. Custom Property Editor allows you to edit the text within custom property fields to which a filter is applied. The following procedures show how to use filters within Custom Property Editor.

Creating Custom Properties Filters

The following procedure creates a custom properties filter.
Note: Orion Network Performance Monitor users may also create filters for interface custom properties.

To create a filter:

1. Click **Start > All Programs > SolarWindsOrion > Grouping and Access Control > Custom Property Editor**.
2. Click **Properties > Edit Object Properties**, where Object is **Node** or **Volume**, as appropriate.
3. Click **Filter Active** or **No Active Filter**, and then click **Apply Filter**.
   Note: The text of the **Filter Active** / **No Active Filter** button changes dynamically, indicating the filter status for the currently viewed data.
4. Click the hyperlinked text to select the appropriate criteria.
5. Click the ellipsis, 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.

   Note: The lists of available linked descriptors are dynamically generated in consideration of all other variables within the same condition. Click **Browse** (**…**) to select a condition type.

Select **Move current condition forward** or **Move current condition backward** to change the order of your conditions accordingly.

6. Continue to click hyperlinked text and use the cascading menus to select filtering criteria.
7. ***If you have completed the configuration of your filter,*** click **OK**.
   Note: The Edit Object Properties view changes, based upon the selected filter, and the text of the **Filter Active** / **No Active Filter** now displays “Filter Active”, indicating that the filter is being applied to the currently viewed properties.

Removing Custom Properties Filters

The following procedure removes a custom properties filter.
Note: Orion Network Performance Monitor users may also remove filters for interface custom properties.

To remove a filter:

1. Click **Start > All Programs > SolarWinds Orion > Grouping and Access Control > Custom Property Editor**.
2. Click **Properties > Edit** Object **Properties**, where Object is **Node** or **Volume**, as appropriate.
3. Click **Filter Active**, and then click **Remove Filter**.

   Note: The Edit Object Properties view now displays all custom properties.

Chapter 23: Managing the Orion Database

All Orion network monitoring and management products use a Microsoft SQL Server database to store web console settings and collected network performance and configuration data.

Your Orion installations provides two utilities that allow you to perform the most commonly required database tasks without having to access either the Microsoft SQL Server or its associated tools. These are the Database Manager and Database Maintenance tools, and their use is covered in the first part of this chapter.

The rest of this chapter gives a brief guide to creating a database maintenance plan using the Microsoft SQL management tool and how to backup and restore your database if you need to upgrade or move the SQL server.

Database Manager

The Database Manager enables you to add SQL servers to your Orion configuration. It also lets you view database information, perform queries and edit database values. For more information, see Using Database Manager.

Database Maintenance

The Database Maintenance utility allows you to summarize, clean, and compact your Orion database. For more information, see Database Maintenance.

Using Database Manager

The Database Manager is used to add addition servers to your Orion configuration, perform queries, view database and table details, export data, and edit database values. The following procedures cover these basic database management operations.

For more advanced database maintenance, it is recommended that you use the Server Management Studio provided with Microsoft SQL Server to back up, clear historical maintenance records and perform other maintenance. For more information, see Creating a Maintenance Plan with SQL Server Management Studio.

Adding a Server

If you have not already designated a backup or supplementary database for use with Orion, you can use the following steps to add a SQL server. Once added, your selected server and associated databases are displayed in the tree structure in the left pane of Database Manager.

To add a SQL server using the Database Manager:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Manager**.
2. ***If you have a default server and wish to use it***, click **Add default server**.
3. ***To select a server***, complete the following steps:
    a. Click **Add Server**.
    b. Select or enter the SQL Server instance you want to use in `server/instance` format.
    c. Select the appropriate authentication method, enter your credentials, and click **Connect**.

Viewing Database Details

The two tabs displayed in the Database Details view of the Database Manager show the database properties and tables.

To view database details:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Manager**.
2. ***If the SQL Server hosting your Orion database is not listed in the left pane,*** you must add the SQL Server hosting your Orion database. For more information, see Adding a Server.
3. Click **+** in the left pane to expand the SQL Server hosting your Orion database, and then right-click the database.
   Note: The default database name is **SolarWindsOrion**.
4. Click **Database details**.

   Notes:

   - The Properties tab shows general statistics and descriptions of the selected database.
   - The Tables tab lists the tables and their respective sizes.
5. If you have not yet made a backup of the database, the **Last Backup** field on the Properties tab is blank. For more information, see Creating a Maintenance Plan with SQL Server Management Studio.

Viewing Table Details

The Database Manager Table Details window provides property, column, and index information about the selected table. You can also query the selected table directly from the Table Details window.

To access table details:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Manager**.
2. ***If the SQL Server hosting your Orion database is not listed in the left pane,*** you must add the SQL Server hosting your Orion database. For more information, see Adding a Server
3. Click **+** in the left pane to expand the SQL Server hosting your Orion database, and then click **+** to expand your Orion database.

   Note: The default database name is **SolarWinds Orion**.
4. Right-click a table to view, and then click **Table details.**

Note: The Properties tab includes general statistics relating to the selected table size and creation date. The Columns tab lists keys, column names, size and data types in the selected table. The Indexes tab shows indexes used in the table.

5. ***To execute a query***, right-click on the table name, and then click **Query Table**. The SQL query displayed lists the contents of the table. Users familiar with writing SQL queries can edit this query as required. Click **Execute** to run this query.
6. ***To edit the data within a table***:
    a. Right-click on the table name, and click **Query Table**.
    b. Click **Execute** to run the query, which lists the contents of the table in the Results page.
    c. Click **Enable table editing**. You can now edit the data fields within the table as required.

    Warning! Table editing should only be performed by a database administrator or other expert user. Changes made here can jeopardize the integrity of your data. It is recommended that you use the Settings with your Orion Web Console to make any necessary changes to database settings and values.
7. ***To export a table***, right-click on the table name, and click **Export to CSV**. You will be asked to enter a name for the comma separated value file created.

Database Maintenance

The primary tasks involved in maintaining your SolarWinds database are data summarization and database compaction. Data summarization occurs automatically as a regular part of the automated maintenance program. However, you can also run database maintenance as required from the Windows Start menu.

Running Database Maintenance

Database maintenance consists of a series of data summarizations to optimize the size of your Orion database. Data summarization gathers the collected network data for a defined period, calculates statistics from the data, and then discards the data itself while retaining the statistics.

Database maintenance is run automatically every day at a specified time.

To specify when Data Maintenance is run:

1. From the Orion Web Console, click **Settings**, and then click on **Polling Settings** in the Thresholds and Polling section.
2. Scroll down to the Database Settings section, and enter the time you want Data Maintenance to take place in the Archive Time field.

To launch Data Maintenance manually:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Maintenance**.
2. Click **Start**.

Note: Administrative privileges are required to run Database Maintenance.

Best Practices for Managing Your Orion Database

As your SQL database matures, or after adding new Orion products, your database may become larger than you originally estimated or might slow unexpectedly. Several factors may cause these issues. This section explores the most common issues and explains how to correct the issues.

Managing Database Growth in the Orion Web Interface

The most common issues with SolarWinds Orion databases are related to the database size. Properly managing size can help you avoid issues with storage capacity and database performance. A primary factor in database size is the data retention settings available in SolarWinds Orion. Each SolarWinds Orion Product allows you to manage the data rollup periods and the data retention limit. The impact of adjusting any of these data retention and rollup windows will be roughly proportional to the effect the Orion Product has on the database size. When considering expanding a data retention period, you may be able to make small changes and examine the impact on size and performance as you approach the desired new limit.

Not all of the data rollup periods are adjustable. Typically, you can alter one intermediate data rollup period and the limit for data retention.

The impact of altering data retention can be summarized by this rule: The shorter the data interval, the greater the effect the setting will have on the database size.

- Extending the detailed data retention will have the largest potential impact on database size and performance.
- Extending hourly retention will have a lesser effect.
- Extending daily retention will have the least effect.

This is due to the summarization of detailed data into hourly data increments and then into daily data increments. Each SolarWinds Orion Product allows similar data retention options and the above guidelines should be followed for each product.

Troubleshooting Your Orion Database

Two of the most common symptoms of database issues are degraded Orion performance, and errors related to the inability to connect to the database.

Note: This section covers only the basics of determining a database issue as the issue pertains to interaction with Orion. It is not intended as an SQL troubleshooting guide.

In the Orion database, the single most important SQL server performance measurement is disk queue length. Queue length is a measurement of the SQL writes that are waiting to be written to disk. When disk queues start lengthening and there is a steady load on the SQL writes, the queues may grow so large that write requests get dropped. This may lead to gaps in data and will affect the overall performance of the SQL server. A good rule of thumb is that disk queue length should not exceed two times the number of effective spindles in the SQL storage. The effective spindle count is the number of striped spindles. For a RAID 10 direct attached storage unit with eight total disks, the effective spindle count is four. Four of the spindles in this array are the primary striped array and the other four are a secondary striped mirror of the four primary spindles. Since no performance gain is achieved by mirroring disks, only the primary striped set is used to measure performance.

For additional information on database performance, see the Managing Orion Performance Technical Reference (PDF).

When errors occur that point to a loss of the connection to the database the following steps can help isolate the issue:

1. Ping the SQL server from the Orion server to check network connectivity.
2. Open SQL Server Management Studio or the Orion Database Manager and attempt to connect to the database.
3. If both of the above are successful, run the Orion Configuration Wizard against the database by selecting Database in the first wizard screen. Ensure that you are using the proper database credentials.
4. Open the Orion web UI to test connectivity again.
5. Test opening an ODBC connection from the Orion server using a Microsoft utility such as ODBCPing.

If all of this fails, then the issue is a failure with the SQL server. At this point, you will need to go directly to the SQL server and begin troubleshooting. Troubleshooting SQL is very specific for each version and implementation, and it is recommended that you consult the Microsoft Support site and search for information pertaining to your version.

Upgrading Your Database

At some point, you may need to upgrade or move your Orion database. For example, you may have to change your version of Microsoft SQL Server or move your data to a different server. This section gives information on backing up your current database, reinstalling it on a new server and then reconfiguring Orion to use this database.

Requirements

Before you attempt to modify or back up your existing database, ensure:

- The new database server is installed correctly.
- The SQL Browser Service is running on the server to which you are moving your existing database. This service runs on UDP port 1434, and it may be blocked by internal firewalls.
- You have the `sa` password for both your existing Orion database server and your new database server.
- You have the credentials to an account with administrator rights on both your existing Orion database server and your new database server.
- You have scheduled a maintenance window during which you can safely shut down your Orion services. You need to stop data collection to ensure that your backup file matches your last active database state.

Stopping Orion Services

Before you back up your database, it is important to stop the Orion services that are currently writing to the database. This ensures that you do not have data inconsistencies when you bring your new database server online.

To stop Orion services:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Orion Service Manager.**
2. Expand **Services**.
3. Click each service, except the SQL Server service, and click **Stop**.

Notes:

- If you have more than one Polling Engine, you will need to stop each additional Polling Engine before continuing.
- Do not stop the SQL Service. The SQL Service needs to be running in order to make the necessary changes to the database.

4. Click **File > Exit.**

Creating a Database Backup

When your Microsoft SQL Server was installed, the database management utility, Management Studio, should also have been installed. You can use this utility to create and install backups of your Orion database.

The procedures for backing up your database is similar for each version and can be found at the Microsoft Support website:

- SQL Server 2014
- SQL Server 2012
- SQL Server 2008 R2
- SQL Server 2008
- SQL Server 2005

While these external links were correct at the time of writing, they cannot be guaranteed after this. If the required page has been moved, go to the Microsoft Support page and search for the version of the SQL server you are using.

Restoring a Database Backup

After you have backed up your Orion database, you can now restore it on the new server. This should be done with the management tool associated with the new server.

The procedures for restoring your database is similar for each version and can be found at the Microsoft Support website:

- SQL Server 2014
- SQL Server 2012
- SQL Server 2008 R2

- SQL Server 2008
- SQL Server 2005

While these external links were correct at the time of writing, they cannot be guaranteed after this. If the required page has been moved, go to the Microsoft Support page and search for the version of the SQL server you are using.

Updating Orion to Use New Database

After you have restored your Orion database backup file, you must update your Orion server to recognize the restored database on the new database server, as shown in the following procedure.

Note: SolarWinds recommends that you use SQL Server Authentication with the `sa` login and password to ensure that Orion can always access your SQL Server database, even if it is hosted remotely on a separate server.

To update Orion to use a new database:

1. Log on to your Orion server.
2. Click **Start > All Programs > SolarWinds Orion > Configuration and Auto-Discovery > Configuration Wizard**.

   Note: In older versions of Orion, the correct path may be **Start > All Programs > SolarWinds Orion > Configuration Wizard.**
3. Check **Database**, and then click **Next**.
4. Specify your new database server in the **SQL Server** field.
5. ***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 Orion has required access to your migrated database
   - The New Account must be a member of the `securityadmin` server role
   - The `sysadmin` role and the `sa` user account are always members of `securityadmin`

10. Provide and confirm an account **Password**.
11. Click **Next** to start database configuration, and then click **Finish** to exit the Configuration Wizard.

Creating a Maintenance Plan with SQL Server Management Studio

While it is not within the scope of this Administration Guide to cover the use of the any of the Microsoft SQL Server and its associated tools, the following procedures gives a brief guide to configuring a daily Orion database maintenance plan using the SQL Server management tool provided with your server.

Notes:

- Your specific environment may require additional configuration.
- You may need to contact your database administrator to gain access to SQL Server Management Studio for your Orion database.
- The following procedure clears historical maintenance records and creates a backup of your Orion database. In general, however, SolarWinds recommends that you contact your database administrator and reference the Microsoft documentation provided with SQL Server for instructions on using SQL Server Management Studio to manage your Orion database.

To use SQL Server Management Studio to manage your Orion database:

1. Click **Start > Microsoft SQL Server > SQL Server Management Studio**.
2. Click **View > Object Explorer**.

3. Expand the SQL Server instance containing your Orion database in the Object Explorer pane on the left.
   Note: Expand the Databases folder for any instance to confirm included databases. By default, the Orion database is named **SolarWinds Orion**.
4. Expand the Management folder, right-click the Maintenance Plans folder, and then click **Maintenance Plan Wizard**.
   Note: The Maintenance Plans folder will only be visible if you have Administrator rights.
5. Click **Next** to start the SQL Server Maintenance Plan Wizard.
6. Provide an appropriate **Name** and **Description** for your maintenance plan.
7. Click **Browse (…)** next to the **Server** field.
8. Check your SQL Server\Instance, and then click **OK**.
   Note: If your SQL Server\Instance is not in the list, provide it manually.
9. Select the authentication type that is used to connect to the SQL server, and, if required, provide appropriate **User name** and **Password** credentials.
   Note: Use the same authentication type and credentials you provided in the Orion Configuration Wizard to access your Orion database.
10. Check **Clean Up History** and **Back Up Database (Full) Note:** When a task is clicked, the Maintenance Plan Wizard provides a brief task description.
11. Click **Next**.
12. Set the order of task execution, top to bottom, by selecting tasks and clicking **Move Up** and **Move Down** as needed.
    Note: The following steps assume the Clean Up History task precedes the Back Up Database (Full) task.
13. Click **Next** when the task execution order is set.
14. On the Define Cleanup History Task view, check the types of historical data to delete, and then set the threshold age for historical data removal.
15. Click **Next**.
16. On the Database Back Up (Full) view, complete the following steps:
    a. Click the **Databases** field.
    b. Select **These databases**.
    c. Check your Orion database.

17. Click **OK**.
18. Select **Database** in the Backup component area.
19. In the Destination area, complete the following steps:
    a. Select **Disk**.
    b. Select **Create a backup file for every database**.
    c. Click **Browse (…)** to select an appropriate database backup file destination with sufficient free space.
20. Click **Next**.
21. On the Select Plan Properties view, click **Change**.
22. Configure the database maintenance job schedule as follows:
    a. Provide an appropriate **Name** for the new job schedule.
    b. Select **Recurring** as the **Schedule type**.
    c. Check **Enabled**, and then select **Daily** in the **Occurs** field.
    d. Provide an off-peak network usage time in the **Occurs once at** field.
    e. Select a **Start date**, and then select **No end date**.
23. Click **OK**.
24. Click **Next**, and then check **Write a report to a text file**.
25. Click **Browse (…)** to select an appropriate maintenance report file destination.
26. Review wizard results, click **Finish**, and then, when the wizard successfully finishes, click **Close**.

For further information on using SQL server Management Studio, visit the Microsoft Support Website at http://support.microsoft.com.

Chapter 24: Orion Product Family

The SolarWinds Orion family of products delivers easy-to-use, scalable solutions to meet your network, systems, and storage monitoring and management needs. The following sections provide more information about individual products in the Orion family:

- Monitoring Network Application Data (SAM)
- Managing IP Addresses (IPAM)
- Managing IP Service Level Agreements (SolarWinds VoIP and Network Quality Manager)
- Monitoring NetFlow Traffic Analysis Data (NTA)
- Orion Scalability Engines
- Using an Orion Additional Web Server
- Orion Failover and Disaster Recovery

Monitoring Network Application Data (SAM)

SolarWinds Server & Application Monitor (SAM) provides focused application monitoring for network engineers, but it is much more than merely up/down status checks and process monitoring. By allowing you to create and monitor your own custom collection of monitored components, SAM provides an open field of opportunity to the network engineer. With SAM you can focus monitoring on your core services while easily ensuring application outages do not originate in the network. SAM provides the following features to help:

- Network service monitoring
- General TCP port monitoring
- WMI and SNMP process monitoring
- Service monitoring
- User experience monitoring using HTTP or HTTPS content checking

Built on the proven capabilities and solid architecture of SolarWinds Orion Platform Services, you know your current needs will be met and, as your needs grow, both the Orion platform and SAM will scale with you.

For more information about monitoring network applications with SolarWinds Server & Application Monitor, see the SolarWinds Server & Application Monitor Administrator Guide at www.solarwinds.com.

Managing Network Configurations (NCM)

SolarWinds NCM extends the SolarWinds family of powerful network monitoring, alerting, and reporting capabilities to configuration management. Network engineers can proactively monitor their entire network infrastructure from a single intuitive pane of glass, viewing network monitoring statistics alongside enterprise-wide configuration health indicators. SolarWinds NCM can help engineers quickly isolate network issues regardless of their origin. SolarWinds NCM leverages Orion's agentless architecture to allow network engineers themselves to deploy and begin managing network device configurations in just minutes without requiring expensive consultants. SolarWinds NCM continues Orion's tradition of providing easy to use software, a robust feature set, and enterprise scalability at an affordable price point. SolarWinds NCM's scalability and licensing flexibility allow network engineers to easily purchase and grow their monitoring solution whether their business has only a few network devices or thousands.

SolarWinds NCM lets users manage network configuration files from multiple device vendors using a highly intuitive web interface. It continuously monitors device configurations and provides notification of any configuration changes to help you resolve problems before they impact users. SolarWinds NCM users can quickly fix issues without requiring engineers to manually Telnet or SSH change configuration parameters on the devices in question. SolarWinds NCM additionally allows users to quickly check compliance reports and confirm their devices are meeting regulatory and corporate standards. The standalone application can integrate with Orion Network Performance Monitor (NPM) to provide a comprehensive web-based network fault, performance, and configuration management solution.

Managing IP Addresses (IPAM)

IP Address Manager (IPAM) is an NPM module that leverages the intuitive point-and-click interface of the Orion Web Console to allow you to easily investigate IP address space issues. By periodically scanning the network for IP address changes, IPAM maintains a dynamic list of IP addresses and allows engineers to plan for network growth, ensure IP space usage meets corporate standards, and reduce IP conflicts. Using IPAM, network engineers can discover non-responsive IP addresses, coordinate team access to your IP space, and track network changes.

Built on enterprise Orion Platform Services, IPAM allows network engineers to create, schedule, and share IP space reports from a single reporting engine. Finally, network engineers can monitor network devices for fault, performance, configuration, and now IP address health indicators.

- Manage your entire IP infrastructure from an intuitive web console
- Consolidate your IP addresses into a single repository
- Keep better records by periodically scanning your network for IP address changes
- Create, schedule and share reports on the IP address space percent utilization
- Keep network devices up by identifying and eliminating IP address conflicts
- Coordinate team access to your address space with role-based access control and track changes
- Identify non-responsive IP addresses to optimize your IP space

For more information about IP Address Manager, see the SolarWinds IP Address Manager Administrator Guide at www.solarwinds.com.

Managing IP Service Level Agreements (SolarWinds VoIP and Network Quality Manager)

SolarWinds VoIP and Network Quality Manager offers an easy-to-use, scalable IP SLA network monitoring solution that can integrate seamlessly with other SolarWinds products on the Orion platform.

Internet Protocol Service Level Agreement (IP SLA) technology offers a cost-effective and efficient response to the needs of enterprises of all sizes. As a network manager, you face more than the simple question of whether your network is up or down. You need to know specific quality of service measurements for your network. VoIP and Network Quality Manager gives you the tools to quickly test the fitness of your current network and then determine and track quality of service on your network over time.

SolarWinds VoIP and Network Quality Manager leverages the proven functionality of SolarWinds Network Performance Monitor (NPM) by adding IP SLA-specific data collection and presentation tools that enable IP SLA network monitoring and real-time status reporting. As a module of NPM, VoIP and Network Quality Manager maintains the function of NPM while allowing you to narrow your network management and monitoring focus to the IP SLA-capable devices of your wider network. VoIP and Network Quality Manager is also available as a standalone solution which still leverages the underlying NPM technology to discover and monitor your nodes.

For more information about SolarWinds VoIP and Network Quality Manager, see the SolarWinds VoIP and Network Quality Manager Administrator Guide at http://www.solarwinds.com/.

Why Install VoIP & Network Quality Manager

Internet Protocol Service Level Agreement (IP SLA) technology offers a cost-effective and efficient response to the needs of enterprises of all sizes. As a network manager, you face more than the simple question of whether your network is up or down. You need to know specific quality of service measures for your network, and you need to know them both historically and in real time. SolarWinds VoIP & Network Quality Manager gives you the tools to quickly test your current network fitness and then determine and track quality of service on your network over time.

SolarWinds VoIP & Network Quality Manager leverages the proven functionality of NPM, adding a number of IP SLA-specific data collection and presentation tools that enable IP SLA network monitoring and realtime status reporting. Because it is a module of NPM, SolarWinds VoIP & Network Quality Manager maintains the function of NPM while allowing you to narrow your network management and monitoring focus to the IP SLA-capable devices of your wider network.

What SolarWinds VoIP & Network Quality Manager Does

SolarWinds VoIP & Network Quality Manager provides a full-featured solution that gives you the ability to monitor and report both real-time and historical performance statistics for your IP SLA-capable network. SolarWinds VoIP & Network Quality Manager offers the following features to help you manage your entire network.

- Quality of Service (QoS) Monitoring with Cisco IP SLA Operations
- Custom Charts and Gauges
- Custom Alerts and Actions
- Custom Reporting
- Call Manager Monitoring

For more information about SolarWinds VoIP & Network Quality Manager, see the SolarWinds VoIP & Network Quality Manager Administrator Guide at www.solarwinds.com.

Monitoring NetFlow Traffic Analysis Data (NTA)

NetFlow Traffic Analyzer (NTA) is an NPM module providing an easy-to-use, scalable network monitoring solution for IT professionals who are juggling any size Cisco NetFlow-enabled network. NetFlow-enabled Cisco routers and switches provide a wealth of IP-related traffic information. NTA collects this NetFlow data, correlates the data into a useable format, and then provides this data, along with detailed network performance data collected by NPM, as easily read graphs and reports on bandwidth use in and to your network. These reports help you monitor bandwidth, track conversations between internal and external endpoints, analyze traffic, and plan bandwidth capacity needs.

NTA also provides the same flow data analysis capabilities for devices using sFlow and J-flow packets.

For more information about NetFlow Traffic Analyzer, see the SolarWinds NetFlow Traffic Analyzer Administrator Guide at www.solarwinds.com.

Monitoring Network User Connections (User Device Tracker)

SolarWinds User Device Tracker (SolarWinds UDT) allows you to monitor devices and ports for your network. With SolarWinds UDT, you can analyze your port usage and capacity and be alerted to issues before they occur. SolarWinds UDT allows you to find where devices are connected in your network and detailed information about capacity analysis. UDT regularly polls switches and routers for information about what is connected to them. Based on this information, SolarWinds UDT stores current and historical information about where a device has been connected. It also provides alerts and reports about devices connected to the network. For capacity analysis, SolarWinds UDT can report on how many ports are used on switches currently, as well as over time, so you can better understand the true utilization of the ports on your switches.

- SolarWinds UDT provides focused device and port monitoring for network engineers. SolarWinds UDT provides many features to help, including:
- Quickly find where a device (MAC address, hostname or IP Address) is connected in the network
- Find out where a device has been connected in the past and find out what has been connected to a port over time
- Provides port capacity analysis for a switch (how many ports are being used, including both monitored and un-monitored ports)
- Provides global port capacity analysis for used/available ports and network capacity planning
- Configure a watchlist to track when specific devices appear on the network and alert when the devices appear

For more information about SolarWinds UDT, see the SolarWinds User Device Tracker Administrator Guide at http://www.solarwinds.com/.

Orion Scalability Engines

Orion Scalability Engines allow you to scale the monitoring and management capabilities of your primary Orion installation as your enterprise network expands and your network management needs change. For more information about using SolarWinds scalability engines, see the SolarWinds Technical Reference, "Scalability Engine Guidelines".

SolarWinds offers the following scalability engine options for SolarWinds NPM:

- Distribute polling across multiple servers with Additional Polling Engines.
- Enable more users to access the Orion Web Console with Orion Additional Web Servers. For more information, see Using an Orion Additional Web Server.
- Protect against monitoring outages with the Orion Failover Engine and Hot Standby Server. For more information, see Orion Failover and Disaster Recovery.

Using an Orion Additional Web Server

The Orion Additional Web Server enables remote access to the Orion Web Console from a location other than your primary Orion server. With an Additional Web Server installed, remote users can view the primary Orion Web Console without deploying an entire Orion installation or excessively taxing the resources of your primary SolarWinds server. The following procedure installs the Orion Additional Web Server.

To install an Orion Additional Web Server:

1. ***If you downloaded the Orion Additional Web Server executable from the SolarWinds website,*** navigate to your download location, and then launch the executable.
2. ***If you received the Orion Additional Web Server executable on physical media,*** browse to the executable file, and then launch it.
   Note: The executable extracts to a folder containing an HTML readme, an Installer Guide, and Additional Web Server installers for all Orion products that support Additional Web Servers.
3. Launch the installer that corresponds to the Orion product installed on your primary server.
   Note: To ensure full functionality if you have multiple products installed on your main SolarWinds server, install the Additional Web Server for each product.
4. On the Welcome window of the Compatibility Check, provide the following information:
   - The **Hostname or IP Address** of your main Orion server.
   - The **User name** and **Password** of a user with administrative privileges to the Orion Web Console on your main Orion server.
5. Click **Next**.
6. ***If you are prompted to install requirements,*** click **Install**, and then complete the installation, including a reboot, if required.

   Notes:

   - Downloading and installing Microsoft .NET Framework 3.5 SP1 may take more than 20 minutes, depending on your existing system configuration.

- If a reboot is required, after restart, you may need to launch the installer again. If the installer launches automatically, click **Install** to resume installation, and then click **Next** on the Welcome window.

7. Review the Welcome text, and then click **Next**.
8. Accept the terms of the license agreement, and then click **Next**.
9. ***If you want to install the Orion Additional Web Server to a folder other than the indicated default,*** click **Browse**, and then provide a different destination folder on the Choose Destination Location window.
10. Click **Next** on the Choose Destination Location window.
11. Confirm the settings on the Start Copying Files window, and then click **Next**.
12. Click **Finish** when the Orion Network Performance Monitor Setup Wizard completes.
13. ***If you are evaluating NPM,*** click **Continue Evaluation**.
14. ***If you are installing a production version of an NPM Additional Web Server,*** click **Enter Licensing Information**, and then complete the following procedure to license your NPM 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,*** check **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 NPM server,*** select **This server does not have internet access…**, click **Next**, and then complete the steps provided.

15. ***If the Configuration Wizard does not start automatically,*** click **Start > All Programs > SolarWinds Orion > Configuration and Auto-Discovery > Configuration Wizard**.
16. Click **Next** on the Welcome tab of the Configuration Wizard.
17. Select or type the **SQL Server** used by your primary Orion server.
18. ***If you are using Windows NT Integrated Security***, select **Use Windows Authentication**, and then click **Next**.

19. ***If you are using a SQL Server login and password***, complete the following steps:
    a. Select **Use SQL Server Authentication**.
    b. Provide your **Login** and **Password**.
    c. Click **Next**.
20. Select or type the **Database Name** that is connected to your Orion server, and then click **Next**.
21. ***If a dialog appears that says that multiple polling engines have been detected,*** click **OK** to continue database upgrade/verification.
22. When the database structure validation completes, click **Next**.
23. Specify a SQL account **User Name** and **Password** for the polling engine and web site to use to access the database, and then click **Continue**.
    Note: If you already have a SQL account, you can specify the credentials for that account.
24. To set up the web console, click **Next** on the Create Website tab, and then complete the following procedure:
    a. Specify the **IP Address** of the local server on which you are installing the new web-only interface.
    b. Specify the **TCP Port** through which you want to access the web console.
    Note: If you specify any port other than **80**, you must specify that port in the URL that is used to access the web console. For example, if you specify an IP address of **192.168.0.3** and port **8080**, your URL is http://192.168.0.3:8080.
    c. Specify the volume and folder in which you want to install the web console files, and then click **Continue**.
25. ***If you are asked to overwrite an existing website,*** click **Yes**.
26. When the new web console has been created, click **Continue**.
27. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
28. Enter the local IP address in the Address bar.
29. ***If you already have an Admin account and password,*** enter them in the respective fields, and then click **Login**.
    Note: You can log in without a password using **Admin** as the Account ID.

30. Confirm that the new Additional Web Server displays the same view for the same account, as used both locally and on your primary Orion server.
31. ***If you intend to install either Orion NetFlow Traffic Analyzer or Server & Application Monitor on this Orion Additional Web Server,*** complete the following steps to install the required Additional Web Server components.
    a. Using your SolarWinds **Customer ID** and **Password**, log in to the Customer Port at **http://www.solarwinds.com/customerportal/**.
    b. Click **Additional Components** in the Customer Portal menu on the left.
    c. Click **Download Orion NPM Components**.
32. ***If you intend to use Server & Application Monitor with this Orion Additional Web Server,*** complete the following steps.
    a. Click **Application Performance Monitor Additional Web Console—v2** in the Additional Components – Orion v8 and v9 section, and then click **Save**.
    b. Browse to an appropriate location, and then click **Save**.
    c. When the download completes, click **Open**.
    d. Launch the executable, and then complete the configuration wizard.
33. ***If you intend to use Orion NetFlow Traffic Analyzer with this Orion Additional Web Server,*** complete the following steps.
    a. Click **Application NetFlow Traffic Analyzer Additional Web Console—v3** in the Additional Components – Orion v8 and v9 section, and then click **Save**.
    b. Browse to an appropriate location, and then click **Save**.
    c. When the download completes, click **Open**.
    d. Launch the executable, and then complete the configuration wizard.

Orion Failover and Disaster Recovery

Depending on the version of NPM you currently have installed, SolarWinds provides either of two failover and disaster recovery solutions: Hot Standby Engine and Orion Failover Engine. The Hot Standby Engine provides limited failover protection for NPM installations older than version 10.0. For NPM version 10.0 and higher, SolarWinds offers the Orion Failover Engine, which can protect your primary NPM installation and any installed modules.

For more information about the Orion Failover Engine, see the SolarWinds Orion Failover Engine Administrator Guide and related documentation provided at http://www.solarwinds.com/support/failoverengine/FailoverEngineDoc.aspx.

For more information about the Orion Hot Standby Engine, see the SolarWinds Knowledge Base article, "Installing, Configuring, and Testing a Hot Standby Engine".

Chapter 25: Managing Orion Polling Engines

To ensure that your polling engines are optimized to run at peak performance, you will need to occasionally tune them. If you use more than one polling engine, you will need to balance the load so that each engine can perform optimally.

When migrating servers, be sure that all nodes are assigned to the correct polling engine name. To check the status of nodes being polled, you can use the following out-of-the-box alerts: Node polling failed on last 5 tries or Node not polled in last 10 minutes. For more information about migrating servers, see Migrating SolarWinds NPM.

Viewing Polling Engine Status in the Web Console

The Orion Web Console provides the Polling Engines view, giving you immediate insight into the performance of all polling engines in your Orion installation.

To display the Polling Engine view:

1. Log in to the Orion Web Console as an administrator, and then click **Settings** in the top right of the web console.
2. Click **Polling Engines** in the Details group.

For more information about configuring the settings, see Configuring Polling Engine Settings.

Configuring Polling Engine Settings

Settings for your Orion polling engine are configured on the Orion Polling Settings view within the Orion Web Console.

To open the Orion Polling Settings view:

1. Log in to the Orion Web Console as an administrator, and then click **Settings** in the top right of the web console.
2. Click **Polling Settings** in the Settings group.

For more information, see Orion Polling Settings.

Orion Polling Settings

The following poller settings are configurable on the Orion Polling Settings view. **Note:** Depending on the Orion products and modules you have installed, additional Polling Settings may be available. For more information about module-specific polling settings, see your SolarWinds NPM Administrator Guide.

Polling Intervals

The following settings configure default polling intervals. To apply poller settings, click **Re-Apply Polling Intervals**.

You can improve SolarWinds NPM performance by entering longer polling intervals.

Default Node Poll Interval

Devices are regularly polled to determine status and response time on this designated interval. By default, this interval is 120 seconds.

Default Interface Poll Interval

Interfaces are regularly polled to determine status on this designated interval. By default, this interval is 120 seconds.

Default Volume Poll Interval

Volumes are regularly polled to determine status on this designated interval. By default, this interval is 120 seconds.

Default Rediscovery Interval

Your entire network is polled on this interval to detect any re-indexed interfaces. Monitored network devices are also checked for IOS upgrades permitting EnergyWise support. By default, this interval is 30 minutes.

Note: In Orion platform products released prior to Orion NPM version 10.1, the minimum interval allowed is 1 minute. Beginning with Orion NPM version 10.1, the minimum rediscovery interval is 5 minutes. The default rediscovery interval must be set to at least 5 minutes before you can change polling interval settings.

Lock custom values

This option is enabled by default. When enabled, all polling customizations made on the Polling Settings view are automatically saved.

Polling Statistics Intervals

The following settings configure default polling intervals for device statistics. To apply poller settings, click **ReApply Polling Statistic Intervals**.

Note: Depending on the Orion products and modules you have installed, additional Polling Settings may be available. For more information about any module-specific polling settings, see your SolarWinds NPM Administrator Guide.

Default Node Topology Poll Interval

Topology data are regularly polled on this interval. By default, this interval is 30 minutes. To reduce network load, you may want to increase this polling interval.

Default Node Statistics Poll Interval

Device performance statistics are regularly polled on this interval. By default, this interval is 10 minutes.

Default Interface Statistics Poll Interval

Interface performance statistics are regularly polled on this interval. By default, this interval is 9 minutes.

Default Volume Statistics Poll Interval

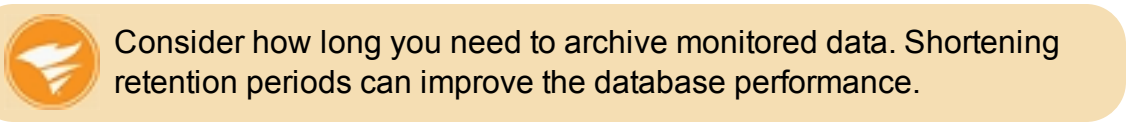
Volume performance statistics are regularly polled on this interval. By default, this interval is 15 minutes.

Dynamic IP Address and Hostname Resolution

The **Default IP Address Resolution** setting determines the type of IP address resolution that is used when a dual-stack monitored device returns both IPv4 and IPv6 addresses. By default, IPv4 is used.

Database Settings

The following options configure Orion database maintenance and retention settings.



Archive Time

The Archive Time is the time of day when Orion database maintenance occurs. For more information, see Database Maintenance.

Auditing Trails Retention

All audit trails data is kept for the period of time designated as the Auditing Trails Retention period. By default, this period is 365 days.

Detailed Statistics Retention

All statistics collected on any basis shorter than 1 hour are summarized into hourly statistics after the period of time designated as the Detailed Statistics Retention period. By default, this period is 7 days. This setting specifies the retention period for node statistics such as availability and response time.

Hourly Statistics Retention

All statistics collected on any basis shorter than 1 day but longer than 1 hour are summarized into daily statistics after the period of time designated as the Hourly Statistics Retention period. By default, this period is 30 days. This setting specifies the retention period for node statistics such as availability and response time.

Daily Statistics Retention

All statistics in the Orion database that are collected on a daily basis are kept for this designated period of time. By default, this period is 365 days. This setting specifies the retention period for node statistics such as availability and response time.

Baseline Data Collection Duration

This setting specifies the number of days of data that will be included in the baseline. The default is 7 days. The value specified here should not be greater than the value specified in the Detailed Statistics Retention setting. This setting applies to nodes and interfaces as well.

Interface Baseline Calculation Frequency

The frequency with which the interface baseline calculation is performed. The baseline for nodes is calculated every time when database maintenance is performed.

Detailed Interface Availability Statistics Retention

All interface statistics collected on any basis shorter than 1 hour are summarized into hourly statistics after the period of time designated as the Detailed Interface Availability Statistics Retention period. By default, this period is 7 days.

Hourly Interface Availability Statistics Retention

All interface statistics collected on any basis shorter than 1 day but longer than 1 hour are summarized into daily statistics after the period of time designated as the Hourly Interface Statistics Retention period. By default, this period is 30 days.

Daily Interface Availability Statistics Retention

All interface statistics in the Orion database that are collected on a daily basis are kept for this designated period of time. By default, this period is 365 days.

Detailed Wireless Statistics Retention

All wireless statistics collected on any basis shorter than 1 hour are summarized into hourly statistics after the period of time designated as the Detailed Wireless Statistics Retention period. By default, this period is 3 days.

Hourly Wireless Statistics Retention

All wireless statistics collected on any basis shorter than 1 day but longer than 1 hour are summarized into daily statistics after the period of time designated as the Hourly Wireless Statistics Retention period. By default, this period is 14 days.

Daily Wireless Statistics Retention

All wireless statistics in the Orion database that are collected on a daily basis are kept for this designated period of time. By default, this period is 180 days.

Detailed UnDP Statistics Retention

All UnDP statistics collected on any basis shorter than 1 hour are summarized into hourly statistics after the period of time designated as the Detailed UnDP Statistics Retention period. By default, this period is 3 days.

Hourly UnDP Statistics Retention

All UnDP statistics collected on any basis shorter than 1 day but longer than 1 hour are summarized into daily statistics after the period of time designated as the Hourly UnDP Statistics Retention period. By default, this period is 14 days.

Daily UnDP Statistics Retention

All UnDP statistics in the Orion database that are collected on a daily basis are kept for this designated period of time. By default, this period is 180 days.

Events Retention

All network events data is deleted from the Orion database after the period of time designated by the Events Retention has passed after the event ending time. By default, this period is 30 days.

Syslog Messages Retention

All received Syslog messages are kept for the period of time designated. By default, this period is 7 days.

Trap Messages Retention

All received trap messages are kept for the period of time designated. By default, this period is 30 days.

Max Alert Execution Time

If it takes longer than the value specified here for an alert to execute, Orion will disable the alert. Alert execution time includes the amount of time required to trigger any configured alert actions.

Alert Acknowledge URL Text

Users with alert acknowledgment rights will see the text provided as a link to acknowledge an associated alert.

Allow alert actions for unmanaged objects

If this option is enabled, the Alerting Engine will execute alert actions for all monitored objects that trigger alerts, including monitored objects that are temporarily unmanaged. By default, this option is disabled.

Discovery Retention

All configured discovery profiles are kept for the period of time designated. By default, this period is 60 days. For more information about discovery profiles, see Discovering and Adding Network Devices.

Downtime History Retention

All records of downtime is retained in your database for the period of time designated. By default, this period is 30 days.

Network

The following settings configure ICMP and SNMP requests.

ICMP Timeout

All ICMP (ping) requests made by the Orion poller time out if a response is not received within the period designated. By default, this period is 2500ms.

ICMP Data

This string is included within all ICMP packets sent by Orion.

SNMP Timeout

All SNMP requests made by the Orion poller time out if a response is not received within the period designated. By default, this period is 2500ms.

SNMP Retries

If a response to an SNMP poll request made by the Orion poller is not received within the configured SNMP Timeout, the Orion poller will conduct as many retries as designated by this value. By default, this value is 2.

UCS API Timeout

All UCS API requests made by the Orion poller time out if a response is not received within the period designated. By default, this period is 240 seconds.

Perform reverse DNS lookup

If you want Orion to perform reverse DNS lookups on monitored DHCP nodes, confirm that this option is checked. By default, reverse DNS lookup for DHCP nodes is enabled.

Calculations & Thresholds

The following settings designate methods for calculating availability and transmission rate baselines, select the node warning level and counter type, and indicate security preferences for community strings and other potentially sensitive information in the web console.

Availability Calculation (advanced)

This setting designates the type of calculation performed to determine device availability. For more information, see Calculating Node Availability.

Baseline Calculation (advanced)

When enabled, baselines for the transmission rates of the various elements of your network are calculated upon startup. This baseline is used as a starting point for any comparison statistics. For more information, see Calculating a Baseline.

Enable Auto Dependencies

This settings allows your SolarWinds Orion server to collate topology information from your networked devices and create dependency links between relevant devices.

Allow Secure Data on Web (advanced)

In the interest of security, sensitive information about your network is not available in the Orion Web Console. If your network is properly secured, check this option to allow users to view community strings and other potentially sensitive information within the web console.

Note: This setting does not affect the display of custom reports that you export to the web.

Node Warning Level

Devices that do not respond to polling within this designated period of time display as Down in the web console. By default, this value is 120 seconds.

Counter Rollover

This option sets the type of counter used. For more information, see Handling Counter Rollovers.

Default Assigned IP Address

In the event that DNS resolution fails for a monitored node, the IP address provided in this setting will be recorded as the node IP address. If blank, no IP address will be stored.

Disable HTML Encoding for Polled Data

HTML encoding provides added security for polled data in the web console.

Calculating Node Availability

The Availability Calculation setting on the Orion Polling Settings view provides a choice between the following two methods for determining device availability.

Node Status

The default method is based upon the historical up or down status of the selected node. The selected node is polled for status on the Default Node Poll Interval defined on the Orion Polling Settings view. For more information, see Orion Polling Settings.

If the selected node responds to a ping within the default interval, the node is considered up, and a value of **100** is recorded in the Response Time view. If the node does not respond to a ping within the default interval, the node is considered down and a value of **0** is recorded in the Response Time view. To calculate node availability over a selected time period, the sum of all Response Time table records for the selected node over the selected time period is divided by the selected time period, providing an average availability over the selected time period.

Percent Packet Loss

The second method is a more complicated calculation that effectively bases the availability of a selected node on its packet loss percentage. As in the Node Status method, the selected node is polled for status. If it responds within the Default Node Poll Interval defined on the Orion Polling Settings view, a value of **100** is averaged with the previous 10 availability records. For more information, see Orion Polling Settings.

The result of the Percent Packet Loss calculation is a sliding-window average. To calculate node availability over a selected time period, the sum of all results in the Response Time table for the selected node over the selected time period is divided by the selected time period, providing an average availability over time.

Note: The Percent Packet Loss method introduces a historical dependency into each availability node record. In general, it is best to leave calculations based on Node Status unless you specifically need node availability based on packet loss.

Calculating a Baseline

Much of the raw data that Orion polls from monitored network objects is provided initially as counter values. For example, one of the values that SolarWinds NPM polls from interfaces is **ifInOctets**, which returns the number of bytes the polled interface has received since the device last booted. While this value can be useful information in itself, generally, from a network performance monitoring standpoint, it is more useful to know the rate of bytes received by the interface.

In order to determine a rate, two values are required. On a new install or after a shutdown, when the SolarWinds Network Performance Monitor service starts, there is no current network data in your Orion database. In this situation, by default, your SolarWinds Orion server calculates a baseline for the transmission rates of the various elements of your network. To calculate this baseline, all network resources are polled immediately upon startup, and then, as soon as the initial poll is complete, the network is polled again.

The resulting two sets of data are used to calculate a performance baseline. If you do not need statistics immediately, or if you do not want your SolarWinds Orion server to calculate a baseline at startup, disable baseline calculation by setting the Baseline Calculation option to **False**. For more information about configuring the settings on this view in addition to configuring all other available polling engine variables, see Configuring Polling Engine Settings.

Note: Baseline calculation requires significant data gathering and processing. Until baseline calculation is completed, both SolarWinds Orion server performance and the CPU performance of some of network routers may be adversely affected.

Orion Baseline Data Calculation

Using the baselining feature, you can display baselines on different charts in the Orion Web Console. In the Orion Web Console, you can define general static thresholds for every entity, and you can base alerts on the global static thresholds. However, you can also override the global threshold, and specify a custom dynamic baseline threshold on an entity per entity basis.

The baseline is calculated based on the normal historical distribution of data, taking the mean and standard deviations into account. Baselines can be used to detect and alert on deviations from the average values. Baselines can be calculated automatically, and can be applied as soon as sufficient statistical data becomes available. You can also recalculate baselines on demand.

SolarWinds Orion platform products have always provided performance statistics and threshold comparisons in the web console to give you a clear picture of network performance. In any sort of performance analysis baselines are critical to establishing useful and valid performance benchmarks and expectations against which current performance can be measured. Statistical baseline data calculation is a feature that significantly improves the accuracy and validity of established performance benchmarks. As a result, the Orion Web Console can provide better quality information. By performing statistical analysis on collected data, SolarWinds is able to provide data that is both more accurate and better able to indicate when and where there are performance issues on your network. The baseline statistics are recalculated on a custom basis, and they are used to define thresholds for use in web console charts and alerts.

What Data is Affected?

The following types of data are subject to statistical baseline data calculation:

Nodes	Interfaces	Volumes
CPU Load	Received (Incoming) Errors & Discards	Percent Disk Usage
Percent Memory Used	Transmitted (Outgoing) Errors & Discards	
Response Time	Received (Incoming) Percent Utilization	

Nodes	Interfaces	Volumes
Percent Loss	Transmitted (Outgoing) Percent Utilization	

When Are Baselines Calculated?

By default, node baseline calculations are performed daily, and interface baseline calculations are performed weekly, on Sunday. Only the interface baseline calculation schedule may be edited in the Database Settings section of the Orion Polling Settings view. The node baseline calculation schedule is not customizable.

To customize the schedule of interface baseline data calculation:

1. Log in to the Orion Web Console using an account with administrative privileges.
2. Click **Settings** in the top right.
3. In the Settings grouping, click **Polling Settings**.
4. Under the Database Settings, select the desired **Interface Baseline Calculation Frequency**.
5. If you want to change the default amount of data that is used to make the interface baseline calculation, enter the desired number of days to include as the **Baseline Data Collection Duration**.
   Note: The **Baseline Data Collection Duration** cannot exceed the **Detailed Statistics Retention** that is configured in the same section.
6. Click **Submit**.

Why Are Only Interface Baselines Customizable?

In most monitored environments, the number of monitored interfaces is much larger than the number of nodes. Performing daily baseline calculations on nodes will not, in most environments, potentially affect performance as much as performing the same calculations for all monitored interfaces.

Setting the Node Warning Level

A device may drop packets or fail to respond to a poll for many reasons. Should the device fail to respond, the device status is changed from Up to Warning. On the Orion Polling Settings view, you can specify the Node Warning Level, which is the length of time a device is allowed to remain in the Warning status before it is marked as Down. During the interval specified, the service performs "fast polling" to continually check the node status.

Note: You may see events or receive alerts for down nodes that are not actually down. This can be caused by intermittent packet loss on the network. Set the Node Warning Interval to a higher value to avoid these false notifications. For more information about packet loss reporting, see Managing Packet Loss Reporting.

To set the Node Warning Level:

1. Log in to the Orion Web Console using an account with administrative rights.
2. Click **Settings** in the upper right of the web console, and then click **Polling Settings** in the Settings group of the Orion Website Administration view.
3. In the Calculations and Thresholds group, set the Node Warning Level to an appropriate interval, in seconds.

   Note: The default Node Warning Level interval is 120 seconds.
4. Click **Submit**.

Managing Packet Loss Reporting

To manage the amount of network-wide packet loss reported by Orion, configure the Response Time Retry Count for your polling engine. This setting designates the number of times Orion retries ICMP pings on a monitored device before packet loss is reported.

Note: This configuration change requires an insertion into your Orion database. If possible in your environment, SolarWinds recommends installing and using the SQL Server Management Studio to perform this insertion.

To configure the Response Time Retry Count for your polling engine:

1. Create a full backup of your Orion database.
2. On your Orion server, click **Start > All Programs > SolarWinds Orion > Advanced Features > Orion Service Manager**.
3. Click **Shutdown Everything**.
4. On your Orion database server, click **Start > All Programs > Microsoft SQL Server > SQL Server Management Studio**.
5. Select your Orion database **Server name**.
6. Select an appropriate **Authentication** type, provide any required credentials, and then click **Connect**.
7. Expand **Databases > *OrionDatabaseName* > Tables**, and then click **New Query**.
8. Type the following query into the empty SQL query field:
   Note: Specify your own custom values for Maximum, CurrentValue, and DefaultValue.

   INSERT INTO [OrionDatabaseName].[dbo].[Settings] (SettingID, Name, Description, Units, Minimum, Maximum, CurrentValue, DefaultValue) VALUES ('SWNetPerfMon-Settings-Response Time Retry Count', 'Response Time Retry Count', 'Number of times Orion retries ICMP pings on a monitored device before reporting packet loss', '', 1, Maximum, CurrentValue, DefaultValue**)**
9. Click **Execute**, and then close SQL Server Management Studio.
10. Click **Start > All Programs > SolarWinds Orion > Advanced Features >**

Orion Service Manager.

11. Click **Start Everything**.

Deleting Polling Engines

If there are any polling engines in your SolarWinds environment that are not currently assigned any monitored objects, you can delete them directly from the Polling Engine details view.

Notes:

- This method for deleting polling engines from your SolarWinds environment is only available for polling engines to which there are no longer any assigned objects for monitoring.
- If you want to delete an existing polling engine to which monitored objects are currently assigned, use Node Management to reassign monitored objects to other polling engines, as necessary, and then delete the polling engine as indicated in this procedure.

To delete a polling engine:

1. Log in to the Orion Web Console as a user with administrative rights.
2. Click **Settings** in the top right of the web console.
3. Click **Polling Engines** in the Settings group.
4. ***If the Elements listing for the polling engine you want to delete reports "0 elements assigned",*** click **Delete unused polling engine**.
5. Confirm the polling engine deletion by clicking **Yes, delete.**

Using Additional Polling Engines

Because larger networks can quickly become too extensive for a single SolarWinds NPM polling engine to adequately monitor, Additional Polling Engines are available to increase the monitoring capacity of your SolarWinds NPM installation by enabling multiple monitoring engines that work in parallel across your network.

Required Settings

If you have an additional polling engine, you need to add its IP address to Windows Servers on the Security tab.

Make sure that the following options are set:

- Ensure that a case-sensitive community name has been specified.
- Ensure that **Accept SNMP packets from any host** is selected OR ensure that the ipMonitor system is listed within the **Accept SNMP packets from these hosts** list.
- Ensure that your network devices allow SNMP access from the new polling engine. On Cisco devices, you can for example modify the Access Control List.

Note: In SolarWinds NPM 10.2 and higher, Additional Polling Engines no longer require that the primary SolarWinds NPM polling engine in your environment is also running to support data collection for Universal Device Pollers, and EnergyWise, ESX Server, and wireless devices.

Additional Polling Engine Guidelines

The following table provides guidance for SolarWinds NPM installations that use scalability engines to expand monitoring capacity.

Network Performance Monitor (NPM) Scalability Engine Guidelines	
Stackable Pollers Available?	Yes. Up to three total polling engines may be installed on a single server (i.e. one primary NPM polling engine with one or two additional polling engines or three additional polling engines on the same server).

Network Performance Monitor (NPM) Scalability Engine Guidelines	
	Note: A stack requires only 1 IP address for any number of APEs
Poller Remotability Available?	Yes, for NPM versions 10.4 and higher Note: Poller remotability is a feature enabling the local storage, using MSMQ, of up to ~1 GB of polled data per poller in case the connection between the polling engine and the database is temporarily lost.
Primary Poller Limits	~12k elements at standard polling frequencies: • Node and interface up/down: 2 minutes/poll • Node statistics: 10 minutes/poll • Interface statistics: 9 minutes/poll 25-50 concurrent Orion Web Console users SNMP Traps: ~500 messages per second (~1.8 million messages/hr) Syslog: 700-1k messages/second (2.5 - 3.6 million messages/hr) Note: If you are monitoring more than ~100,000 elements, consider using SolarWinds Enterprise Operations Console.
Scalability Options	One polling engine for every ~12k elements Maximum of 100k elements per primary SolarWinds NPM server (i.e. 1 NPM server + 9 APEs). For more information about licensing, see "How is SolarWinds NPM licensed?"
WAN and/or Bandwidth Considerations	Minimal monitoring traffic is sent between the primary NPM server and any APEs that are connected over a WAN. Most traffic related to monitoring is between an APE and the SolarWinds database.

Additional Polling Engine System Requirements

System requirements for an Additional Polling Engine are the same as system requirements for a primary NPM polling engine. For more information about system requirements, see SolarWinds NPM Requirements.

Notes:

- NPM is not able to add nodes to an Additional Polling Engine if DNS cannot resolve the name of the server hosting the Additional Polling Engine.
- SNMP access must be allowed to all SolarWinds polling engines. For more information, see the installation instructions in the Administrator Guide for your SolarWinds product.
- If you are using basic alerts supported in SolarWinds NPM 11.0.1 and previous versions, please note that basic alerts are configured and managed from your primary SolarWinds server. If there are multiple polling engines in your environment, the Basic Alert Manager on your primary SolarWinds server will give you the opportunity to select the engine that is monitoring the devices to which you want the basic alert to apply. For more information, see Configuring Basic Alerts in the SolarWinds NPM online help.

Installing Additional Polling Engines

The installation and initial configuration of a new Additional Polling Engine follows the same steps as the installation and configuration of a primary SolarWinds polling engine, with the following additional considerations:

- The most recent installer is available in your SolarWinds Customer Portal within the **Orion_Additional_Polling_Engine_**version**.zip** archive.
- If you want to monitor or manage devices polled by an additional polling engine in any Orion module, you must install the additional polling engine for the appropriate module. For more information, see the SolarWinds documentation for your Orion module.
- Individual licenses must be activated for each polling engine in a stackable poller installation.
- If you have configured an alert with a Send Email action to trigger on a node monitored by an additional polling engine, confirm that the additional polling engine has access to your SMTP server.

To install an Orion Additional Polling Engine:

1. Launch the appropriate executable, which you have downloaded from the SolarWinds website.
   Notes:
   - The executable extracts to a folder containing an HTML readme, an Installer Guide, and Additional Polling Engine installers for all Orion products that support Additional Polling Engines.
   - Launch the installer that corresponds to the SolarWinds product installed on your primary SolarWinds NPM server.
   - If you have multiple Orion products installed on your primary SolarWinds NPM server, install the additional polling engine for each product to ensure full functionality.
2. On the Welcome window of the Compatibility Check, provide the following information:
   - The **Hostname or IP Address** of your primary SolarWinds NPM server.
   - The **User name** and **Password** of a user with administrative privileges to the Orion Web Console on your primary SolarWinds NPM server.
3. Click **Next**, and then complete the installation as you would on a primary SolarWinds NPM server.

Upgrading an Additional Polling Engine

Upgrading an Additional Polling Engine follows the same steps required to upgrade a primary NPM polling engine. For more information, see Upgrading SolarWinds Network Performance Monitor.

Notes:

- The most recent installer is available in your SolarWinds Customer Portal within the **Orion_Additional_Polling_Engine_version.zip** archive.
- Confirm that you have upgraded your main Orion server before you upgrade your Additional Polling Engine.

- If you are upgrading an Additional Polling Engine that is currently in service, the Additional Polling Engine will shutdown temporarily with the result that you may lose some polling data. SolarWinds recommends that you perform any Additional Polling Engine upgrades during off-peak hours.

Configuring an Additional Polling Engine

Configuration typically occurs after an initial installation, but it may also be required when a non-standard configuration change is made or when a module is added to your Additional Polling Engine.

In general, the steps to configure an Additional Polling Engine are the same as those required to configure a primary NPM polling engine, with the following additional considerations:

- If you are using custom properties to monitor your network, you must copy related schema (***.schema**) and configuration (***.config** and ***.cfg**) files from your primary Orion server to the server hosting your Additional Polling Engine.

  Note: By default, ***.schema** files are located on your primary SolarWinds server in **C:\Program Files\SolarWinds\Orion\Schemas**; ***.config** and ***.cfg** files are located in **C:\Program Files\SolarWinds\Orion**.

- If you are using any basic alerts to monitor your network, you must make copies of all basic alert definitions in your Orion database, and then assign the copies to your Additional Polling Engine.
- If you want to use any Orion modules for monitoring or managing any devices polled with an Additional Polling Engine, you must install the Additional Polling Engine version of the module you want to use on the server hosting your Additional Polling Engine.

For more information about optimizing an additional polling engine configuration, see Managing Orion Polling Engines.

Note: During configuration, the Additional Polling Engine will shutdown temporarily with the result that, if you are actively polling, you may lose some data. SolarWinds recommends configuring polling engines during off-peak hours.

Changing Polling Engine Node Assignments

Reassigning nodes to new polling engines may be required in the following situations:

- Moving or renaming your NPM server
- Deleting an existing polling engine
- Merging two or more Orion servers

If these or any other conditions present the need for reassignment, complete the following procedure to reassign nodes to a new polling engine.

To change a polling engine node assignment:

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 Nodes** in the Node & Group Management grouping.
3. Locate the node to manage using either of the following methods:
    - Use the search tool above the node list to search your Orion database for the device you want to manage.
    - Select an appropriate **Group by** criteria, and then click the appropriate group including the node to manage.
4. Check the node for which you want to change the polling engine.
5. Click **More Actions**, and then click **Change Polling Engine**.

    Note: The current number of Assigned Objects is listed for each available polling engine. This number is updated with each automatic polling engine synchronization. Updates to the Assigned Objects count can only be completed for polling engines that are operationally up.

6. Select the new polling engine, and then click **Change polling engine**.

Chapter 26: Using Orion Scalability Engines

Orion scalability engines, including Additional Polling Engines and Additional Web Servers, can extend the monitoring capacity of your SolarWinds installation.

Requirements and recommendations will vary from product to product. Refer to the Administrator Guide for your specific product for more information.

Scalability Engine Requirements

Scalability engine requirements are generally the same as the requirements for a primary polling engine. For more information, see SolarWinds NPM Requirements.

Note: SNMP access must be allowed to all SolarWinds polling engines. For more information, see the installation instructions in the Administrator Guide for your SolarWinds product.

Scalability Engine Guidelines by Product

The following sections provide guidance for using scalability engines to expand the capacity of your SolarWinds installation.

Note: Requirements and recommendations will vary from product to product. Refer to the Administrator Guide for your specific product for more information.

- Network Performance Monitor (NPM)
- Enterprise Operations Console (EOC)
- Server & Application Monitor (SAM)
- NetFlow Traffic Analyzer (NTA)
- Network Configuration Manager (NCM)
- User Device Tracker (UDT)
- Storage Resource Monitor (SRM)
- VoIP & Network Quality Manager (VNQM)
- Web Performance Monitor (WPM)
- IP Address Manager (IPAM)
- Engineer's Toolset on the Web
- DameWare in Centralized Mode
- Serv-U FTP Server and MFT Server
- Log and Event Manager (LEM)
- Virtualization Manager (vMan)
- Quality of Experience (QoE)
- Database Performance Analyzer (DPA)
- Patch Manager (SPM)

Network Performance Monitor (NPM)

Network Performance Monitor (NPM) Scalability Engine Guidelines	
Stackable Pollers Available?	Yes. Up to three total polling engines may be installed on a single server (i.e. one primary NPM polling engine with one or two additional polling engines or three additional polling engines on the same server). **Note**: A stack requires only 1 IP address, regardless of the number of APEs
Poller Remotability Available?	Yes, for NPM versions 10.4 and higher Note: Poller remotability is a feature that enables the local storage, using MSMQ, of up to ~1 GB of polled data per poller in the event that the connection between the polling engine and the database is temporarily lost.
Primary Poller Limits	~12k elements at standard polling frequencies: • Node and interface up/down: 2 minutes/poll • Node statistics: 10 minutes/poll • Interface statistics: 9 minutes/poll 25-50 concurrent Orion Web Console users SNMP Traps: ~500 messages per second (~1.8 million messages/hr) Syslog: 700-1k messages/second (2.5 - 3.6 million messages/hr) Note: If you are monitoring more than ~100,000 elements, consider using SolarWinds Enterprise Operations Console.
Scalability Options	One polling engine for every ~12k elements Maximum of 100k elements per primary SolarWinds NPM server (i.e. 1 NPM server + 9 APEs). For more information about licensing, see "How is SolarWinds NPM licensed?"

Network Performance Monitor (NPM) Scalability Engine Guidelines	
WAN and/or Bandwidth Considerations	Minimal monitoring traffic is sent between the primary NPM server and any APEs that are connected over a WAN. Most traffic related to monitoring is between an APE and the SolarWinds database.
Other Considerations	How much bandwidth does SolarWinds require for monitoring? For hardware requirements, see Orion Server Hardware Requirements in the SolarWinds Orion NPM Administrator Guide.

Enterprise Operations Console (EOC)

Enterprise Operations Console (EOC) Scalability Engine Guidelines	
Stackable Pollers Available?	No
Poller Remotability Available?	No
Primary Poller Limits	25k elements per Orion server
Scalability Options	Maximum of 25k elements per Orion server Maximum 1 million elements on 75 primary SolarWinds NPM servers (i.e. 1 NPM server + 1 APE). For more information, see Network Performance Monitor (NPM).
WAN and/or Bandwidth Considerations	Minimal monitoring traffic is sent between the primary NPM server and any APEs that are connected over a WAN. Most traffic related to monitoring is between an APE and the SolarWinds database.
Other Considerations	See "Section 4 — Deployment Strategies" of NetFlow Basics and Deployment Strategies

Server & Application Monitor (SAM)

Server & Application Monitor (SAM) Scalability Engine Guidelines	
Stackable Pollers Available?	Yes, for SAM version 6.2 and higher. Two polling engines can be installed on a single server
Poller Remotability Available?	Yes, for SAM versions 5.5 and higher **Note**: Poller remotability is a feature that enables the local storage, using MSMQ, of up to ~1 GB of polled data per poller in the event that the connection between the polling engine and the database is temporarily lost.
Primary Poller Limits	~8-10k component monitors per polling engine 25-50 concurrent Orion Web Console users
Scalability Options	One APE for every 8-10k component monitors Maximum of 150k component monitors per primary SolarWinds SAM installation (i.e. 1 SAM server + 4 APEs). You can use up to 14 APEs. For more information about licensing, see Why are you licensing by monitors instead of by servers?
WAN and/or Bandwidth Considerations	Minimal monitoring traffic is sent between the primary SAM server and any APEs that are connected over a WAN. Most traffic related to monitoring is between an APE and the SolarWinds database. Bandwidth requirements depend on the size of the relevant component monitor. Based on 67.5 kB / WMI poll and a 5 minute polling frequency, the estimate is 1.2 Mbps for 700 component monitors. For more information, see How do SNMP and WMI polling compare? Note: WMI is best suited for environments where latency is < 100ms.
Other Considerations	WMI Security Blog

NetFlow Traffic Analyzer (NTA)

NetFlow Traffic Analyzer (NTA) Scalability Engine Guidelines	
Stackable Pollers Available?	No
Poller Remotability Available?	No
Primary Poller Limits	For more information, see Network Performance Monitor (NPM).
Scalability Options	For more information, see Network Performance Monitor (NPM).
WAN and/or Bandwidth Considerations	1.5 - 3% of total traffic seen by exporter
Other Considerations	See "Section 4 — Deployment Strategies" of NetFlow Basics and Deployment Strategies

Network Configuration Manager (NCM)

Network Configuration Manager (NCM) Scalability Engine Guidelines	
Stackable Pollers Available?	No
Poller Remotability Available?	No
Primary Poller Limits	~10k devices
Scalability Options	One APE for every 10k devices, for NCM versions 7.1 and higher Maximum of 30k devices per primary SolarWinds NCM instance (i.e. NCM server + 2 NCM APEs) Integrated standalone mode

Network Configuration Manager (NCM) Scalability Engine Guidelines	
WAN and/or Bandwidth Considerations	None
Other Considerations	None

User Device Tracker (UDT)

User Device Tracker (UDT) Scalability Engine Guidelines	
Stackable Pollers Available?	No
Poller Remotability Available?	No
Primary Poller Limits	100k ports
Scalability Options	One APE per 100k additional ports Maximum of 500k port per instance (1 main poller and 4 additional)
WAN and/or Bandwidth Considerations	None
Other Considerations	UDT version 3.1 supports the ability to schedule port discovery. In UDT version 3.1 the Max Discovery Size is 2,500 nodes/150,000 ports

Storage Resource Monitor (SRM)

Storage Resource Monitor (SRM) Scalability Engine Guidelines	
Stackable Pollers Available?	No. One APE instance can be deployed on a single host.

Storage Resource Monitor (SRM) Scalability Engine Guidelines	
Poller Remotability Available?	Yes **Note**: Poller remotability is a feature enabling the local storage, using MSMQ, of up to ~1 GB of polled data per poller in case the connection between the polling engine and the database is temporarily lost.
Primary Poller Limits	10k disk per poller 25-50 concurrent Orion Web Console users
Scalability Options	1 APE per 10k disk polled
WAN and/or Bandwidth Considerations	Minimal monitoring traffic is sent between the primary SRM server and any APEs that are connected over a WAN. Most traffic related to monitoring is between an APE and the SolarWinds database.

VoIP & Network Quality Manager (VNQM)

VoIP & Network Quality Manager Scalability Engine Guidelines	
Stackable Pollers Available?	No
Poller Remotability Available?	No
Primary Poller Limits	~5,000 IP SLA operations ~200k calls/day with 20k calls/hour spike capacity
Scalability Options	One APE per 5,000 IP SLA operations and 200,000 calls per day Maximum of 15,000 IP SLA operations and 200,000 calls per day per SolarWinds VNQM instance (i.e. SolarWinds VNQM + 2 VNQM APEs)

VoIP & Network Quality Manager Scalability Engine Guidelines	
WAN and/or Bandwidth Considerations	Between Call Manager and VNQM: 34 Kbps per call, based on estimates of ~256 bytes per CDR and CMR and based on 20k calls per hour
Other Considerations	None

Web Performance Monitor (WPM)

Web Performance Monitor (WPM) Scalability Engine Guidelines	
Stackable Pollers Available?	No
Poller Remotability Available?	No, but recordings may be made from multiple locations
Primary Poller Limits	Dozens of recordings per player
Scalability Options	One APE per dozens additional recordings, with the complexity of transactions determining the limits per player
WAN and/or Bandwidth Considerations	None
Other Considerations	None

IP Address Manager (IPAM)

IP Address Manager (IPAM) Scalability Engine Guidelines	
Scalability Options	3 million IPs per SolarWinds IPAM instance

Engineer's Toolset on the Web

Engineer's Toolset on the Web Scalability Engine Guidelines	
Scalability Options	45 active tools per Engineer's Toolset on the Web instance 3 tools per user session 1 active tool per mobile session 10 nodes monitored at the same time per tool 48 interfaces monitored at the same time per tool 12 metrics rendered at same time per tool

DameWare in Centralized Mode

DameWare Scalability Engine Guidelines	
Scalability Options	150 concurrent Internet Sessions per Internet Proxy 5,000 Centralized users per Centralized Server 10,000 Hosts in Centralized Global Host list 5 MRC sessions per Console

Serv-U FTP Server and MFT Server

Serv-U FTP Server and MFT Server Scalability Engine Guidelines	
Scalability Options	500 simultaneous FTP and HTTP transfers per Serv-U instance 50 simultaneous SFTP and HTTPS transfers per Serv-U instance For more information, see the Serv-U Distributed Architecture Guide.

Log and Event Manager (LEM)

Log and Event Manager (LEM) Scalability Engine Guidelines	
Scalability Options	Maximum 120 million events per day 10,000 rule hits per day

Virtualization Manager (vMan)

Virtualization Manager (vMan) Scalability Engine Guidelines	
Scalability Options	3000 VMs* 700 Hosts 75 Clusters 1800 Datastores *By using federated collectors, you can monitor 10,000 or more VMs. For information about federated collectors, see the Virtualization Manager documentation.

Quality of Experience (QoE)

Quality of Experience (QoE) Scalability Engine Guidelines	
Scalability Options	1,000 QoE sensors 50 application per sensor

Database Performance Analyzer (DPA)

Database Performance Analyzer (DPA) Scalability Engine Guidelines	
Scalability Options	Less than 20 database instances monitored on a system with 1 CPU and 1 GB RAM 20-50 database instances monitored on a system with 2 CPU and 2 GB RAM 51-250 database instances monitored on a system with 4 CPU and 4 GB RAM

Patch Manager (SPM)

Patch Manager (SPM) Scalability Engine Guidelines	
Scalability Options	1,000 nodes per automation server 1,000 nodes per SQL Server Express instance (SQL Server does not have this limitation)

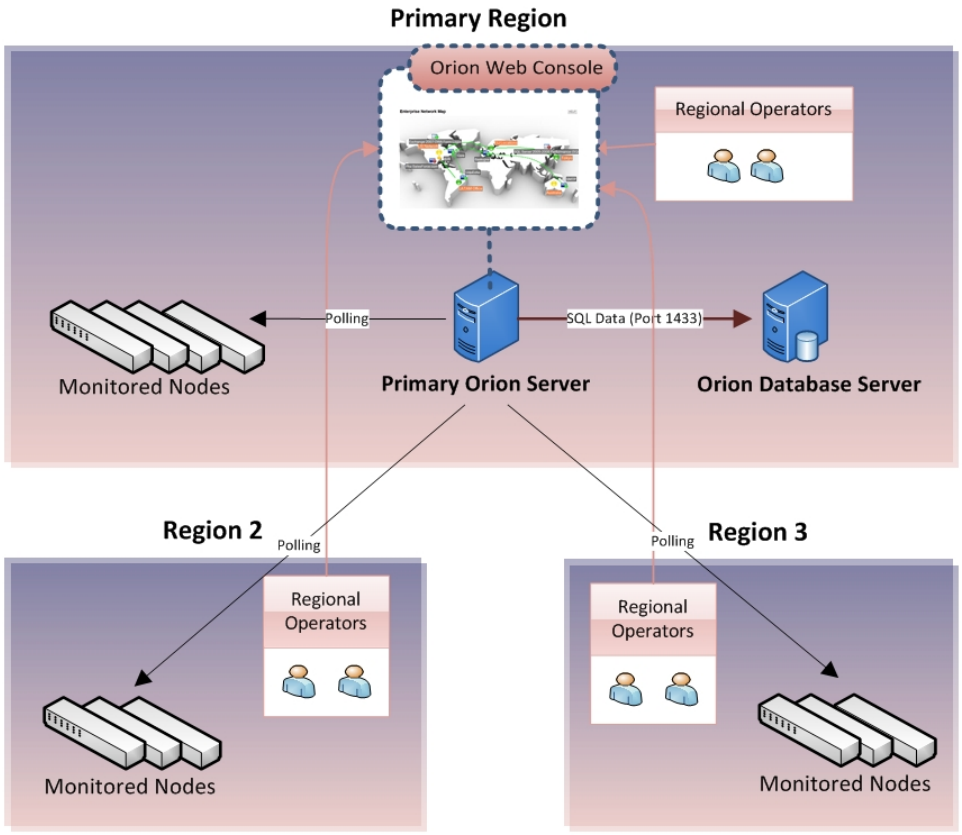
Scalability Engine Deployment Options

The following sections discuss common scalability engine deployment options:

Centralized Deployment

This is the simplest deployment option, as there is only one SolarWinds Orion server, and software is only installed in the Primary region. This option is well suited to environments where most of the monitored nodes are located in a single, primary region and where other regional offices are much smaller. This deployment is optimal when the following conditions apply:

1. The remote office is not large enough to require a local SolarWinds Orion server instance or polling engine.
2. There are not enough monitored nodes to require a local SolarWinds Orion server instance or polling engine.
3. You prefer to have a central point of administration for the SolarWinds Orion server.



In a typical centralized deployment, the primary SolarWinds Orion server polls all data that is then stored centrally in the database server. Both the primary SolarWinds Orion server and the database server are in the Primary Region. To view data Regional Operators in each region must log into the Orion Web Console in the primary region, where your Orion platform products are installed. Additional Web Servers are available and may be installed in secondary regions. If an Additional Web Server is deployed, a Regional Operator can log into a local web console to view all network data.

A reliable static connection is required between the primary region and all monitoring regions. This connection continually transmits monitoring data. The quantity of bandwidth consumed will depend on many factors, including the type and number of SolarWinds Orion platform products that are installed and the types and quantity of monitored elements. It is difficult to precisely estimate bandwidth requirements, as each SolarWinds monitoring environment is unique.

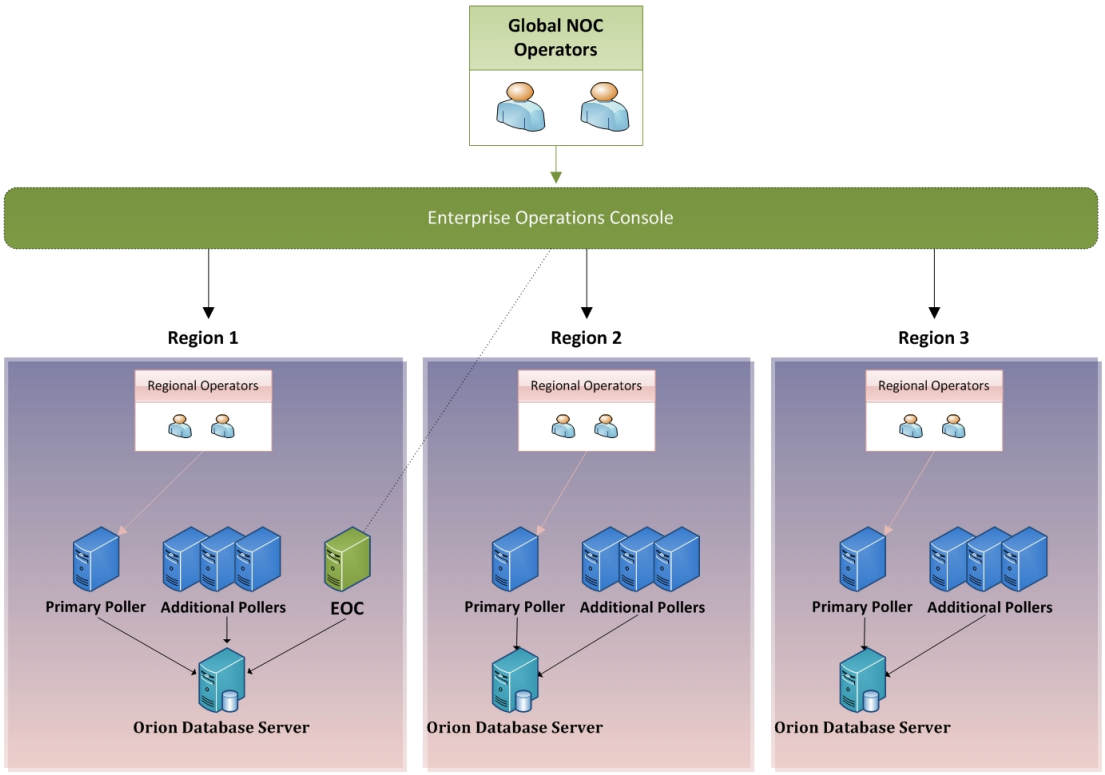
Notes:

- All nodes are polled from a single SolarWinds Orion server instance in the Primary Region, and all data is stored centrally on the database server in the primary region.
- Each installed module will need to have enough available licenses to cover all regions.
- All KPI's, such as Node Response Times, will be calculated from the perspective of the Primary Orion Server. For example, the response time for a monitored node in Region 2 will be equal to the round trip time from the Primary Orion Server to that node.

Distributed Deployment

This is the traditional SolarWinds Orion distributed deployment option, comprising separate instances of SolarWinds Orion platform products installed locally in each region with the Enterprise Operations Console (EOC) available as a top level dashboard to access data across all related instances.

This option is well suited to organizations with multiple regions or sites where the quantity of nodes to be monitored in each region would warrant both localized data collection and storage. It works well when there are regional teams responsible for their own environments, and when regional teams need autonomy over their monitoring platform. This option gives regional operators this autonomy and the ability to have different modules and license sizes installed in each region to match individual requirements. While the systems are segregated between regions, all data can still be accessed from the centrally located Enterprise Operations Console (EOC).



Each region is licensed independently, and data are polled and stored locally in each region. Modules and license sizes may be mixed and matched accordingly. In the example provided,

- Region 1 has deployed NPM SLX, SAM AL1500, UDT 50,000, and three additional polling engines
- Region 2 has deployed NPM SL500, NTA for NPM SL500, UDT 2500, and three additional polling engines
- Region 3 has deployed NPM SL100 only and three additional polling engines

As in this example, if EOC is used as a centralized dashboard to access data stored regionally, the following considerations apply:

- A reliable static connection is required between EOC and all monitoring regions.

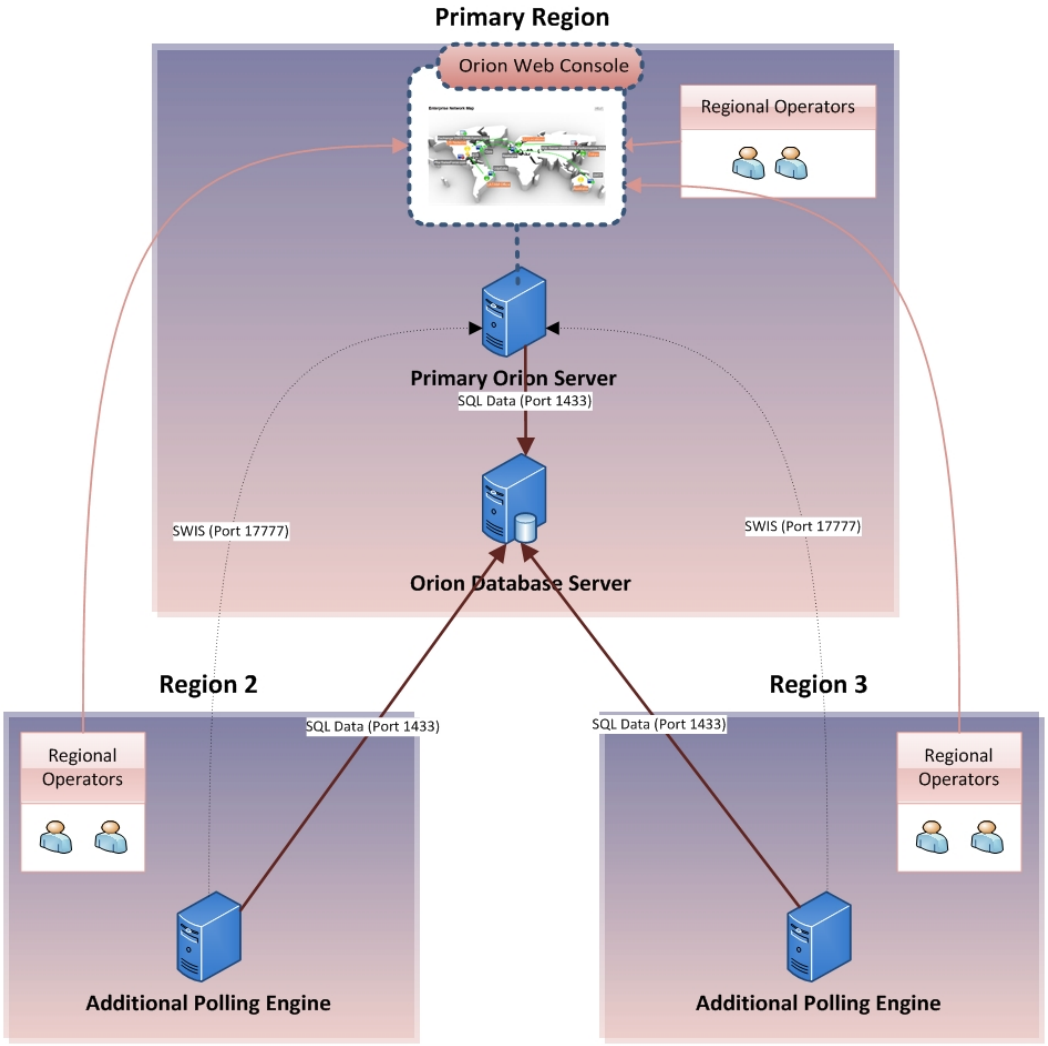
- Each SolarWinds Orion server is incrementally polled for current status and statistics only. EOC does not store historical data. Because it only performs incremental polling for current status and statistics, the bandwidth used by EOC is not considered to be significant.

Notes:

- Each region is managed, administered, and upgraded independently. For example, node, user, alert, and report creation, deletion and modification are performed separately in each region. Certain objects, such as alert definitions, Universal Device Pollers, and Server and Application Monitor templates can be exported and imported between instances.
- Each region can scale independently by adding additional polling engines as required.

Centralized Deployment with Remote Polling Engines

This option combines the benefits of a centralized Orion instance with the flexibility of localized data collection. Management and administration is done centrally on the primary server. This is well suited to organizations that require centralized IT management and localized collection of monitoring data.



In a centralized deployment with remote polling engines, additional polling engines poll data locally in each region, and the polled data is then stored centrally on the database server in the primary region. Regional Operators in each region log into the Orion Web Console in the Primary Region where the primary SolarWinds Orion server is installed to view data.

Additional Web Servers are available and may be installed in secondary regions. Using an Additional Web Server, a Regional Operator can then log into a local web console to view all network data.

Notes:

- The combination of the Primary Orion Server, database server and all remotely deployed polling engines is considered to be a single SolarWinds Orion instance.
- This single instance is being managed and administered centrally. For example, node, user, alert, and report creation, deletion and modification is performed centrally on the Primary Orion Server only.
- When nodes are added, the user selects the polling engine to which the node is assigned. All data collection for that node is then performed by that polling engine, and nodes can be re-assigned between polling engines, as required.
- A reliable static connection must be available between each region.
    - This connection will be continually transmitting MS SQL Data to the Orion Database Server; it will also communicate with the Primary Orion Server.
    - The latency (RTT) between each additional polling engine and the database server should be below 300ms. Degradation may begin around 200ms, depending on your utilization. In general, the remote polling engine is designed to handle connection outages, rather than high latency. The ability to tolerate connection latency is also a function of load. Additional polling engines polling a large number of elements may be potentially less tolerant of latency conditions.
    - To calculate the bandwidth requirement for a remote polling engine, consider the following example. If the additional polling engine polls 800 SNMP nodes, each node containing 12 interfaces and two volumes, then the data flow between the polling engine and the database server is approximately 300 KB/s. This calculation only considers the polling activity with disabled topology, and does not take into account the bandwidth requirement associated with syslogs, traps and alerts.

- Each polling engine uses Microsoft Message Queuing (MSMQ).
    - This allows data to be cached locally on the additional polling engine servers in the event of a connection outage to the Orion Database Server.
    - The amount of data that can be cached depends on the amount of disk space available on the polling engine server. The default storage space is 1 GB. A general guideline is that up to one hour of data can be cached. When the connection to the database is restored, the Orion Database Server is updated with the locally cached data. The synchronization occurs in a FIFO order, meaning that the oldest data is processed first. This means that after the connection is restored, a period of time elapses before the most up-to-date polling data appears instantly in the database.
    - If the database connection is broken for a longer time and the collector queue becomes full, the newest data is discarded until a connection to the database is re-established.
    - Data queuing is supported for modules that use the collector.
- Regional Operators in each region will log into the Orion Web Console in the Primary Region where you SolarWinds Orion platform products are installed to view data.
- An optional Additional Web Server is available, and it can be installed in secondary regions. Regional operators can then log into their local web consoles.
- All KPIs, such as Node Response Times, will be calculated from the perspective of each regional Additional Polling Engine. For example, the response time for a monitored node in Region 2 will be equal to the round trip time from the Additional Polling Engine in Region 2 to that node.

Installing Additional Polling Engines

The installation and initial configuration of a new Additional Polling Engine follows the same steps as the installation and configuration of a primary SolarWinds polling engine, with the following additional considerations:

- The most recent installer is available in your SolarWinds Customer Portal within the **Orion_Additional_Polling_Engine_**version**.zip** archive.
- If you want to monitor or manage devices polled by an additional polling engine in any Orion module, you must install the additional polling engine for the appropriate module. For more information, see the SolarWinds documentation for your Orion module.
- Individual licenses must be activated for each polling engine in a stackable poller installation.
- If you have configured an alert with a Send Email action to trigger on a node monitored by an additional polling engine, confirm that the additional polling engine has access to your SMTP server.

To install an Orion Additional Polling Engine:

1. Launch the appropriate executable, which you have downloaded from the SolarWinds website.
   Notes:
   - The executable extracts to a folder containing an HTML readme, an Installer Guide, and Additional Polling Engine installers for all Orion products that support Additional Polling Engines.
   - Launch the installer that corresponds to the SolarWinds product installed on your primary SolarWinds NPM server.
   - If you have multiple Orion products installed on your primary SolarWinds NPM server, install the additional polling engine for each product to ensure full functionality.
2. On the Welcome window of the Compatibility Check, provide the following information:
   - The **Hostname or IP Address** of your primary SolarWinds NPM server.

- The **User name** and **Password** of a user with administrative privileges to the Orion Web Console on your primary SolarWinds NPM server.

3. Click **Next**, and then complete the installation as you would on a primary SolarWinds NPM server.

Activating Stackable Poller Licenses

When installing additional polling engines in a stacked poller installation, licenses must be activated using the Smart Bundle installer.

Choose from the scenarios below:

1. Main Orion Server + Stackable Pollers
    a. Use Full Installer to install main poller.
    b. Use Smart Bundle to install stackable poller(s). The license will be initiated on the first screen.
2. Additional Polling Engine + Stackable Pollers
    a. Use Smart Bundle to install Additional Polling Engine. This will install bits for all needed modules/products (unless something is not included by Smart Bundle).
    b. Use Smart Bundle to install stackable poller(s). The license will be asked on the first screen
3. Add stackable Pollers to existing APE (could be installed by previous Smart Bundle or regular APE installer).
    a. Use Smart Bundle to install any missing or out-of-date modules. If some modules are not included in the Smart Bundle, it will provide instruction for you to download a regular Additional Poller installer and install the missing parts.

Frequently Asked Questions

The following questions address some common issues encountered when using scalability engines with a SolarWinds installation.

Does each module have its own polling engine?

No, any additional polling engine may have all relevant modules installed on it, and it will perform polling for all installed modules. An additional polling engine essentially works in the same way as your primary polling engine on your main server.

If I am monitoring with both NPM and SAM, do I need to install a NPM polling engine and a separate SAM polling engine?

No, any additional polling engine may have all relevant modules installed on it, and it will perform polling for all installed modules. An additional polling engine essentially works in the same way as your primary polling engine on your main server.

Are polling limits cumulative or independent? For example, can a single polling engine poll 12k NPM elements AND 10k SAM monitors together?

Yes, a single polling engine can poll up to the limits of each module installed, providing sufficient hardware resources are available.

Are there different size license available for the Additional Polling Engine?

No, the Additional Polling Engine is only available with an unlimited license.

Can you add an Additional Polling Engine to any size module license?

Yes, you can add an Additional Polling Engine to any size license.
Note: Adding an Additional Polling Engine **does not** increase your license size. For example, if you are licensed for an NPM SL100, adding an additional polling engine does not increase the licensed limit of 100 nodes/interfaces/volumes, but the polling load is spread across two polling engines instead of one.

Will an Additional Polling Engine allow me to monitor overlapping IP's?

Yes, you will be able to add nodes with the same IP Address to separate polling engines allowing you to monitor overlapping IP Addresses.

Appendix A: References

This section provides reference information relevant for SolarWinds SolarWinds Network Performance Monitor.

- Troubleshooting
- Orion Variables and Examples
- Status Icons and Identifiers
- Regular Expression Pattern Matching
- 95th Percentile Calculations

Troubleshooting

If you have problems with an Orion product, the causes are usually related to an incorrect configuration or corrupted files. The following suggestions can often clear up these problems.

Back Up Your Data

As a first step in any troubleshooting procedure, you should back up your Orion database.

For more information about creating database backups, see the section, "Creating Orion NPM Database Backup Files" in the SolarWinds NPM online documentation.

Verify Program Operation

SolarWinds NPM runs many components at the same time to deliver a view of your network status.

Confirm that the following components are running:

- Services:
  - Message Queuing
  - Net.Tcp Port Sharing Service
  - SolarWinds Alerting Engine service
  - SolarWinds Collector Data Processor, Management Agent, and Polling Controller services
  - SolarWinds Information Service
  - SolarWinds Job Engine and Job Engine v2
  - SolarWinds Job Scheduler
  - SolarWinds Orion Information Service
  - SolarWinds Orion Module Engine
  - SolarWinds Syslog and Trap Services
- SQL Server
- Internet Information Service (IIS)
- SolarWinds Web Console

Stop and Restart

Many problems disappear when programs are restarted. Stopping and restarting Internet Information Service (IIS) may eliminate web page problems. Problems with polling or data gathering may be eliminated by stopping and restarting Job Engine or Collector services using the available shutdown tool that you can locate as follows:

Click **Start > All Programs > SolarWinds Orion > Advanced Features > Orion Service Manager**.

For a complete refresh of the system, reboot the computer.

Run the Configuration Wizard

Running the Configuration Wizard, which refreshes files on the web server and performs checks on the structure of your database, may solve many problems.

Note: Before you run the Configuration Wizard, you should close all open applications.

Working with Temporary Directories

The following sections provide procedures for moving Windows and SQL Server temporary directories to optimize Orion server performance and resources.

- Moving the SQL Server Temporary Directory
- Redefining Windows System Temporary Directories

Moving the SQL Server Temporary Directory

The SQL Server temporary directory, **tempdb**, where temporary database objects generated during table creation and sorting are stored, is typically created in the same location on your Orion database server as the **master**, **model**, and **msdb** databases. Moving the **tempdb** database to a physical drive separate from your Orion database can significantly improve overall system performance.

For more information about moving the SQL Server 2005 temporary directory, **tempdb**, see "Moving System Databases – Example A: Moving the tempdb Database".

For more information about moving the SQL Server 2008 temporary directory, **tempdb**, see "Moving System Databases – Example A: Moving the tempdb Database".

Redefining Windows System Temporary Directories

Following established Windows standards, the SolarWinds NPM installer may use Windows User and System TEMP and TMP variable directories as temporary scratch spaces for file expansion and execution. If you do not have the required scratch space available in the default User or System TEMP and TMP directories, use the following procedure to redefine your default locations.

Note: Regardless of where you actually install SolarWinds NPM, some common files may be installed where the operating system of your Orion server are located.

To redefine default system temporary directories:

1. Log on to your Orion server as a user with administrative rights.
2. Right-click **My Computer**, and then click **Properties**.
3. Click **Advanced**, and then click **Environment Variables**.
4. Select the variable name representing the directory you want to redefine, click **Edit**, and then provide a new path as the **Variable value** for the selected temporary directory variable.

Slow Performance on Windows Server 2008

If Orion is installed on Windows Server 2008 and there are any devices on your network, between your Orion server and your database server, that do not support RFC 1323, the TCP window size auto-tuning feature of Windows Server 2008 may prevent your Orion server from successfully connecting with your Orion database.

This TCP auto-tuning feature is intended as a network-sensitive restriction, applied by the receiver—your SolarWinds Orion server—on the amount of data it is allowed or able to receive. If any devices along the network path between your Orion server and your Orion database do not support the TCP window scaling detailed in RFC 1323, the allowed size of the TCP window in packets sent to your Orion server may not match the TCP window size reported by packets sent from your Orion server. This mismatch may lead to failed connections between your Orion server and your Orion database. The following procedure disables this TCP auto-tuning feature, resetting the TCP receive window to 64kB.

To disable tcp auto-tuning:

1. Click **Start > All Programs > Accessories**.
2. Right-click **Command Prompt**, and then click **Run as administrator**.
3. ***If you are prompted by User Account Control,*** click **Continue** to open the elevated command prompt.

   Note: In some cases, having User Account Control (UAC) enabled on Windows Server 2008 can lead to installation errors. For more information about disabling UAC, see the article "Disabling User Account Control (UAC)" in the SolarWinds Knowledge Base.

4. At the prompt, enter the following:

   netsh interface tcp set global autotuninglevel=disabled

5. Close the command prompt window, and then restart your Orion server.

Adjusting Interface Transfer Rates

SolarWinds NPM monitors the actual transfer rates on the interfaces and calculates the percent utilization in real time, as it is requested in reports or within the user interface. Usually when you see interface utilization over 100% it is because the Transmit and Receive bandwidth values for this interface in SolarWinds NPM are incorrect.

To update interface transfer rates:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. In the web console, click the node that contains the interface you want to update. This opens the Node Details view for the parent node of the interface you want to edit.
3. In the Current Percent Utilization of Each Interface, or any other interface-related resource on the Node Details view, click the interface you want to edit. This opens the Interface Details view for the interface you want to edit.
4. In the Interface Details resource, click **Edit Interface**.
5. Check **Custom Bandwidth**.
6. Enter desired values in the **Transmit Bandwidth** and **Receive Bandwidth** fields, and then click **Submit**.

Using Integrated Remote Desktop

Sometimes it is necessary to console into a remote server to troubleshoot an issue. This can be accomplished within the Orion Web Console as follows.

Note: Press **Ctrl+Alt+Break** to enter/exit full screen mode.

To launch Integrated Remote Desktop:

1. Open the Node Details view for the server you want to view remotely.

   Note: The easiest way to open the Node Details view is to click the remote server you want to view in any All Nodes resource.

2. Click  , located at the of the Node Details view.

   Note: Depending on the security settings of your browser, you may be asked to install an ActiveX control for remote desktop viewing. Follow all prompts to install this required control.

3. Verify the **Server** IP address or hostname, select an appropriate **Screen Size**, and then click **Connect**.

Running SolarWinds Diagnostics

SolarWinds Diagnostics is a tool that collects active diagnostics which can be used for troubleshooting.

To run active diagnostics:

1. Navigate to **Orion Diagnostics** via **Start > All Programs > SolarWinds Orion > Documentation and Support**.
2. In SolarWinds Diagnostics, click the **Run Active Diagnostics** button. The SolarWinds Active Diagnostics window will open.
3. Right-click the appropriate category in the tree, such as UnDP, and select **Run Tests**.

   Active Diagnostics for the selected category will complete and the selected category icon will change color to reflect the results.

   - green - tests passed successfully

- yellow - tests passed with a warning
- red - tests failed

To run all available active diagnostics, click **Run Diagnostics**.

4. If a test in the category completed with a warning or failed, the whole category icon color changes. Expand the category and select the issue. The issue details will be displayed in the upper left-hand pane.
   The lower pane displays the progress of running tests in the selected category, and the status of tests after the tests are completed.
5. Click Export Results, save the log file (.json) and provide it to SolarWinds support.

Orion Variables and Examples

Orion platform products, including the Alert Manager, the Traps Viewer, the Syslog Viewer, and Network Atlas can employ Orion variables. These variables are dynamic and, in the case of alerts, parse when the alert is triggered or reset.

As of Orion Platform version 2015.1, variables have changed to a more flexible format. The previous implementation was SQL based, and the new version is based on SolarWinds Information Service (SWIS). For example, the variable **${ResponseTime}** is now **${N=SwisEntity;M=ResponseTime}**.

Tip: Check your version number by scrolling to the bottom of the page in the Orion Web Console.

Variable Construction

Variables are designated by a $ and enclosed in {brackets}. There are three attributes per variable, but only two are necessary.

Note: All variables are available in the variable picker in the Orion Web Console. You do not need to create or enter variables manually.

${N=context;M=macroName;F=format}

N

This is the context of the variable and required. You can use the following contexts:

- **Alerting** - uses variables specific to alerting
- **OrionGroup**- uses variables specific to groups
- **SwisEntity** - uses variables specific to the objects you monitor in the context of the alert
- **Generic** - uses variables specific to general environmental properties

M

This is the variable or macro name and required. You can use entity names from the SWIS.

F

This converts the data to a user-friendly format. Use formats that correlate to the data. For example, use DateTime with AcknowledgedTime, not with ObjectType. You can convert data to specific formats using the variable picker.

Variable Modifiers

Variables can be modified by using 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

Add modifiers to variables by the following examples below:

${N=*context*;M=*Modifier*(*macroName*)}

${N=*Alerting*;M=*Previous*(*AcknowledgedBy*)}

Alert Variables

General Alert Variables

The following are valid, general alert variables.

General Variable	Description
${N=Alerting; M=AlertID}	The ID of the alert
${N=Alerting; M=AlertName}	The name of the alert from the alert field **Name of alert definition** in Alert Properties
${N=Alerting; M=AlertDescription}	The description of the alert from the alert field **Description of alert definition** in Alert Properties
${N=Alerting; M=AlertDetailsURL}	The URL used to get more information about the triggered alert
${N=Alerting; M=AlertMessage}	The alert message from the alert field **Message displayed when this alert is triggered** in Trigger Actions
${N=Alerting;M=DownTime}	The amount of time the alert has been active
${N=Alerting; M=ObjectType}	The object type that the alert is monitoring
${N=Alerting; M=Severity}	The severity of the alert from the alert field **Severity of Alert** in Alert Properties
${N=Alerting; M=LastEdit}	The last time the alert definition has been edited
${N=Alerting; M=Acknowledged}	Acknowledged status
${N=Alerting; M=AcknowledgedBy}	Who the alert was acknowledged by
${N=Alerting; M=AcknowledgedTime}	Time the alert was acknowledged
${N=Alerting; M=Notes}	Information from the **Notes** field when you acknowledge alerts through the Web Console

General Variable	Description
${N=Alerting; M=AlertTriggerCount}	Count of triggers
${N=Alerting; M=AlertTriggerTime}	Date and time of the last event for this alert. (Windows control panel defined “Short Date” and “Short Time”)
${N=Generic; M=Application}	SolarWinds application information
${N=Generic; M=Copyright}	Copyright information
${N=Generic; M=Release}	Release information
${N=Generic; M=Version}	Version of the SolarWinds software package

It is possible to use previous generation variables, for example ${NodeName}. However, when using the variable picker, the new format is displayed by default. Previous generation variables can only be entered manually.

Note: Some variables are no longer valid. See Defunct Alert Variables.

Date Time

The following are valid date and time variables.

Date/Time Variable	Description
${N=Generic; M=AMPM}	AM/PM indicator
${N=Generic; M=AbreviatedDOW}	Current day of the week. Three character abbreviation.
${N=Generic; M=Day}	Current day of the month
${N=Generic; M=Date; F=Date}	Current date. (Short Date format)

Date/Time Variable	Description
${N=Generic; M=DateTime; F=DateTime}	Current date and time. (Windows control panel defined “Long Date” and “Long Time” format)
${N=Generic; M=DayOfWeek}	Current day of the week.
${N=Generic; M=DayOfYear}	Numeric day of the year
${N=Generic; M=Hour}	Current hour
${N=Generic; M=HH}	Current hour. Two digit format, zero padded.
${N=Generic; M=Past2Hours}	Last two hours
${N=Generic; M=Past24Hours}	Last 24 hours
${N=Generic; M=Last7Days;F=Date}	Last seven days (Short Date format)
${N=Generic; M=PastHour}	Last hour
${N=Generic; M=LocalDOW}	Current day of the week. Localized language format.
${N=Generic; M=LocalMonthName}	Current month name in the local language.
${N=Generic; M=LongDate}	Current date. (Long Date format)
${N=Generic; M=Month}	Current numeric month
${N=Generic; M=MM}	Current month. Two digit number, zero padded.

Date/Time Variable	Description
${N=Generic; M=AbbreviatedMonth}	Current month. Three character abbreviation.
${N=Generic; M=MonthName}	Full name of the current month
${N=Generic; M=MediumDate}	Current date. (Medium Date format)
${N=Generic; M=Minute}	Current minute. Two digit format, zero padded.
${N=Generic; M=Second}	Current second. Two digit format, zero padded.
${N=Generic; M=Time}	Current Time. (Short Time format)
${N=Generic; M=Today; F=Date}	Today (Short Date format)
${N=Generic; M=Year}	Four digit year
${N=Generic; M=Year2}	Two digit year
${N=Generic; M=Yesterday; F=Date}	Yesterday (Short Date format)

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 Orion platform products, use **${SQL:{query}}** as shown in the following example that returns the results of the SQL query:

Select Count(*) From Nodes:

Note: SolarWinds does not support SQL queries directly. Visit our user forums on thwack for help from our community.

Status Values

When using the **${N=SwisEntity; M=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	Partly Available
16	Misconfigured
17	Could Not Poll
19	Unconfirmed

Status Value	Description
22	Active
24	Inactive
25	Expired
26	Monitoring Disabled
27	Disabled
28	Not Licensed
29	Other
30	Not Running

Node Variables

The following are valid node variables.

Node Variable	Description
${N=SwisEntity;M=AgentPort}	Node SNMP port number
${N=SwisEntity;M=Node.Allow64BitCounters}	Node allows 64-bit counters (1), or not (0)
${N=SwisEntity;M=AvgResponseTime}	Average node response time, in msec, to ICMP requests
${N=SwisEntity;M=BlockUntil}	Day, date, and time until which node polling is blocked

Node Variable	Description
${N=SwisEntity;M=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
${N=SwisEntity;M=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
${N=SwisEntity;M=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
${N=SwisEntity;M=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
${N=SwisEntity;M=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

Node Variable	Description
${N=SwisEntity;M=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
${N=SwisEntity;M=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
${N=SwisEntity;M=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
${N=SwisEntity;M=BufferNoMemThisHour}	Count of buffer errors due to low memory on node in current hour
${N=SwisEntity;M=BufferNoMemToday}	Count of buffer errors due to low memory on node in current day

Node Variable	Description
${N=SwisEntity;M=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
${N=SwisEntity;M=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
${N=SwisEntity;M=Caption}	User friendly node name
${N=SwisEntity;M=Community}	Node community string
${N=SwisEntity;M=Contact}	Contact information for person or group responsible for node
${N=SwisEntity;M=CPULoad}	Node CPU utilization rate at last poll
${N=SwisEntity;M=CustomPollerLastStatisticsPoll}	Day, date, and time of last poll attempt on node
${N=SwisEntity;M=CustomPollerLastStatisticsPollSuccess}	Day, date, and time that node was last successfully polled

Node Variable	Description
${N=SwisEntity;M=NodeDescription}	Node hardware and software
${N=SwisEntity;M=DNS}	Fully qualified node name
${N=SwisEntity;M=DynamicIP}	If node supports dynamic IP address assignment via BOOTP or DHCP (1); static IP address return (0)
${N=SwisEntity;M=EngineID}	Internal unique identifier of the polling engine to which node is assigned
${N=SwisEntity;M=GroupStatus}	Filename of status icon for node and, in Orion NPM, its interfaces
${N=SwisEntity;M=IOSImage}	Family name of Cisco IOS on node
${N=SwisEntity;M=IOSVersion}	Cisco IOS version on node
${N=SwisEntity;M=IP_Address}	Node IP address
${N=SwisEntity;M=IPAddressType}	Node IP address version (IPv4 or IPv6)
${N=SwisEntity;M=LastBoot}	Day, date and time of last node boot

Node Variable	Description
${N=SwisEntity;M=LastSync}	Time and date of last node database and memory synchronization
${N=SwisEntity;M=Location}	Physical location of node
${N=SwisEntity;M=MachineType}	Node manufacturer or distributor and family or version information
${N=SwisEntity;M=MaxResponseTime}	Maximum node response time , in msec, to ICMP requests
${N=SwisEntity;M=MemoryUsed}	Total node memory used over polling interval
${N=SwisEntity;M=Stats.MinResponseTime}	Minimum node response time , in msec, to ICMP requests
${N=SwisEntity;M=NextPoll}	Day, date and time of next scheduled node polling
${N=SwisEntity;M=NextRediscovery}	Time of next node rediscovery
${N=SwisEntity;M=NodeID}	Internal unique identifier of node
${N=SwisEntity;M=PercentLoss}	ICMP packet loss percentage when node last polled

Node Variable	Description
${N=SwisEntity;M=PercentMemoryUsed}	Percentage of total node memory used over polling interval
${N=SwisEntity;M=PollInterval}	Node polling interval, in seconds
${N=SwisEntity;M=RediscoveryInterval}	Node rediscovery interval, in minutes
${N=SwisEntity;M=ResponseTime}	Node response time, in milliseconds, to last ICMP request
${N=SwisEntity;M=SNMPv3Credentials.RWAuthenticationKey}	SNMPv3 read/write credential authentication key
${N=SwisEntity;M=SNMPv3Credentials.RWAuthenticationKeyIsPassword}	States if the SNMPv3 read/write credential authentication key is the password
${N=SwisEntity;M=SNMPv3Credentials.RWAuthenticationMethod}	SNMPv3 read/write credential authentication method
${N=SwisEntity;M=SNMPv3Credentials.RWContext}	SNMPv3 read/write security context information
${N=SwisEntity;M=SNMPv3Credentials.RWPrivacyKey}	SNMPv3 read/write credential key

Node Variable	Description
${N=SwisEntity;M=SNMPv3Credentials. RWPrivacyKeyIsPassword}	States if the SNMPv3 read/write credential privacy key is the password
${N=SwisEntity;M=SNMPv3Credentials. RWPrivacyMethod}	SNMPv3 read/write credential privacy encryption method
${N=SwisEntity;M=SNMPv3Credentials. RWUsername}	User friendly name for SNMPv3 read/write credential

Node Variable	Description
${N=SwisEntity;M=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 SAM, 100 points is provided for an application in a warning state, 200 points for an application in critical state, 500 is status is unknown, and 1000 for a down application.
${N=SwisEntity;M=SNMPv3Credentials.AuthenticationKey}	SNMPv3 authentication key
${N=SwisEntity;M=SNMPv3Credentials.AuthenticationKeyIsPassword}	States if node SNMPv3 authentication key is password
${N=SwisEntity;M=SNMPv3Credentials.AuthenticationMethod}	SNMPv3 authentication type

Node Variable	Description
${N=SwisEntity;M=SNMPv3Credentials.Context}	Group or domain of user with SNMPv3 access to node
${N=SwisEntity;M=SNMPv3Credentials.PrivacyKey}	SNMPv3 credential key
${N=SwisEntity;M=SNMPv3Credentials.PrivacyKeyIsPassword}	States if node SNMPv3 credential key is the password
${N=SwisEntity;M=SNMPv3Credentials.PrivacyMethod}	SNMPv3 credential key type
${N=SwisEntity;M=SNMPv3Credentials.Username}	User friendly name for SNMPv3 credential
${N=SwisEntity;M=SNMPVersion}	States the version of SNMP used by the node
${N=SwisEntity;M=StatCollection}	Statistics collection frequency, in minutes
${N=SwisEntity;M=Status;F=Status}	Numerical node status. For more information, see Status Values.
${N=SwisEntity;M=StatusDescription}	User friendly node status
${N=SwisEntity;M=StatusLED}	Filename of node status icon

Node Variable	Description
${N=SwisEntity;M=SysName}	String reply to SNMP SYS_ NAME OID request
${N=SwisEntity;M=SysObjectID}	Vendor ID of the network management subsystem in OID form. Clearly determines the type of node.
${N=SwisEntity;M=SystemUpTime}	Time, in hundredths of a second, either since network monitoring started (WMI) or since the monitored device rebooted (SNMP).
${N=SwisEntity;M=TotalMemory}	Total node memory available
${N=SwisEntity;M=UnManaged}	States if node is currently unmanaged
${N=SwisEntity;M=UnManageFrom}	Day, date, and time when node is set to “Unmanaged”
${N=SwisEntity;M=UnManageUntil}	Day, date, and time when node is scheduled to be managed
${N=SwisEntity;M=Vendor}	Node manufacturer or distributor

Node Variable	Description
${N=SwisEntity;M=VendorIcon}	Filename of node vendor logo

Defunct Alert Variables

The following variables are no longer valid:

- **${Property}** - The property the alert is monitoring. You can select a new variable with the specific property you want to view.
- **${TriggeredValue}** - The value that triggered the alert. You can select a new variable with the specific property you want to view.
- **${AlertStartTime}** - When the alert active. You can use the Time of Day scheduler to control when the alert is active.
- **${AlertEndTime}** - When the alert is no longer active. You can use the Time of Day scheduler to control when the alert is not active.
- **${ObjectSubType}** - Determines if the node supports SNMP or is ICMP-only. You can use Node.ObjectSubType as the macro name.

NPM-Specific Alert Variables

In addition to the advanced alerts and alert variables that are available to all Orion products, the monitoring features that NPM alone provides can also use the following NPM-specific alert variables:

- Interface Poller Variables
- Interface Variables
- Universal Device Poller
- Wireless Node Variables

Interface Poller Variables

The following are valid interface poller variables.

Note: At least one of the **CustomPollerStatus** variables from the tables below must be included in the trigger condition of all interface poller alerts.

Interface Poller Assignment Variable	Description
${AssignmentName}	User friendly name of a specific assignment in the form: <PollerName> - <NodeName> - <InterfaceName>. Interface name is '0' if this is a node poller.
${N=SwisEntity;M=CustomPollerAssignment.CustomPollerAssignmentID}	Internal unique ID (as guid) of specific assignment of a poller to a node or interface.
${N=SwisEntity;M=InterfaceID}	Internal unique ID of interface (as integer) in this assignment. '0' if this is a node poller.

Interface Poller Assignment Variable	Description
${N=SwisEntity;M=NodeID}	Internal unique ID of node (as integer) in this assignment.
${N=SwisEntity;M=CustomPollerAssignment.CustomPoller.CustomPollerID}	Internal unique poller ID (as guid) in this assignment

Interface Poller Status Variable	Description
${N=SwisEntity; M=CustomPollerAssignment.CustomPollerAssignmentID}	Internal unique ID (as guid) of the specific assignment of a poller to a node or interface.
${N=SwisEntity;M=DateTime}	Date and time poller statistic was last collected.
${DateTimeUTC}	UTC Date/time statistics last collected for this assignment
${N=SwisEntity;M=Rate}	For a poller with a MIB value type of 'Rate', this field contains numeric data collected from the OID.

Interface Poller Status Variable	Description
	For a poller with a MIB value type of 'Counter', this field contains the change in the previous value as normalized to the polling interval. For a 'Raw Value' poller this field is null.
${N=SwisEntity;M=RawStatus}	For poller with a MIB value type 'Rate' or 'Counter', this field is null. For a poller with MIB value 'Raw Value' and an OID response value that is numeric, this field contains the numeric value. For a poller with MIB value 'Raw Value' and an OID response value that is not numeric, this field is null.

Interface Poller Status Variable	Description
	For enumerations this field contains the actual numeric value returned from the OID instead of the user friendly text. Status comparisons that are numeric (greater than and less than) should use this field. Status values that are text descriptions should use the 'Status' field.
${N=SwisEntity;M=Status}	For a poller with a MIB value type of 'Rate' or 'Counter', this field is null. For a poller with a MIB value of 'Raw Value' this field contains the value from the OID 'cooked' according to its sub-type.

Interface Poller Status Variable	Description
	Enumerations contain user friendly text instead of a numeric value returned from the OID.
${N=SwisEntity;M=Total}	For a poller with a MIB value type of 'Rate', this field is null. For a poller with a MIB value type of 'Counter' this field contains the change in the previously collected value. For a poller with a MIB value of 'Raw Value' this field is null.

Rate pollers only write to the 'Rate' field; counter pollers only write to the 'Total' and 'Rate' fields; and status pollers only write to the 'Status' field, unless they can be successfully converted to a numeric value, in which case the numeric value is also written to the 'RawStatus' field.

Interface Poller Variable	Description
${DefaultDisplayTimeUnitID}	Internal unique ID of time units as represented by UI
${N=SwisEntity;M=Description}	Poller description

Interface Poller Variable	Description
${Enabled}	(1) indicates poller currently up and collecting, otherwise (0)
${Format}	Currently unused
${GroupName}	User friendly name of group to which this poller belongs
${IncludeHistoricStatistics}	(1) indicates that every statistic collection is inserted as a new record. (0) indicates that this statistic is updated so that it only has one statistic record.
${N=SwisEntity;M=InterfaceLastChange}	Date and time that poller record last changed
${LastChangeUTC}	Date and time that poller record last changed (universal time)
${MIB}	Generally recognized OID name
${NetObjectPrefix}	(N) if this is a node poller. (I) if this is an interface poller

Interface Poller Variable	Description
${OID}	OID used to gather information
${ParserID}	Internal unique ID of the parser (sub-type) of this poller, where 1=None, 2=text, 3=enum, 4=macAddress, 5=counter, 6=gauge, 10=TrueFalse, 11=FalseTrue, 12=CleanMac, 14=TimeTicks, 15=HighBandwidth, 16=AdminStatus, 17=OperationalStatus
${N=SwisEntity; M=CustomPollerAssignment.CustomPoller.CustomPollerID}	Poller unique ID (guid)
${PollerType}	(R) for rate poller, (C) for counter poller, (S) for status poller
${SNMPGetType}	SNMP request type (Get or GetNext)
${TimeUnitID}	Internal unique ID of time unit (msec/sec/min/hr/days) to which poller is normalizing

Interface Poller Variable	Description
${TimeUnitQuantity}	Number of time units to which poller is normalizing
${UniqueName}	Poller user friendly name
${Unit}	User-entered description of unit collected (bytes/degrees/dbs)

Interface Variables

The following are valid interface variables.

Interface Variable	Description
${N=SwisEntity;M=AdminStatus}	Numeric administrative status of interface. For more information, see Status Icons and Identifiers.
${N=SwisEntity;M=AdminStatusLED}	Filename of current interface administrative status icon
${N=SwisEntity;M=Caption}	User friendly description of interface combining name with other identifying information
${N=SwisEntity;M=Counter64}	States if interface supports IF-MIB high capacity counters
${CustomBandwidth}	Indicates if transmit and receive bandwidth fields are user-controlled (1) or controlled by automated detection via ifSpeed MIB (0)

Interface Variable	Description
${CustomPollerLastStatisticsPoll}	Day, date, and time that this interface was last polled by the current poller
${N=SwisEntity;M=FullName}	User friendly name combining captions of parent node and interface
${N=SwisEntity;M=Caption}	Internal name discovered for this interface with the ifName OID
${N=SwisEntity;M=InterfaceID}	Internal unique identifier of selected interface
${N=SwisEntity;M=InBandwidth}	Incoming bandwidth of interface
${N=SwisEntity;M=Inbps}	Current incoming traffic, in bps, to interface
${N=SwisEntity;M=InDiscardsThisHour}	Number of incoming packets discarded by interface in last hour
${N=SwisEntity;M=InDiscardsToday}	Number of incoming packets discarded by interface in current day
${N=SwisEntity;M=InErrorsThisHour}	Number of interface receive errors in last hour
${N=SwisEntity;M=InErrorsToday}	Number of interface receive errors in current day
${N=SwisEntity;M=InMcastPps}	Current incoming multicast traffic, in packets per second, to interface
${N=SwisEntity;M=InPercentUtil}	Current percent utilization of interface receive

Interface Variable	Description
${N=SwisEntity;M=InPktSize}	Average size of incoming packets to interface
${N=SwisEntity;M=InPps"}	Current incoming traffic, in packets per second, to interface
${N=SwisEntity;M=InterfaceAlias}	Alias or description of interface discovered from parent node
${N=SwisEntity;M=InterfaceIcon}	Filename of the icon used to represent the interface type
${N=SwisEntity;M=InterfaceIndex}	Index of selected interface on parent node
${N=SwisEntity;M=InterfaceLastChange}	sysUpTime value when the interface entered current operational state
${InterfaceMTU}	Interface Maximum Transfer Unit: the largest packet the interface can handle
${N=SwisEntity;M=InterfaceName}	User friendly name
${N=SwisEntity;M=InterfaceSpeed}	Interface bandwidth
${N=SwisEntity;M=InterfaceType"}	IANA type of selected interface
${InterfaceTypeDescription}	User friendly description of interface type
${N=SwisEntity;M=InterfaceTypeName}	User friendly name of interface IANA type
${N=SwisEntity;M=InUcastPps}	Current incoming unicast traffic, in packets per second, to interface

Interface Variable	Description
${LastSync}	Time and date of last interface database and memory synchronization
${N=SwisEntity;M=NextPoll}	Day, date and time of next scheduled interface polling
${N=SwisEntity;M=NextRediscovery}	Next interface rediscovery time
${N=SwisEntity;M=NodeID}	Internal unique identifier of node that is parent to the selected interface
${N=Alerting;M=ObjectSubType}	States if parent node supports SNMP or is ICMP only
${N=SwisEntity;M=OperStatusLED}	Filename of current interface operational status icon
${N=SwisEntity;M=OutBandwidth}	Outgoing bandwidth of interface
${N=SwisEntity;M=Outbps}	Current outgoing traffic, in bps, from interface
${N=SwisEntity;M=OutDiscardsThisHour}	Number of outgoing packets discarded by interface in last hour
${N=SwisEntity;M=OutDiscardsToday}	Number of outgoing packets discarded by interface in current day
${N=SwisEntity;M=OutErrorsThisHour}	Number of interface transmit errors in last hour
${N=SwisEntity;M=OutErrorsToday}	Number of interface transmit errors in current day

Interface Variable	Description
${N=SwisEntity;M=OutErrorsToday"}	Current outgoing multicast traffic, in packets per second, from interface
${N=SwisEntity;M=OutPercentUtil}	Current percent utilization of interface transmit
${N=SwisEntity;M=OutPktSize}	Average size of outgoing packets from interface
${N=SwisEntity;M=OutPps}	Current outgoing traffic, from interface, in pps
${N=SwisEntity;M=OutUcastPps}	Current outgoing unicast traffic, in packets per second, from interface
${PhysicalAddress}	Physical address of interface
${N=SwisEntity;M=PollInterval}	Interval, in seconds, between polling attempts for interface
${N=SwisEntity;M=RediscoveryInterval}	Interval, in minutes, between rediscovery attempts for interface
${N=SwisEntity;M=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
${N=SwisEntity;M=StatCollection}	Interface statistics collection frequency, in minutes
${N=SwisEntity;M=Status;F=Status" objectType="Interface}	Numeric interface status. For more information, see Status Icons and Identifiers.
${N=SwisEntity;M=StatusLED}	Filename of current interface status icon

Universal Device Poller

The following are valid Universal Device Poller variables.

Universal Device Poller Variable	Description
${CustomPollerStatus.RawStatus}	The value returned by a Raw Value-type Universal Device Poller
${DateTime}	Date/Time
${Description}	Assigned description of a Universal Device Poller
${Enabled}	Enabled status of a Universal Device Poller
${MIB}	The Management Information Base in which the OID polled by a Universal Device Poller is located
${OID}	The object ID polled by a Universal Device Poller
${Rate}	The value returned by a Rate-type Universal Device Poller
${Status}	Functional status of the Universal Device Poller
${Total}	Total
${UniqueName}	Assigned name of a Universal Device Poller

Wireless Node Variables

The following are valid wireless node variables.

Wireless Node Variable	Description
${WirelessAP}	States if node is being polled by the wireless poller (1) or not (0)
${WirelessLastStatPoll}	Date and time node last polled by wireless poller
${WirelessPollInterval}	Interval, in minutes, between wireless polling attempts on node
${WirelessStatBlockUntil}	Date and time node may be polled again by wireless poller

Network Atlas Tooltip Variables

Many of the variables that are available for use in NPM alerts are also available for use in Network Atlas tooltips. These variables are dynamic, and they parse when the tooltip is opened. For example, the variable **${CPULoad}** will parse with the current processor utilization of the node you are viewing.

Notes:

- For more information about viewing and customizing Network Atlas tooltips, see Customizing Orion Web Console Tooltips.
- In some cases, the table name may be required for alert variables, as in **${Nodes.Description}**. The following tables provide the table name in listed variables when it is required.
- In earlier versions of Network Atlas, variables were referred to as macros.

The following sections provide tables of variables corresponding to the types of objects you can map with Network Atlas.

Application Variables

The following application variables are valid for use in Network Atlas tooltips.

Variable	Description
${ApplicationID}	Internal unique identifier of the application

Variable	Description
${ApplicationTemplateID}	Internal unique identifier of the parent template
${Name}	Application name
${NodeID}	Internal unique identifier of assigned node
${Status}	Numerical application status code. For more information see "Status Icons and Identifiers" in the *SolarWinds Network Performance Monitor Administrator Guide*.
${StatusDescription}	User friendly application status
${UnManaged}	States if application is currently unmanaged

Application Component Monitor Variables

The following application component monitor variables are valid for use in Network Atlas tooltips.

Variable	Description
${ApplicationId}	Internal unique identifier of the associated application
${ComponentId}	Internal unique identifier of the component
${ComponentType}	Numerical component monitor type code. For more information, see "SolarWinds SAM Alerts" in the *SolarWinds Server & Application Monitor Administrator Guide*.
${Name}	Component monitor name
${Status}	Numerical application status code. For more information see "Status Icons and Identifiers" in the *SolarWinds Network Performance Monitor Administrator Guide*.
${StatusDescription}	User friendly application status

Variable	Description
${TemplateID}	Internal unique identifier of the parent template

Date and Time Variables

The following date and time variables are valid for Network Atlas tooltips.

Variable	Description
${AbreviatedDOW}	Abbreviated current day of the week.
${AMPM}	AM/PM indicator
${D}	Current day of the month
${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
${DD}	Current day of the month (two digit number, zero padded)
${H}	Current hour
${HH}	Current hour. Two digit format, zero padded.
${Last24Hours}	Time period: the last 24 hours
${Last2Hours}	Time period: the last 2 hours
${Last7Days}	Time period: the last 7 days
${LastHour}	Time period: the last hour
${LocalDOW}	Current day of the week. Localized language format.
${LocalMonthName}	Current month name in the local language.

Variable	Description
${LongDate}	Current date. (Long Date format)
${M}	Current numeric month
${MediumDate}	Current date. (Medium Date format)
${Minute}	Current minute. Two digit format, zero padded.
${MM}	Current month. Two digit number, zero padded.
${MMM}	Current month. Three character abbreviation.
${MMMM}	Full name of the current month
${S}	Current second.
${Second}	Current second. Two digit format, zero padded.
${Time}	Current Time. (Short Time format)
${Today}	Time period: today
${Year}	Four digit year
${Year2}	Two digit year
${Yesterday}	Time period: yesterday

General Variables

The following general variables are valid for use in Network Atlas tooltips.

Variable	Description
${Acknowledged}	Acknowledged status
${AcknowledgedBy}	Who the alert was acknowledged by
${AcknowledgedTime}	Time the alert was acknowledged
${AlertTriggerCount}	Count of triggers

Variable	Description
${AlertTriggerTime}	Date and time of the last event for this Alert. (Windows control panel defined “Short Date” and “Short Time”)
${Application}	SolarWinds application information
${Copyright}	Copyright information
${CR}	Line Feed – Carriage Return
${ObjectName}	Description/Name of the object in the alert
${Release}	Release information
${Version}	Version of the SolarWinds software package

Group Variables

The following group variables are valid for use in Network Atlas tooltips.

Variable	Description
${ContainerID}	Designated identifier for a mapped group
${DetailsURL}	URL of the Group Details view for a mapped group
${Frequency}	Interval on which group membership is evaluated and group snapshots are taken.
${IsDeleted}	When a group is marked for deletion, it is not deleted immediately. If a group is marked for deletion but not yet deleted, ${IsDeleted} returns **1**.
${LastChanged}	The date and time of the last change made to the definition of a group. This does not include changes made to group members resulting from dynamic queries.
${Name}	The name assigned to the mapped group
${Owner}	Orion product appropriate to the mapped group type

Variable	Description
${RollupType}	Name of roll-up logic calculator that evaluates status of the mapped group based on member statuses. **0** = Mixed, **1** = Worst, **2** = Best. The “Worst” method reports group status as the worst status of any of its members. The “Mixed” method reports group status as ”Warning” when members are of multiple different statuses. The “Best” method reports group status as the best status of any of its members.
${Status}	Status of the mapped group. For more information, see “Managing the Display of Group Status” in the SolarWinds Orion Common Components Administrator Guide.
${StatusCalculator}	Name of roll-up logic calculator that evaluates status of the mapped group based on member statuses. **0** = Mixed, **1** = Worst, **2** = Best. The “Worst” method reports group status as the worst status of any of its members. The “Mixed” method reports group status as ”Warning” when members are of multiple different statuses. The “Best” method reports group status as the best status of any of its members.
${Uri}	Uri used by SolarWinds Information Service (SWIS) to refer to the selected group member within the web console.
${WebUri}	URL of the Group Details view for a mapped group

Interface Variables

The following interface variables are valid for use in Network Atlas tooltips.

Variable	Description
${AdminStatus}	Numeric administrative status of interface. For more information see "Status Icons and Identifiers" in the *SolarWinds Network Performance Monitor Administrator Guide*.
${AdminStatusLED}	Filename of current interface administrative status icon
${Caption}	User friendly description of interface combining name with other identifying information
${Counter64}	States if interface supports IF-MIB high capacity counters
${CustomBandwidth}	Indicates if transmit and receive bandwidth fields are user-controlled (1) or controlled by automated detection via ifSpeed MIB (0)
${CustomPollerLastStatisticsPoll}	Day, date, and time that this interface was last polled by the current poller
${InBandwidth}	Incoming bandwidth of interface
${Inbps}	Current incoming traffic, in bps, to interface
${InDiscardsThisHour}	Number of incoming packets discarded by interface in last hour
${InDiscardsToday}	Number of incoming packets discarded by interface in current day
${InErrorsThisHour}	Number of interface receive errors in last hour

Variable	Description
${InErrorsToday}	Number of interface receive errors in current day
${InMcastPps}	Current incoming multicast traffic, in packets per second, to interface
${InPercentUtil}	Current percent utilization of interface receive
${InPktSize}	Average size of incoming packets to interface
${InPps}	Current incoming traffic, in packets per second, to interface
${InterfaceIcon}	Filename of the icon represent the interface type
${InterfaceID}	Internal unique identifier of selected interface
${InterfaceIndex}	Index of selected interface on parent node
${InterfaceLastChange}	sysUpTime value when the interface entered current operational state
${InterfaceMTU}	Interface Maximum Transfer Unit: the largest packet the interface can handle
${InterfaceName}	User friendly name
${InterfaceSpeed}	Interface bandwidth
${InterfaceType}	IANA type of selected interface
${InterfaceTypeDescription}	User friendly description of interface type
${InterfaceTypeName}	User friendly name of interface IANA type

Variable	Description
${InUcastPps}	Current incoming unicast traffic, in packets per second, to interface
${LastSync}	Time and date of last interface database and memory synchronization
${MaxInBpsTime}	Time when ${MaxInBpsToday} was measured
${MaxInBpsToday}	Maximum measured traffic, in bps, into interface
${MaxOutBpsTime}	Time when ${MaxOutBpsToday} was measured
${MaxOutBpsToday}	Maximum measured traffic, in bps, out from interface
${NextPoll}	Day, date and time of next scheduled interface polling
${NextRediscovery}	Next interface rediscovery time
${NodeID}	Internal unique identifier of node that is parent to the selected interface
${ObjectSubType}	States if parent node supports SNMP or is ICMP only
${OperStatus}	Numeric operational status of interface. For more information see "Status Icons and Identifiers" in the *SolarWinds Network Performance Monitor Administrator Guide*.
${OperStatusLED}	File name of current interface operational status icon
${OutBandwidth}	Outgoing bandwidth of interface

Variable	Description
${Outbps}	Current outgoing traffic, in bps, from interface
${OutDiscardsThisHour}	Number of outgoing packets discarded by interface in last hour
${OutDiscardsToday}	Number of outgoing packets discarded by interface in current day
${OutErrorsThisHour}	Number of interface transmit errors in last hour
${OutErrorsToday}	Number of interface transmit errors in current day
${OutMcastPps}	Current outgoing multicast traffic, in packets per second, from interface
${OutPercentUtil}	Current percent utilization of interface transmit
${OutPktSize}	Average size of outgoing packets from interface
${OutPps}	Current outgoing traffic, from interface, in pps
${OutUcastPps}	Current outgoing unicast traffic, in packets per second, from interface
${PhysicalAddress}	Physical address of interface
${PollInterval}	Interval, in seconds, between polling attempts for interface
${RediscoveryInterval}	Interval, in minutes, between rediscovery attempts for interface

Variable	Description
${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
${StatCollection}	Interface statistics collection frequency, in minutes
${Status}	Numeric interface status. For more information see "Status Icons and Identifiers" in the *SolarWinds Network Performance Monitor Administrator Guide*.
${StatusLED}	Filename of current interface status icon
${UnManaged}	States if interface is currently unmanaged
${UnPluggable}	States if interface is designated as unpluggable

IP SLA Variables

The following variables related to IP SLA operations are valid for use in Network Atlas tooltips.

Variable	Description
${DateChangedUtc}	The last time operation information was updated
${Description}	A user defined explanation of the operation
${Frequency}	How often the operation is performed
${IpSlaOperationNumber}	The time between operation executions
${IsAutoConfigured}	This value is **True** if it was created by VoIP & Network Quality Manager, **False** if it was created by the user

Variable	Description
${OperationInstanceID}	The internal ID of the operation.
${OperationName}	The name of the operation as it appears in Orion
${OperationTypeID}	Numerical operation status code. **1**=DHCP, **2**=DNS, **3**=FTP, **4**=HTTP, **5**=ICMP Echo, **8**=TCP Connect, **9**=UDP Echo, **10**=UDP Jitter, **11**=VoIP UDP Jitter
${SourceNodeID}	The Orion node ID of the source node
${Status}	Numerical operation status code. For more information see "Status Icons and Identifiers" in the *SolarWinds Network Performance Monitor Administrator Guide*.
${StatusMessage}	A message that describing the ${Status} value.
${TargetNodeID}	The Orion node ID of the node the operation is targeting

Node Variables

The following node variables are valid for use in Network Atlas tooltips.

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
${Caption}	User friendly node name

Variable	Description
${Community}	Node community string
${CPULoad}	Node CPU utilization rate at last poll
${CustomPollerLastStatisticsPoll}	Day, date, and time of last poll attempt on node
${CustomPollerLastStatisticsPollSuccess}	Day, date, and time that node was last successfully polled
${DateTime}	Current date and time. (Windows control panel defined “Long Date” and “Long Time” format)
${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
${External}	States if node is currently designated as external
${GroupStatus}	Filename of status icon for node and its interfaces
${IOSImage}	Family name of Cisco IOS on node
${IOSVersion}	Cisco IOS version on node

Variable	Description
${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
${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
${NodeName}	Node hostname. Defaults to node IP address **${IP_Address}** if hostname does not resolve.
${ObjectSubType}	States if node supports SNMP or is ICMP-only
${PercentLoss}	ICMP packet loss percentage when node last polled

Variable	Description
${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
${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.
${SNMPVersion}	States the version of SNMP used by the node
${StatCollection}	Statistics collection frequency, in minutes
${Status}	Numerical node status. For more information see "Status Icons and Identifiers" in the *SolarWinds Network Performance Monitor Administrator Guide*.
${StatusDescription}	User friendly node status
${StatusLED}	Filename of node status icon

Variable	Description
${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 monitoring started
${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 icon

Volume Variables

The following volume variables are valid for use in Network Atlas tooltips.

Variable	Description
${Caption}	User friendly volume name
${FullName}	User friendly volume name including captions of parent node and interface

Variable	Description
${LastSync}	Time and date volume last synchronized in database and memory models
${NodeID}	Internal unique identifier of parent node
${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 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

Variable	Description
${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

Wireless Variables

The following wireless variables are valid for use in Network Atlas tooltips.

Variable	Description
${WirelessAP}	States if node is being polled by the wireless poller (1) or not (0)
${ WirelessLastStatPoll }	Date and time node last polled by wireless poller
${ WirelessPollInterval }	Interval, in minutes, between wireless polling attempts on node
${ WirelessStatBlockUntil }	Date and time node may be polled again by wireless poller

Syslog Alert Variables

The following variables can be used in Syslog alert messages. Each variable must begin with a dollar sign and be enclosed in curly braces as, for example, **${**VariableName**}**. Syslog alerts also support the use of Node alert variables. For more information on the use of variables, see Orion Variables and Examples.

Syslog Date/Time Variables

Syslog Date/Time Variable	Description
${AbbreviatedDOW}	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 â€œShort Dateâ€ and â€œShort Timeâ€ 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.

Syslog Date/Time Variable	Description
${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
${Hostname}	Host name of the device triggering the alert
${IP_Address}	IP address of device triggering alert
${Message}	Status of device triggering alert
${MessageType}	The name of the triggered alert

${Severity}	A network health score indicating node states as follows:
	`INTERFACE_UNKNOWN = 1`
	`INTERFACE_WARNING = 1`

Syslog Variable	Description

	`INTERFACE_DOWN = 1000`
	`NODE_UNKNOWN = 1000000`
	`NODE_WARNING = 1000000`
	`NODE_DOWN = 100000000`
	
	The `Up` score for Nodes and Interfaces is zero.

${Version}	Version of the SolarWinds software package

Trap Alert Variables

The following variables can be used in trap alert messages with the Orion Trap Server. Each variable must begin with a dollar sign and be enclosed in curly braces as, for example, **${**VariableName**}**.

Note: Trap alerts may also use any valid node variables. For more information about node alert variables, see Orion Variables and Examples.

Other 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_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

Trap Variable	Description
${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}.
${vbData1}	Trap variable binding value
${vbName1}	Trap variable binding name

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

Trap Date/Time Variable	Description
${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

Example Messages Using Variables

The following examples illustrate messages that you can create using variables. You can use variables in the message body or the subject. You can also use variables in alert conditions.

SolarWinds recommends using the variable picker by clicking **Insert Variable**.

Message with variables	Message with resolved variables
Previous reboot was at **${N=SwisEntity;M=Previous(LastBoot)}.**	Previous reboot was at **10/29/2014 12:02:00 PM**.
Alert: The SNMP Community string used to query **${N=SwisEntity;M=Caption}** has been changed from **${N=SwisEntity;M=Previous(Community)}** to **${N=SwisEntity;M=Community}.**	Alert: The SNMP Community string used to query **Houston_backup** has been changed from **1234** to **5678**.
Alert: **${N=SwisEntity;M=Caption}** has exceptionally high response time. Average Response Time is **${N=SwisEntity;M=AvgResponseTime}** and is varying from **${N=SwisEntity;M=MinResponseTime}** to **${N=SwisEntity;M=MaxResponseTime}**.	Alert: **DevOP_VMs** has exceptionally high response time. Average Response Time is **1200 ms** and is varying from **500 ms** to **1700 ms**.
Current packet loss for **${N=SwisEntity;M=Caption}** is **${N=SwisEntity;M=PercentLoss}**. Average Response time is **${N=SwisEntity;M=AvgResponseTime}** and is varying from **${N=SwisEntity;M=MinResponseTime}** to **${N=SwisEntity;M=MaxResponseTime}**.	Current packet loss for **MainWebServer** is **43%**. Average Response time is **500 ms** and is varying from **200 ms** to **800 ms**.

You can also manually add a repeater when you expect multiple objects to be included in an alert. For example, if you have an alert set up to notify you when 5 nodes go down, you can use <<< >>> to repeat both text and variables. See the examples below.

This message with no repeater displays every node that is down in a separate sentence: **${N=SwisEntity;M=Caption}** is **${N=SwisEntity;M=Status;F=Status}**.

This message displays only the text included in the repeater, in this case each node that is down: **<<< ${N=SwisEntity;M=Caption}>>>** is **${N=SwisEntity;M=Status;F=Status}**.

This message displays each node that is down and the status of each node: **<<< ${N=SwisEntity;M=Caption}** is **${N=SwisEntity;M=Status;F=Status}.>>>**

Note: When using a repeater, you cannot use the PREVIOUS variable.

Using Macro Formatters

Be aware that using macro formatters can significantly change the macro result. For example:

${N=Generic;M=Date;F=**Date**} - Tuesday, December 2, 2014

${N=Generic;M=Date;F=**OriginalValue**} - 12/2/2014

These formatters are available in the UI from the macro variable picker, and a different set of formatters is available depending on the variable value type.

Status Icons and Identifiers

NPM and Orion modules use a number of different icons as status indicators. In the case of alerts and events, further information is provided with the icon within the resource.

Status Indicators

The following table lists SolarWinds NPM icons with associated status indications, status types, and numerical status identifiers, proceeding from the worst.

Note: Status levels of type Ignore are not displayed in any status rollup mode.

Icon	Status Indication	Type	ID
	Node or Interface is Down (Polling request timed-out)	Error	2
	Shutdown	Error	4
	Lower Layer Down	Error	8
	Unreachable	Error	12
	Node is in a Warning state (dropped packets or down interface)	Warning	3
	Critical	Warning	14
	Mixed Availability	Warning	15
	Misconfigured	Warning	16
	Could Not Poll	Warning	17
	Unconfirmed	Warning	19
	Polling Engine Shutdown, Monitoring Stopped, System Error, or Fail Over	Warning	--

Icon	Status Indication	Type	ID
	System Warning; Node, Interface, or Volume Changed; Interface Reappeared; Network Baseline Started/Finished	Warning	--
	Node or Interface is Up	OK	1
	Dormant	OK	6
	Active	OK	22
	Inactive	OK	24
	Expired	OK	25
	Unknown	Ignore	0
	Node or Interface is Unmanaged	Ignore	9
	Interface is Unplugged but not Down	Ignore	10
	Node is defined as External (Not monitored by SolarWinds NPM, but an application or component on the node may be monitored by SAM.)	Ignore	11
	Monitoring Disabled	Ignore	26
	Disabled	Ignore	27
	Not Licensed	Ignore	28
	Informational; Volume Reappeared	N/A	--
	Monitoring Started, NPM Service Started, or Fail Back	N/A	--
	Node, Interface, or Volume Removed Interface Shutdown	N/A	--
	Node Added	N/A	--

Icon	Status Indication	Type	ID
	Interface or Volume Added (Web Console)	N/A	--
	Node Rebooted	N/A	--
	Interface Enabled	N/A	--
	Interface Remapped	N/A	--
	Volume Remapped	N/A	--
?	Interface or Volume Disappeared	N/A	--

Status Rollup Mode

In the Orion Web Console, the Status Rollup Mode designates how the availability status of a group of nodes is displayed.

Three options are available for the case when there are objects at different status levels in a selected group:

- **Show Best Status** is most useful for displaying groups that are defined as collections of redundant or backup devices. The following table indicates how the **Show Best Status** option operates:

  Note: Compare Group Status results under the Show Best Status option with results for the same groups of objects under the Show Worst Status option.

Object States	Group Status
(Up, Warning, Down)	(Up)
(Warning, Down)	(Up)
(Warning, Down, Unknown)	(Warning)

- **Show Worst Status** ensures that the worst status in a group of objects is displayed for the whole group. The following table indicates how the **Show Worst Status** option operates:

Object States	Group Status
(Up, Warning, Down)	(Down)
(Warning, Down)	(Warning)
(Warning, Down, Unknown)	(Down)

- **Mixed Status shows Warning** ensures that the status of a group displays the worst warning-type state in the group. If there are no warning-type states, but the group contains a mix of up and down states, then a Mixed Availability ( ) warning status is displayed for the whole group. The following table indicates how the **Mixed Status shows Warning** option operates:

Object States	Group Status
	(Critical)
	(Critical)
	(Mixed Availability)

Regular Expression Pattern Matching

When editing comparison criteria, the following regular expressions can be used for pattern matching. Examples are provided at the end of this section.

Characters

Character	Description	Example
Any character except [,\,^,$,.,|,?,*,+,(,),	All characters except the listed special characters match a single instance of themselves.	a matches a
\ (backslash) followed by any of [,\,^,$,.,|,?,*,+,(,),	A backslash escapes special characters to suppress their special meaning.	\+ matches +
\xFF where FF are 2 hexadecimal digits	Matches the character with the specified ASCII/ANSI value, which depends on the code page used. Can be used in character classes.	\xA9 matches © when using the Latin-1 code page.
\n, \r and \t	Match an LF character, CR character and a tab character respectively. Can be used in character classes.	\r\n matches a DOS/Windows CRLF line break.

Character Classes or Character Sets [abc]

Character Classes or Sets	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

Character Classes or Sets	Description	Example
^ (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

Anchors

Anchors	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.

Anchors	Description	Example
$ (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.	.$ 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

Quantifiers

Quantifiers	Description	Example
? (question mark)	Makes the preceding item optional. The optional item is included in the match, if possible.	abc? matches ab or abc

Quantifiers	Description	Example
??	Makes the preceding item optional. The optional item is excluded in the match, if possible. This construct is often excluded from documentation due to its limited use.	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
*? (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

Quantifiers	Description	Example
{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

Dot

Dot Character	Description	Example
. (dot)	Matches any single character except line break characters \r and \n.	. matches x or most any other character

Word Boundaries

Word Boundary	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

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

Regular Expression Pattern Matching Examples

The following examples illustrate general 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.

service tcp-keepalives-in.*\n(.*\n)*.*service tcp-keepalives-out

Finds the first line **service tcp-keepalives-in** and then looks for **service tcp-keepalives-out** on any line after that. The regular expression string **.*\n (.*\n)*.*** is used to search any number of lines between strings.

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 log** on the same line. The regular expression string **.*** finds any character and any number of characters on the same line. This expression can 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**.

The following examples illustrate the use of SQL string and regular expression pattern matching in Syslog messages and rules.

Web Console and Syslog Viewer (Search Messages tab)

Regular expression search for syslog messages is not currently supported. Matching is only available on simple SQL string patterns, where `?` or _ are used to indicate single, replaced characters and where `*` or `%` are used to indicate zero characters or to delineate multiple characters, as indicated in the following examples:

IP Address filter:

- `192.168.74.*` - IP addresses in range `192.168.74.1 - 192.168.74.255`
- `192.168.74.?` (or `192.168.74._`) - IP addresses in range `192.168.74.1 - 192.168.74.9`

- `*.168.74*` (or `%.168.74%`) - IP addresses containing `.168.74`
- `%.74.25` (or `*.74.25`) - IP addresses ending with `.74.25`

Message Type filter:

- `orion*` (or `orion%`) - message type starts with "`orion`"
- `message????` - message type starts with "`message`" plus any 4 symbols, like "`message1234`"
- `%orion%` (or `*orion*`) - message type contains "`orion`"

Message Pattern filter:

- `syslog message from 192.168.*` - message starts with "`syslog message from 192.168.`"
- `*Server_ *` messages containing the word "`Server`" and any symbol before the space.

Syslog Rules

Syslog rules allow you to filter matching messages using a Regex pattern or simple SQL string patterns, provided the **Use regular expressions** option is enabled. Regular expressions may be used in syslog message filtering, as follows:

DNS Hostname pattern

- `.*domain.com$` - DNS name ends with `domain.com`
- `^Orion.*` - DNS name starts with `Orion`.
- `.*Orion.*` - DNS name contains `Orion`

Message Type Pattern

- `^[A,B,C]` - message type starts with `A`, `B` or `C`.
- `^[0-9].*log$` - message type starts with number value from `1` to `9` and ends with `log`.

Message Pattern

- `.*[^0-9]10.0.0.1[^0-9].*` - message contains IP address `10.0.0.1`

- `^Orion.*[^0-9]10.0.0.1[^0-9].*` message starts with `Orion` and contains IP address `10.0.0.1`.
  Note: "`.*`" could be omitted at both the end and the beginning of the expression.

95th Percentile Calculations

Calculation of the 95th percentile, a well-known statistical standard used to discard maximum spikes, is based on 5 minute data samples. The calculation gathers these values every 5 minutes for however long you select, throws away the top 5%, yielding the 95th percentile value at the beginning of the list.

Consider the following example of how the 95th percentile is calculated for a 10 hour work day from 8am to 6pm (600 minutes):

1. Over the 10 hours, the following 120 values were collected for inbound traffic (Mb/s):

   0.149 0.623 0.281 0.136 0.024 0.042 0.097 0.185 0.198 0.243 0.274 0.390
   0.971 0.633 0.238 0.142 0.119 0.176 0.131 0.127 0.169 0.223 0.291 0.236
   0.124 0.072 0.197 0.105 0.138 0.233 0.374 0.290 0.871 0.433 0.248 0.242
   0.169 0.116 0.121 0.427 0.249 0.223 0.231 0.336 0.014 0.442 0.197 0.125
   0.108 0.244 0.264 0.190 0.471 0.033 0.228 0.942 0.219 0.076 0.331 0.227
   0.849 0.323 0.221 0.196 0.223 0.642 0.197 0.385 0.098 0.263 0.174 0.690
   0.571 0.233 0.208 0.242 0.139 0.186 0.331 0.124 0.249 0.643 0.481 0.936
   0.124 0.742 0.497 0.085 0.398 0.643 0.074 0.590 0.771 0.833 0.438 0.242
   0.092 0.376 0.231 0.627 0.249 0.663 0.181 0.636 0.224 0.342 0.697 0.285
   0.108 0.211 0.074 0.490 0.271 0.133 0.338 0.242 0.519 0.376 0.331 0.227

2. When reordered from high to low:

   0.971 0.942 0.936 0.871 0.849 0.833 0.771 0.742 0.697 0.690 0.663 0.643
   0.643 0.642 0.636 0.633 0.627 0.623 0.590 0.571 0.519 0.497 0.490 0.481
   0.471 0.442 0.438 0.433 0.427 0.398 0.390 0.385 0.376 0.376 0.374 0.342
   0.338 0.336 0.331 0.331 0.331 0.323 0.291 0.290 0.285 0.281 0.274 0.271
   0.264 0.263 0.249 0.249 0.249 0.248 0.244 0.243 0.242 0.242 0.242 0.242
   0.238 0.236 0.233 0.233 0.231 0.231 0.228 0.227 0.227 0.224 0.223 0.223
   0.223 0.221 0.219 0.211 0.208 0.198 0.197 0.197 0.197 0.196 0.190 0.186
   0.185 0.181 0.176 0.174 0.169 0.169 0.149 0.142 0.139 0.138 0.136 0.133
   0.131 0.127 0.125 0.124 0.124 0.124 0.121 0.119 0.116 0.108 0.108 0.105
   0.098 0.097 0.092 0.085 0.076 0.074 0.074 0.072 0.042 0.033 0.024 0.014

3. Drop the first 6, as these equal the top 5% of the values:

   0.771 0.742 0.697 0.690 0.663 0.643 0.643 0.642 0.636 0.633 0.627 0.623 0.590 0.571 0.519 0.497 0.490 0.481 0.471 0.442 0.438 0.433 0.427 0.398 0.390 0.385 0.376 0.376 0.374 0.342 0.338 0.336 0.331 0.331 0.331 0.323 0.291 0.290 0.285 0.281 0.274 0.271 0.264 0.263 0.249 0.249 0.249 0.248 0.244 0.243 0.242 0.242 0.242 0.242 0.238 0.236 0.233 0.233 0.231 0.231 0.228 0.227 0.227 0.224 0.223 0.223 0.223 0.221 0.219 0.211 0.208 0.198 0.197 0.197 0.197 0.196 0.190 0.186 0.185 0.181 0.176 0.174 0.169 0.169 0.149 0.142 0.139 0.138 0.136 0.133 0.131 0.127 0.125 0.124 0.124 0.124 0.121 0.119 0.116 0.108 0.108 0.105 0.098 0.097 0.092 0.085 0.076 0.074 0.074 0.072 0.042 0.033 0.024 0.014

4. The 95th percentile is **0.771**.

Appendix B: Technical References

This section provides information available as technical references from the SolarWinds documentation page for individual SolarWinds products. The one-off documents have been written to resolve an issue frequently being solved by the SolarWinds support team. The documents are provided as is and are subject to update.

- Migrating SolarWinds Network Performance Monitor
- Introduction to Integrated Virtual Infrastructure Monitoring
- WAN Optimization
- Setting Up a Cisco Unified Computing System as a Managed Node

Migrating SolarWinds Network Performance Monitor

Migrating SolarWinds NPM to a different server is a process that can take as little as 30 minutes or as long as several hours, depending on the size of your SolarWinds Orion database.

Depending on the complexity of your implementation, you may need to perform a number of different procedures when transferring SolarWinds NPM and any modules to different hardware.

Consider scheduling an appropriate maintenance window in which to perform your migration.

Pre-Requisites

Before you start the migration, take into account the following considerations:

- What are you migrating?

  Supposing that you have the SolarWinds Orion database installed on a dedicated server, you might want to move SolarWinds NPM and the Orion platform products, the SolarWinds Orion database or both.

- Check Requirements

  Make sure all general requirements are met. For more information, see General requirements.

  If you are moving the SolarWinds Orion database, make sure the SQL Server is already installed on the appropriate server. For more information, see SolarWinds Orion database requirements.

Migrating both SolarWinds NPM and the SolarWinds Orion database

Migrating both SolarWinds NPM and the SolarWinds Orion database

If you are moving both SolarWinds NPM and the SolarWinds Orion database to new servers, you need to back up the database, install SolarWinds NPM on a new server, restore the database, and migrate the license. Optionally, you can also uninstall SolarWinds NPM on the original server.

To migrate both SolarWinds NPM and SolarWinds Orion database:

1. Stop Services on the original SolarWinds NPM server. For more information, see Stopping SolarWinds services.
2. Back up your SolarWinds Orion database using the SQL Server Management Studio. For more information, search for "back up a database" on the Microsoft TechNet web portal at https://technet.microsoft.com, and consult the help for the appropriate SQL Server Management Studio version.
3. Restore the SolarWinds Orion database on the new server. For more information, search for "restore a database backup" on the Microsoft TechNet web portal at https://technet.microsoft.com, and consult the help for the appropriate SQL Server Management Studio version.

   Note: While restoring the database, use the **Restore with Recovery** option.

4. Install and configure SolarWinds NPM on the new server.

   To install SolarWinds NPM, run the SolarWinds NPM executable and complete the Installation Wizard. For more information, see Completing an SolarWinds NPM Installation in the *SolarWinds Network Performance Monitor Administrator Guide*.

   For more information about configuring SolarWinds NPM, see Updating SolarWinds NPM to use the new SolarWinds Orion database.

5. Migrate your SolarWinds license. This requires deactivating your license on the original SolarWinds NPM server, and re-activating it on the new SolarWinds NPM server. For more information, see Deactivating and Registering Licenses with the License Manager.

6. If you are also running further SolarWinds products, such as SAM, NCM, or NTA, you might need to adjust some product-relevant settings for the appropriate products:
    - For more information about moving SAM certificates, see Moving SolarWinds SAM security certificates to a new server.
    - For more information about moving NCM certificates, see Moving the SolarWinds NCM integration component.
    - For more information about changing SQL Server settings on the NTA Flow Storage Database server, see Adjusting SQL server information on NTA Flow Storage Database server.
7. Reassign nodes. For more information, see Reassigning nodes.
8. If you are using customized Report-Writer reports, copy the customized reports. For more information, see Copying customized reports.
9. Update reports schemas. For more information, see Updating report schemas.
10. Uninstall SolarWinds NPM on the old server. For more information, see Uninstalling SolarWinds NPM from the old server.

Migrating SolarWinds NPM

Migrating SolarWinds NPM

If you are only migrating SolarWinds NPM, and the database stays on the original server, just install and configure SolarWinds NPM, and migrate your license.

To migrate only SolarWinds NPM:

1. Install SolarWinds NPM on a new server and run the Configuration Wizard.

   To install SolarWinds NPM, run the SolarWinds NPM executable and complete the Installation Wizard. For more information, see Completing an SolarWinds NPM Installation in the *SolarWinds Network Performance Monitor Administrator Guide*.

   For more information about configuring SolarWinds NPM, see Updating SolarWinds NPM to use the new SolarWinds Orion database.

2. Migrate your SolarWinds license. This requires deactivating your license on the original SolarWinds NPM server, and re-activating it on the new SolarWinds NPM server. For more information, see Deactivating and Registering Licenses with the License Manager.
3. If you are also running further SolarWinds products, such as SAM, NCM, or NTA, you might need to adjust some product-relevant settings for the appropriate products:
   - For more information about moving SAM certificates, see Moving SolarWinds SAM security certificates to a new server.
   - For more information about moving NCM certificates, see Moving the SolarWinds NCM integration component.
4. Reassign nodes. For more information, see Reassigning nodes.
5. If you are using customized Report-Writer reports, copy the customized reports. For more information, see Copying customized reports.
6. Uninstall SolarWinds NPM on the old server. For more information, see Uninstalling SolarWinds NPM from the old server.

Migrating the SolarWinds Orion database

Migrating the SolarWinds Orion database

If you move just the SolarWinds Orion database and keep SolarWinds NPM on the original server, you only need to back up your SolarWinds Orion database, restore it on the new server, and run the Configuration Wizard to adjust the SQL Database details to the new server.

To migrate the SolarWinds Orion database:

1. Stop Services on the original SolarWinds NPM server. For more information, see Stopping SolarWinds services.
2. Back up your SolarWinds Orion database. For more information, search for "back up a database" on the Microsoft TechNet web portal at https://technet.microsoft.com, and consult the help for the appropriate SQL Server Management Studio version.
3. Restore the SolarWinds Orion database on the new server. For more information, search for "restore a database backup" on the Microsoft TechNet web portal at https://technet.microsoft.com, and consult the help for the appropriate SQL Server Management Studio version.

   Note: While restoring the database, use the **Restore with Recovery** option.
4. Log in to the SolarWinds NPM Server, run the Configuration Wizard, and provide the new SolarWinds Orion database details.
5. If you are also running SolarWinds NTA, you might need to adjust the SQL Server settings on the NTA Flow Storage Database server. For more information, see Adjusting SQL server information on NTA Flow Storage Database server.

If you have any questions about this process, contact support@solarwinds.com.

General requirements

Moving your SolarWinds NPM implementation to a new server requires the following:

- Server hardware meeting minimum requirements for the new SolarWinds NPM implementation. For more information about SolarWinds NPM requirements, see NPM Requirements in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

- Windows user account credentials that have been granted administrative rights on both servers.
- A license reset to register SolarWinds NPM on your new server. You will need to install SolarWinds License Manager to manage the required license migration. For more information, see Maintaining Licenses in the *SolarWinds Orion Common Components Administrator Guide*.

  Note: Maps and map objects created or edited in Orion Network Atlas are stored in the SolarWinds Orion database. If the database is successfully migrated, there is no need to migrate any additional Network Atlas map files.

SolarWinds Orion database requirements

Ensure that you comply with the following requirements before you attempt to modify or back up your existing database:

- Make sure the new SolarWinds Orion database server meets the requirements of your product. SolarWinds NPM 11.5.2 requires SQL Server 2008 or higher. For more information, see Requirements for the Orion Database Server in the *Orion Common Components Administrator Guide*.
- Install your new database server. The following procedures assume you are moving your database from one physical server to another and that the management tool (Enterprise Manager, SQL Server Management Studio Express, or SQL Server Management Studio) is installed on the new database server.
- If you want to use a Microsoft SQL Server Express 2005 or 2008, recognize that the database store is limited to 4 GB. If you are running Microsoft SQL 2008 R2 or a higher version, the database limit is 10 GB.
- Know the **sa** password to both your existing Orion database server and your new database server.
- Know the credentials to an account with administrator rights on both your existing SolarWinds Orion database server and your new database server.
- Have a maintenance window during which you can safely shutdown appropriate SolarWinds services. You need to stop data collection to ensure that your backup file matches your last active database state.

Stopping SolarWinds services

It is important to stop the SolarWinds services that are currently writing to the database. This ensures that you do not have data inconsistencies when you bring your new database server online.

To stop SolarWinds services:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Orion Service Manager**.
2. Click **Shutdown all services**.

   Notes for older SolarWinds NPM versions:

   - If you are running SolarWinds NPM 10.2.2 or older, select each service, except the SQL Server service, and then click **Stop**.
   - If you have more than one Polling Engine, you will need to stop each additional Polling Engine before continuing.
   - Do not stop the SQL Service. The SQL Service needs to be running in order to make the necessary changes to the database.
3. Click **File > Exit**.

Updating SolarWinds NPM to use the new SolarWinds Orion database

After you have restored your SolarWinds Orion database backup file, you must update your SolarWinds NPM 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 NPM can always access your SolarWinds Orion database, even when it is hosted remotely on a separate server.

To update SolarWinds NPM to use a new database:

1. Log on to your SolarWinds NPM server.
2. If you are only migrating SQL Server and you have SolarWinds NTA with remote NTA Flow Storage Database installed, you must uninstall SolarWinds NTA from the main Orion server before proceeding. Data remains untouched.

3. Click **Start > All Programs > SolarWinds Orion > Configuration and Auto-Discovery > Configuration Wizard**.

   Note: In older versions of SolarWinds NPM, the correct path may be **Start > All Programs > SolarWinds Orion > Configuration Wizard**.

4. Check **Database**, and then click **Next**.
5. Specify your new database server in the **SQL Server** field.
6. ***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 SolarWinds Orion database user account.

7. Click **Next**.
8. Select **Use an existing database**, select or type the **Existing Database** name, and then click **Next**.
9. ***If you are prompted to use the existing database***, click **Yes**.
10. Select **Create a new account**, and then provide a **New Account** name.

    Notes:

    - Creating a new account ensures that SolarWinds NPM has required access to your migrated database.
    - The **New Account** must be a member of the **securityadmin** server role.
    - The sysadmin role and the **sa** user account are always members of **securityadmin**.

11. Provide and confirm an account **Password**.
12. Click **Next** to start database configuration, and then click **Finish** to exit the Configuration Wizard.

13. If you uninstalled SolarWinds NTA in step 2, do the following:
    a. Adjust the SQL Server settings on the NTA Flow Storage Database server. For more information, see Adjusting SQL server information on NTA Flow Storage Database server.
    b. Install SolarWinds NTA on the main Orion server.

Reassigning nodes

Configuration Wizard configures all settings necessary for SolarWinds NPM. However, if the nodes stay assigned to the original polling engine after the migration, you might need to reassign them manually.

If a new name is used for the new SolarWinds NPM server, it is added to the database as a new polling engine. All current nodes remain assigned to the old polling engine name and must be reassigned to the new polling engine, as shown in the following procedure.

To reassign items to the new polling engine:

1. Start the **Orion Service Manager** in your **SolarWinds Orion > Advanced Features** program folder.
2. Stop all SolarWinds services.

   Notes:

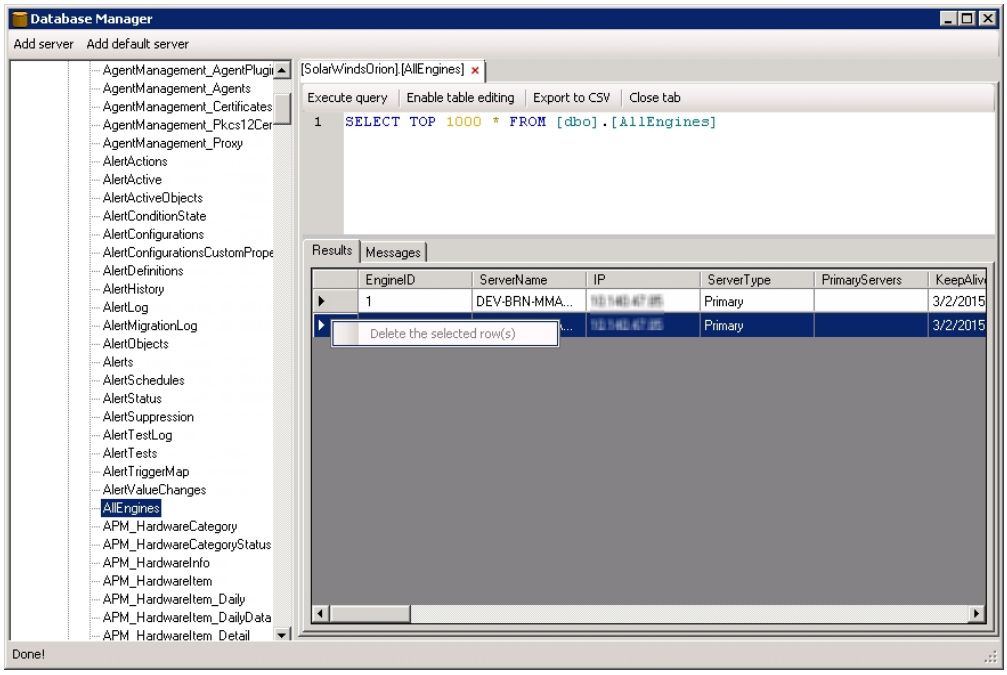
   - If you have more than one Polling Engine, you will need to stop each additional Polling Engine before continuing.
   - Do not stop the SQL Service. The SQL Service needs to be running in order to make the necessary changes to the database.
3. Click **File > Exit**.
4. Start the **Database Manager** in your **SolarWinds Orion > Advanced Features** program folder.
5. Expand your SQL Server in the tree.
6. Expand the SolarWinds Orion database.

   Note: By default, this database is named **SolarWindsOrion**.
7. Right-click on the **AllEngines** table, and then click **Query Table**.
8. Click **Execute query** to display the table entries.

9. Select **Enable table editing**.
10. Replace the value in the **ServerName** field for the old polling engine with the server name of the new polling engine.

    Note: It is not necessary to update the **IP** field. The next time the service is started, SolarWinds NPM discovers the new **IP** address, and the IP field is updated automatically.

11. Right-click the left-most cell in the old polling engine row and then click **Delete the selected row(s)**.



12. Click **Yes** when prompted to confirm deleting the row.

    Note: The final result will display the new server name with the IP address of the old server. The next time the service starts, the IP field will be updated with the IP address of the new server.

13. Close the Database Manager.
14. Restart all services on all polling engines using the Orion Service Manager.

Copying customized reports

There are two report types in SolarWinds NPM - web-based reports, and archaic Report Writer reports. Web-based reports are stored in the SolarWinds Orion database, and are thus automatically moved together with the database.

If you have customized Report Writer reports, you might need to copy them manually to the new SolarWinds NPM server.

To copy your reports:

1. On the old server, copy your custom reports located in the **\Orion\Reports** folder.
2. Paste these reports into the **Orion\Reports** folder on the new server.

Updating report schemas

If you have added custom properties to the database, you will need to upgrade the report schemas on the new server. Updating the report schemas allows Report Writer to display and use custom property information.

To update report schemas for custom properties:

1. Ensure that Report Writer is closed, and then click **Start > All Programs > SolarWinds Orion > Advanced Features > Custom Property Editor**.
2. Right-click on the toolbar, and then click **Customize**.
3. Click the Commands tab.
4. Click the **Properties** in the category list.
5. Drag **Update Report Schemas** to the toolbar to add a new button to the toolbar.
6. Close the Customize window.
7. Click **Update Report Schemas** on the toolbar.
8. Click **OK** after the custom properties have been added to the report schemas.
9. Close Custom Property Editor.

Moving SolarWinds SAM security certificates to a new server

SolarWinds SAM encrypts your sensitive data with a security certificate stored on the original SolarWinds SAM server. To grant a new server access to this encrypted data, you must copy the original security certificate to the new server.

Warning: If you do not replicate the original certificate, SolarWinds SAM on the new server cannot access any credentials used by your component monitors, and all of those component monitors will fail.

To replicate the original certificate:

1. Export the credential from the original server.
    a. On the Start Menu, click **Run**, type **MMC**, and then click **OK**.
    b. On the **File** menu, click **Add/Remove Snapin**, and then click **Add**.
    c. Select **Certificates** and then click **Add**.
    d. Select **Computer account** and then click **Next**.
    e. Select **Local computer** and then click **Finish**.
    f. Click **Close**.
    g. Click **OK**.
    h. Expand the **Certificates (Local Computer) > Personal > Certificates** group.
    i. Right-click **SolarWinds Agent Provision** (if present), and **SolarWinds-Orion**, point to **All Tasks** on the shortcut menu, and then click **Export**.
    j. Click **Next** in the Certificate Export Wizard.
    k. Select **Yes**, export the private key, click **Next**, and then click **Next** again.
    l. Type and confirm a password for this private key, and then click **Next**.
    m. Specify the file name to which you want to save the certificate, click **Next**, and then click **Finish**—the certificate is saved with a **.pfx** file name extension.
2. Copy the **.pfx** certificate file to the new server.
3. Import the certificate to the new server.

a. On the Start Menu, click **Run**, type **MMC**, and then click **OK**.
b. On the **File** menu, click **Add/Remove Snapin**, and then click **Add**.
c. Select **Certificates**, and then click **Add**.
d. Select **Computer account**, and then click **Next**.
e. Select **Local computer**, and then click **Finish**.
f. Click **Close**.
g. Click **OK**.
h. Expand the **Certificates (Local Computer)** group.
i. Expand the **Personal** group.
j. Expand the **Certificates** group.
k. ***If there is a SolarWinds SAM Engine item in the list***, right-click **SolarWinds Agent Provision** and **SolarWinds-Orion** and select **Delete** from the shortcut menu.
l. Right-click the **Certificates—Personal—Certificates** node, point to **All Tasks** in the shortcut menu, and then click **Import**.
m. Click **Next** in the Certificate Import Wizard.
n. Specify the `.pfx` certificate file you copied to the server and then click **Next**.
o. Enter the password for the private key, check **Mark this key as exportable**, and then click **Next**.
p. Select **Place all certificates in the following store**, and then select **Personal** as the Certificate Store.
q. Click **Next** and then click **Finish**.

Moving the SolarWinds NCM integration component

The SolarWinds NCM integration component encrypts your sensitive data with a security certificate stored on the original SolarWinds NPM server. If you have the SolarWinds NCM integration component installed, you might need to grant the additional web console access to the encrypted data.

To grant access to the encrypted data:

1. Export the SolarWinds NCM Certificate from the SolarWinds NPM. For more information, see Exporting NCM integration engine certificate.
2. Import the certificate file to the SolarWinds NPM additional web console. For more information, see Importing certificate file to SolarWinds NPM Additional Web Console.

Exporting NCM integration engine certificate

Export the SolarWinds NCM Integration Engine certificate from the SolarWinds NPM server.

To export the certificate:

1. On the **Start** Menu, click **Run**, type **MMC**, and then click **OK**.
2. On the **File** menu, click **Add/Remove Snapin**, and then click **Add**.
3. Select **Certificates**, and then click **Add**.
4. Select **Computer** account, and then click **Next**.
5. Select **Local computer**, and then click **Finish**.
6. Click **Close**.
7. Click **OK**.
8. Expand the **Certificates (Local Computer)** group.
9. Expand the **Personal** group.
10. Expand the **Certificates** group.
11. Right-click **Orion NCM Integration Engine**, point to **All Tasks** on the shortcut menu, and then click **Export**.
12. Click **Next** in the Certificate Export Wizard.
13. Select **Yes, export the private key**, click **Next**, and then click **Next** again.
14. Type and confirm a password for this private key, and then click **Next**.
15. Specify the file name to which you want to save the certificate, click **Next**, and then click **Finish**—the certificate is saved with a .pfx file name extension.

Importing certificate file to SolarWinds NPM Additional Web Console

To import the certificate file to the SolarWinds NPM additional web console, complete the following procedure.

To import the SolarWinds NCM certificate file to an additional web console:

1. Copy the .pfx certificate file to the computer running the SolarWinds NPM additional web console.
2. On the **Start** Menu, click **Run**, type **MMC**, and then click **OK**.
3. On the **File** menu, click **Add/Remove Snapin**, and then click **Add**.
4. Select **Certificates**, and then click **Add**.
5. Select **Computer** account, and then click **Next**.
6. Select **Local computer**, and then click **Finish**.
7. Click **Close**.
8. Click **OK**.
9. Expand the **Certificates (Local Computer)** group.
10. Expand the **Personal** group.
11. Expand the **Certificates** group.
12. Point to **All Tasks** in the shortcut menu, and then click Import.
13. Click **Next** in the Certificate Import Wizard.
14. Specify the .pfx certificate file you copied to the server, and then click **Next**.
15. Enter the password for the private key, check **Mark this key as exportable**, and then click **Next**.
16. Select **Place all certificates in the following store**, and then select **Personal** as the Certificate Store.
17. Click **Next**, and then click **Finish**.

Adjusting SQL server information on NTA Flow Storage Database server

If you are also running SolarWinds NTA, migrating the SolarWinds Orion database might require further settings on the NTA Flow Storage Database server.

SolarWinds NTA stores flows in the NTA Flow Storage Database. However, NTA also uses information from the SolarWinds Orion database. If you therefore migrate your SolarWinds Orion database, you need to adjust the SolarWinds Orion database server settings on the NTA Flow Storage Database server.

Warning: If the NTA Flow Storage Database is not empty, and you are connecting it to an empty SQL Database, you must delete all data from the NTA Flow Storage Database. Otherwise, the existing data might be associated with wrong nodes and interfaces.

To adjust SolarWinds Orion database server settings after the migration:

1. Log on to your remote NTA Flow Storage Database server.
2. Start the **NTA Flow Storage Configurator** in the **SolarWinds Orion > NetFlow Traffic Analysis** program folder.
3. Fill in the new SQL Database server data and click **OK**.

For more information about migrating the NTA Flow Storage Database, see Moving the NTA Flow Storage Database in the *NTA online documentation*.

Installing License Manager

Install License Manager on the computer on which you want to activate, upgrade or synchronize your license or on which you want to deactivate currently licensed products.

Warning: You must install License Manager on a computer with the correct time. If the time on the computer is even slightly off, in either direction, from Greenwich Mean Time (GMT), you cannot reset licenses without contacting SolarWinds Customer Service. Time zone settings neither affect nor cause this issue.

To install License Manager via SolarWinds UI:

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

   Note: If problems with License Manager occur, download and install the latest version of License Manager.

2. Click **Next** to accept the SolarWinds EULA.
3. ***If you are prompted to install the SolarWinds License Manager application,*** click **Install**.

Downloading the License Manager from the Internet

To download and install the latest version of the License Manager:

1. Navigate to http://solarwinds.s3.amazonaws.com/solarwinds/Release/LicenseManager/LicenseManager.zip.
2. Unzip the downloaded file, and then run LicenseManager.exe.

Deactivating and Registering Licenses with the License Manager

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

To be able to deactivate and reuse a license without contacting SolarWinds Customer Service, your product needs to be under active maintenance.

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

   The deactivated licenses are now available to activate on a new computer.

If you deactivated a license on an offline computer, or if you do not have active maintenance, contact Customer Support at maintenance@solarwinds.com to reuse the available license.

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

Uninstalling SolarWinds NPM from the old server

Once you have completed the previous steps, check System Manager to ensure that all your nodes were transferred successfully. Verify that your alerts, reports, and maps were copied properly, and then check the SolarWinds NPM website to ensure that everything was successfully migrated. As a last step, fully uninstall SolarWinds NPM from the old server, as shown in the following procedure.

To uninstall SolarWinds NPM from the old server:

1. Log on to the old SolarWinds NPM server and click **Start > Control Panel > Add or Remove Programs**.
2. Click **SolarWinds Orion Network Performance Monitor**, and then click **Remove**.

   Note: If you are uninstalling SolarWinds NPM version 8.1 or earlier, click **Start > SolarWinds Orion Network Performance Monitor > Uninstall > Uninstall Orion Network Performance Monitor**.
3. Complete the uninstall wizard, being sure to remove all shared components when prompted.

Introduction to Integrated Virtual Infrastructure Monitoring

SolarWinds Orion Integrated Virtual Infrastructure Monitoring (IVIM) built into NPM lets you monitor today's modern network fabric of virtual networks, virtualized data centers, and private clouds. The deep visibility into your virtualized environments helps you ensure that network performance helps and not hinders your virtualization projects.

VMware Monitoring

Monitor your entire VMware virtual infrastructure from the highest to the lowest level: vCenter → datacenter → cluster → ESX hosts → individual virtual machines. Track availability and performance metrics including CPU, memory, storage, and network bandwidth utilization.

Virtual Machine Auto-Summary

Automatically discover, identify, and monitor new virtual machines added to any VMware host server or updated during vMotion.

Virtualization Alerting and Reporting

The native alerting and reporting capabilities of SolarWinds Orion extend seamlessly to your virtual infrastructure.

For more extensive virtualization monitoring, integrate SolarWinds NPM with SolarWinds Virtualization Manager. For more information, see Virtualization Manager on the SolarWinds website.

Requirements for IVIM

VMware ESX or vCenter accounts used as credentials must have read-only permissions as a minimum.

Activating and Licensing IVIM

There is no separate activation or licensing for SolarWinds Orion IVIM. It is included with the latest version of SolarWinds Orion Network Performance Monitor (SolarWinds NPM).

Managing VMware Assets

The primary way of adding VMware servers to SolarWinds Orion is through the Network Sonar Wizard, but it is also possible to add individual VMware virtual machines (VMs) from the VMware Assets resource.

Polling for VMware Nodes Using the Network Sonar Wizard

Add VMware Vcenter, ESX servers, virtual machines from the Network Sonar Wizard by checking the Poll for VMware option in the wizard. For more information, see Discovering and Adding Network Devices in the SolarWinds Orion Core Administrator Guide.

Adding VMs from the VMware Assets Resource

1. Log in to the web console.
2. Depending on your setup and whether you have Virtualization Manager integrated with Orion, go to either **Virtualization Tab > Virtualization Summary**, or **Home > Virtualization**.
3. Click the **[+]** next to any ESX or VCenter server listed in the **VMware Assets** resource to expand the list of virtual machines.
4. Click a virtual machine that is not currently managed by SolarWinds Orion. Unmanaged VMs are listed in italic type.
5. Click **Manage This Node**.
6. If the VM is not running VMware Tools, manually enter the IP address of the VM in the **Polling Hostname or IP Address** field.
7. Select any additional options required to monitor the VM, and then click **Next**.
8. Follow the remainder of the Add Node wizard to completion, and then click **OK**, **Add Node**.

Viewing the Virtualization Summary

The Virtualization Summary view shows the overall status of your virtualized infrastructure.

To view the Virtualization Summary:

1. Log in to the web console.
2. Depending on your setup and whether you have Virtualization Manager integrated with Orion, go to either **Virtualization Tab > Virtualization Summary**, or **Home > Virtualization**.

The Virtualization Summary view is pre-configured to display the following resources:

Top 10 Hosts by CPU Load	**Top 10 Hosts by Number of Running VMs**
Top 10 Hosts by Percent Memory Used	Top 10 Hosts by Network Utilization
Virtualization Assets	Virtualization Asset Summary
VMware vCenters with Problems	Virtual Clusters with Problems
Hosts with Problems	Guests with Problems

Click **Edit** in the resource to change the properties or contents of any resource.

Viewing ESX Host Details

The ESX Host Details page is displayed when you click an ESX Host server in the Virtualization Summary. This page displays the following resources:

Virtualization Manager Tools	Polling Details
Average Response Time & Packet Loss Graph	Availability Statistics
Virtualization Assets	Virtual Machine CPU Consumption
CPU Load & Memory Utilization Gauge	Guests with Problems
ESX Host Details	Custom properties for Nodes
Management	List of Virtual Machines

Node Details	Average Response Time & Packet Loss
Event Summary	Min/Max Average CPU Load Graph
Top CPUs by PercentLoad	Disk Volumes
Active Alerts on this Node	Virtual Machine Memory Consumption
Virtual Machine Network Traffic	

Click **Edit** in the resource to change the properties or contents of any resource.

Changing Polling Orders for ESX Servers

If your VMware ESX hosts are controlled by VMware vCenter servers, SolarWinds Orion obtains the status of the ESX hosts from the vCenter server instead of polling the ESX hosts directly.

To poll the ESX servers directly you must change the Poll Through setting of the ESX host from the VMware Settings page. From this page, you can also disable and enable polling for ESX hosts and vCenter servers.

To poll a vCenter-managed ESX Host from the SolarWinds Orion server:

1. Log in to the web console.
2. Click **Settings**.
3. In the Settings grouping, click **Virtualization Settings > VMware Settings**.
4. Point to any column heading, click the drop-down arrow, and then click **Columns > Polling Through**.
5. Select the ESX hosts you want to poll directly.
6. Click **Poll Through > Poll ESX server directly**.

Updating VMware Credentials

If you want to update the user name or password of a VMware credential, you can do so from the VMware Credentials Library tab.

To update a VMware credential:

1. Log in to the web console.
2. Click **Settings**.
3. In the Settings grouping, click **Virtualization Settings > VMware Settings**.
4. Click the VMware Credentials Library tab.
5. Select the credential you want to update, and then click **Edit Credential**.
6. Make the necessary updates, and then click **OK**.

WAN Optimization

This document provides step-by-step instructions for leveraging the SolarWinds Orion Network Performance Monitor to generate reports that track and validate wide area network (WAN) traffic optimization from WAN optimization appliances. For more information about configuring or managing your optimization appliance, see your appliance documentation.

SolarWinds Orion Network Performance Monitor provides several WAN Optimization reports that make it easy to view traffic usage by bytes, packets, and % optimized before and after WAN appliance optimization. By following the configuration steps described within this document, you can view these Orion reports in minutes on the Orion Web Console.

You can also use the Orion NetFlow Traffic Analyzer (Orion NTA) module to view traffic flows throughout the network, including optimized WAN links. Orion NTA allows you to view realtime and historical trending data by protocol, IP address, and application across different network links.

Using WAN Optimization Reports

The following sections walk you through obtaining, setting up, and populating the Orion WAN Optimization reports.

Downloading and Saving Your Reports

The SolarWinds WAN Optimization reports can be found within the SolarWinds Customer Portal in the Orion Additional Components section. You can also locate these reports in the SolarWinds Customer Forum at www.thwack.com (**Content Sharing Zone > Orion Custom Reports**).

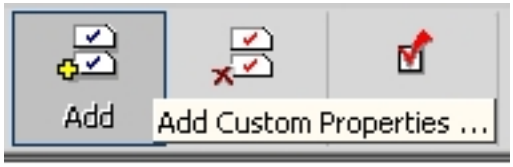
Extract the contents of the **SolarWinds WAN Optimization.zip** to the **..\Program Files\SolarWinds\Orion\Reports** folder or your custom reports folder.

Specifying Traffic Optimized Interfaces

You use the Orion Custom Property Editor to specify your optimized interfaces.

To label your interfaces with the Custom Property Editor:

1. Launch the **Custom Property Editor** by clicking **Start > All Programs > SolarWinds Orion > Advanced Features > Custom Property Editor**.
2. Click **Add** on the menu bar.

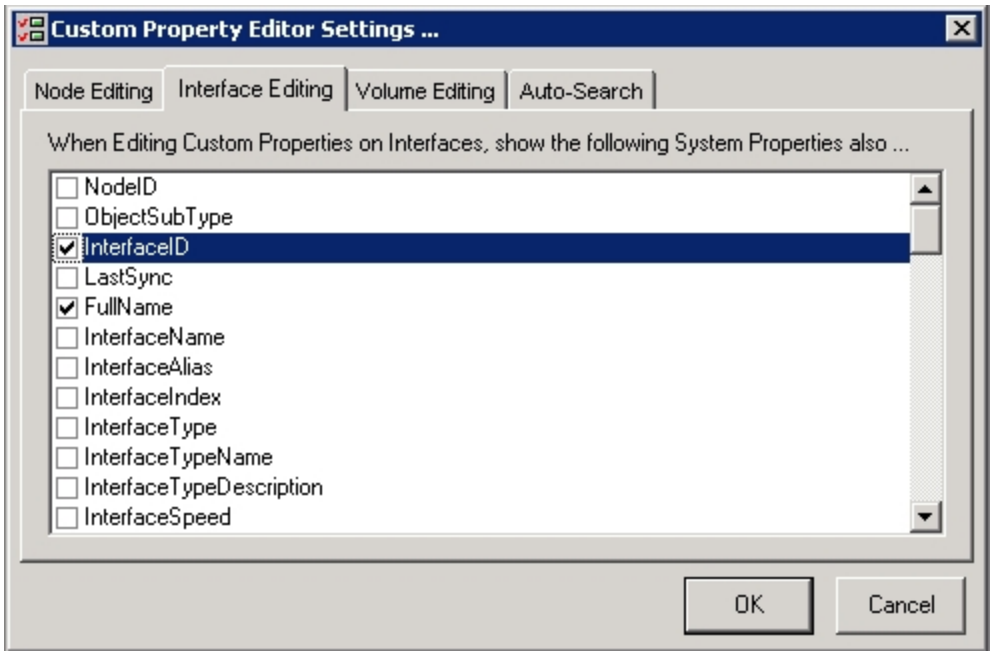


3. Click **Build a Custom Property from scratch,** and then specify the following entries in the appropriate fields:

Field	Selection
Add Property to	Interfaces
Property name	OptimizedInterfaceID
Property Type	Integer Number

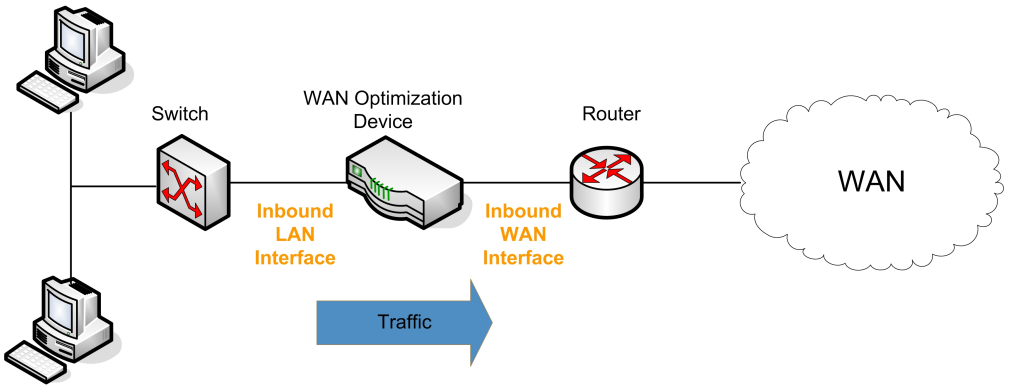
4. Click **OK** on the Add Custom Properties window.

5. Click **Settings** in the menu bar, and then check **Interface ID** on the Interface Editing tab.



6. Click **OK**.
7. Click **Interfaces** on the menu bar.

8. ***If your appliance is not behind a firewall***, complete the following procedure:

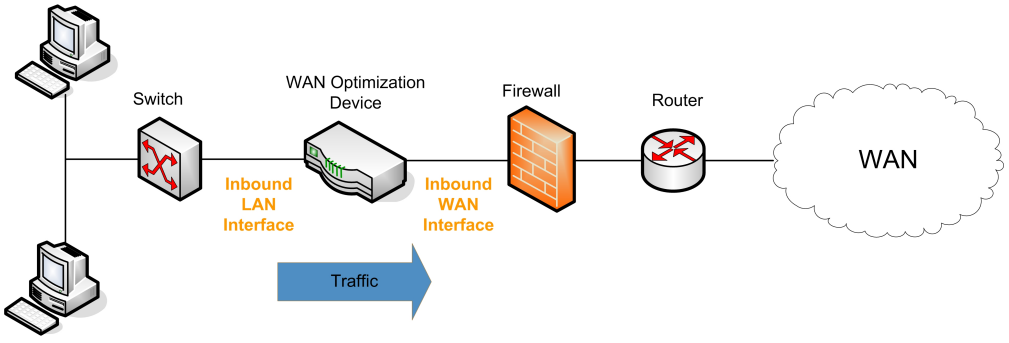


   a. Locate and copy the InterfaceID of the Inbound WAN Interface for the router. The inbound interface is connected on the WAN side of the appliance.

   b. Paste the InterfaceID into the OptimizedInterfaceID column of the Inbound LAN Interface of your appliance. The LAN interface receives all LAN traffic bound for a destination across the WAN.

   c. Repeat **Steps a through b** for each configuration matching this configuration.

9. ***If your appliance is behind a firewall***, complete the following procedure:



   a. Locate and copy the InterfaceID of the Inbound WAN Interface for the firewall. The inbound interface is connected on the WAN side of the appliance.

b. Paste the InterfaceID into the OptimizedInterfaceID column of the Inbound LAN Interface of your appliance. The LAN interface receives all LAN traffic bound for a destination across the WAN.

c. Repeat **Steps a through b** for each configuration matching this configuration.

10. Click **File > Exit**.

Viewing the WAN Optimization Report

You can view your report in either Orion Report Writer or in the Orion Web Console.

Viewing Your Report in Orion Report Writer

The following procedure walks you through viewing your WAN Optimization report in Orion Report Writer.

To view your report:

1. Launch the Orion Report Writer by clicking **Start > All Programs > SolarWinds Orion > Report Writer**.
2. Navigate to the WAN Optimization Traffic reports in the left pane. The following WAN Optimization Traffic reports are available: Last Hour, Last 2 Hours, Last 24 Hours, and Last 7 Days.
3. Click the report you want to view, and then click **Preview**.

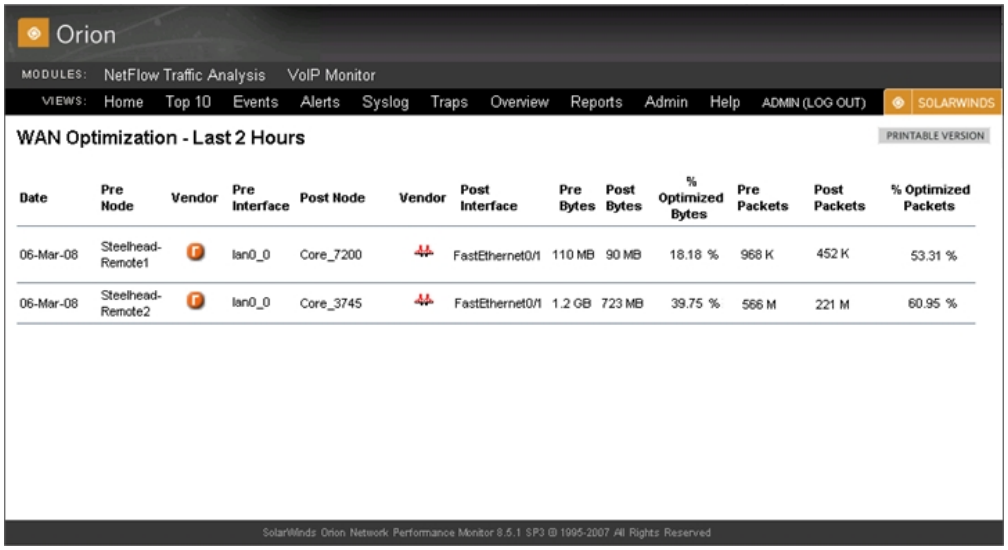
Viewing Your Report in the Orion Web Console

The following procedure walks you through viewing your WAN Optimization report in the Orion Web Console.

To view your report:

1. Launch the Orion Web Console by clicking **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Log on to the Web Console. This account must have access to the folder in which the WAN Optimization reports are located.
3. Click **Reports** on the menu bar. Locate the WAN Optimization Traffic reports: Last Hour, Last 2 Hours, Last 24 Hours, and Last 7 Days.
4. Click the report you want to view.

Note: Ensure you save WAN Traffic Optimization reports to the appropriate Reports directory. If you are having difficulty viewing your reports in the Orion Web Console, check that they have been saved to the appropriate location.



Understanding Your Reports

The following notes may help you further understand the information provided in your WAN Optimization reports:

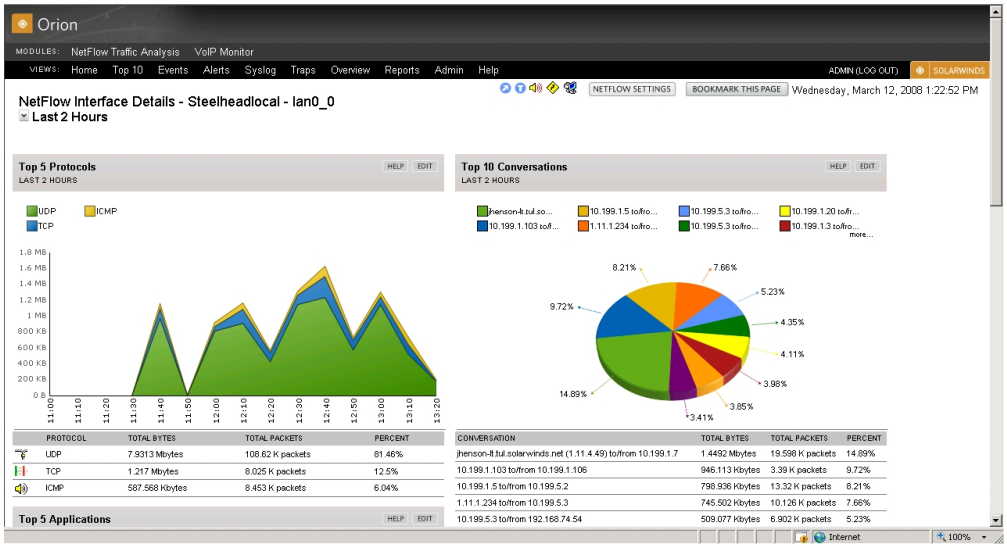
- Traffic originating from the LAN and terminating at the WAN optimization appliance is reflected in the Inbound LAN Interface statistics, not in the Inbound WAN Interface statistics. SNMP, ICMP, and Telnet traffic has minimal impact.
- WAN Traffic originating from the WAN optimization appliance is reflected in the Inbound WAN Interface statistics, not in the Inbound LAN Interface statistics. SNMP, ICMP, and Telnet traffic has minimal impact.

Using Orion NTA for Detailed Traffic Analysis

The Orion NetFlow Traffic Analyzer (Orion NTA) module can be used to view traffic flows throughout the network, including your optimized WAN links. Orion NTA allows you to view realtime and historical trending data by protocol, IP address, and application across different network links.

Orion NTA helps network administrators answer questions the following questions:

- Which applications are consuming network bandwidth?
- Which users are generating the most traffic?
- Which IP addresses are my top talkers?
- Should I install a WAN optimization device and why?
- What is the historical trend of bandwidth over the WAN and within my LAN?
- When my network is running hot, what is going on?



Conclusion

Orion WAN Optimization reports are freely available in the Orion Custom Reports section of the Community Sharing Zone on the SolarWinds community site, Thwack.com. The combination of Orion WAN Optimization reports and Orion NTA provides demonstrable value for anyone considering deploying, currently deploying, or has already deployed WAN optimization devices. Network administrators can easily monitor the bandwidth savings and response time benefits of their WAN optimization devices and ensure ongoing tracking and metrics are met using the full network performance management capabilities of Orion.

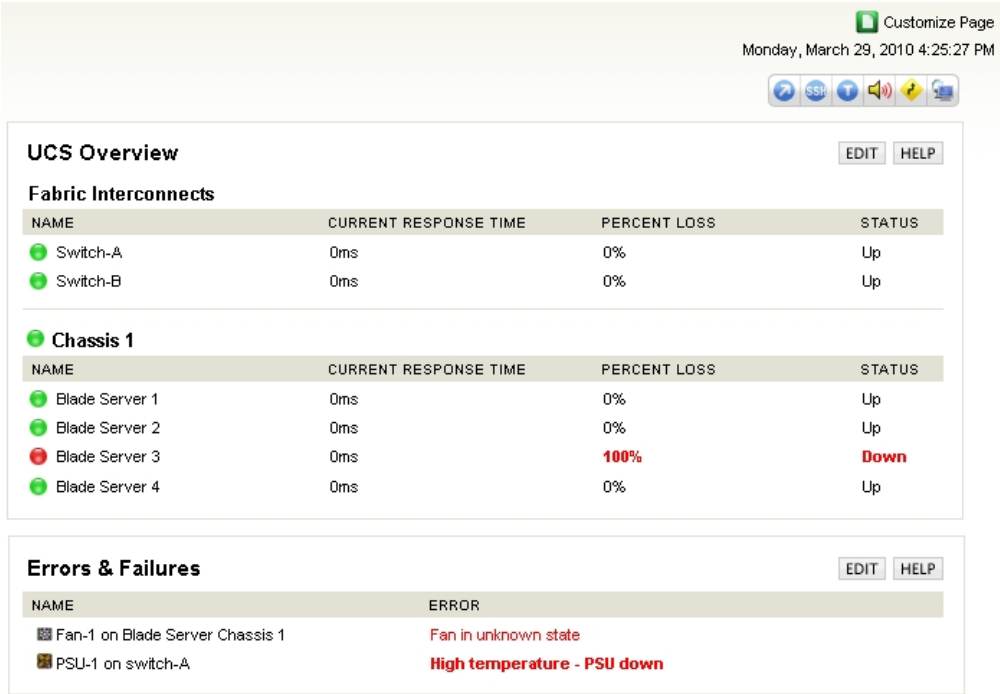
Setting Up a Cisco Unified Computing System as a Managed Node

This paper provides the procedures for setting up a Cisco Unified Computing System (Cisco UCS) for monitoring within Orion products.

Introduction

Cisco's Unified Computing System (UCS) is designed to provision, migrate, and manage Internet working systems in data centers. When you add the UCS master device, and the primary fiber interconnect devices, into the Orion All Nodes resource, you gain a view to all information that UCS provides.

Below is an example of what you see in the detailed view of the UCS master node. The procedures in the following section guide you through the process of setting-up a Cisco UCS with the components shown in the example.



Setting Up and Monitoring a Cisco UCS

Follow these steps to setup a Cisco UCS for monitoring in the Orion All Nodes resource.

To setup Cisco UCS for monitoring:

1. Confirm that LDAP authentication is not enabled on your UCS device:
    a. Open UCS Manager.
    b. On the Admin tab, expand **User Management > User Services**.
    c. Confirm that the full user name is provided for both **Locally** and **Remotely Authenticated Users**.
    d. ***If the default authentication realm is anything other than Local,*** you will need to use another realm for local authentication.
    Note: Authentication should use the full username form, as **in ucs-realm_name\username**, and **ucs-** should always be included.
2. Verify in the UCS console that the fiber connects (Switch A and Switch B in the example) have external IP addresses. For example, this is how to navigate to the values for Switch-A:

    Sys>Switch-A (or Switch-B)>Mgmt>if-1>

ExtGW	**Not 0.0.0.0**
ExtIP	**Not 0.0.0.0**
EXTMask	**Not 0.0.0.0**

    If the external gateway, external IP address, or external mask are set to 0.0.0.0, edit with values valid to external devices.
3. Add the UCS Master node into the Orion All Nodes resource.

Note: If the node already show up in the All Nodes list in italics or with ‘n/a’ as the state, click on it; and then click ‘Yes’ when Orion asks to manage the devices using Orion NPM.

a. Click **Edit** in the All Nodes resource if the node is not in the list.
b. Click **Add Node** and provide the information:
    - Hostname or IP Address
        - Dynamic IP Address
        - ICMP (for Ping only)
        - External
        - UCS Manager credentials
        - Poll for Vmware
    - Polling Engine
    - UCS Port
    - UCS User Name
    - UCS Password
c. Click **Test** under the UCS fields.
d. Click **Next** if the test succeeds. (The wizard disallows progress to the next screen when the test fails.)
e. Check the resources to monitor on the node.
f. Add relevant pollers.
g. Review your information and when you’re ready click **OK, ADD NODE**.

4. Add each UCS fabric interconnect switch and blade device into the Orion All Nodes resource.

Note: If the node already show up in the All Nodes list in italics or with **'n/a'** as the state, click on it; and then click **'Yes'** when Orion asks to manage the devices using Orion NPM.

a. Click **Edit** in the All Nodes resource if the node is not in the list.
b. Click **Add Node** and provide the information:
    - Hostname or IP Address
        - Dynamic IP Address o ICMP (for Ping only)
        - External
        - UCS Manager credentials
        - Poll for Vmware
    - Polling Engine
    - SNMP Version
    - SNMP Port
    - Community String
    - Read/Write Community String
c. Click **Test** under the **SNMP** fields.
d. Click **Next** if the test succeeds. (The wizard disallows progress to the next screen when the test fails.)
e. Check the resources to monitor on the node.
f. Add relevant pollers.
g. Review your information and when you're ready click **OK, ADD NODE**.
h. Perform **steps b-g** for each of the devices.

5. Double click on the UCS Master node in All Nodes and find the UCS Overview resource. Assuming each device status is still the same, you should see the UCS information as presented in the beginning of this document.

Note: To select the proper view we use the existing View By Device Type feature. To ensure that Standard Poller does not overwrite MachineType and other fields we use EntityType to identify UCS node in the Standard Poller (and so force Standard Poller not to overwrite our required fields). This same mechanism is also used for the ESX VMWare API.

6. If any UCS device shown in the UCS Overview is not currently managed in Orion All Nodes, double-click the device. The Orion node management software prompts you to add the node; when you click **OK** the software redirects to the Add Node Wizard.