ADMINISTRATION GUIDE

Server Configuration Monitor

Version 1.0

solarwinds

Last Updated: Monday, August 20, 2018

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

Table of Contents

Introduction

The Server Configuration Monitor (SCM) Administrator Guide provides an overview of product features and related technologies. In addition, it contains recommendations on best practices, instructions for getting started with advanced features, and troubleshooting information for common situations.

System requirements

The following are the system requirements for SolarWinds Server Configuration Monitor (SCM) 1.0.

In addition to the requirements listed below, most SCM monitoring requires the monitored servers to be polled by an Orion Agent for Windows.

> ⓘ For additional information on requirements and configurations, see the Multi-module system guidelines. You should also review your product administration guides and release notes for the exact product requirements beyond these minimums.

Server requirements

TYPE	REQUIREMENTS
Operating System	• Windows Server 2016 • Windows Server 2012 and Windows Server 2012 R2 ⚠ **Deprecation notice**: Although you can install Orion Platform 2018.2 products on Windows Server 2012 and 2012 R2, these versions are deprecated and will not be supported on future Orion Platform versions. **SolarWinds strongly recommends that you upgrade to Microsoft Windows Server 2016 or later at your earliest convenience.** For **evaluation** purposes **only**: • Windows 8.1 including Update 1, 64-bit only (except Standard edition) • Windows 10 ⓘ Installing SolarWinds Orion on Windows Server 2012 R2 Essentials or Windows Server Core is not supported.
Operating System Language	• English • German • Japanese • Simplified Chinese

Type	Requirements	
SolarWinds SCM Server Hardware	CPU Speed	Quad-core processor or better
	Memory	6 GB minimum 8 GB recommended The amount of memory needed by SCM depends on several variables in your environment. For best performance, SolarWinds recommends using at least 16GB of memory on the main Orion server and 32 GB per SQL Server if you plan to monitor over 1000 nodes.
	Hard Drive Space	10 GB minimum 20 GB recommended
Installing Windows Account	Requires administrator permission on the target server.	
File System Access Permissions	Ensure the Network Service account has modify access to the system temp directory: `%systemroot%\temp`.	
SolarWinds Orion Syslog Server	If you want real time change detection triggered through devices sending Syslog messages, the executable must have read and write access to the Orion Platform database.	
SolarWinds Orion Trap Service	If you want real time change detection triggered through devices sending SNMP traps, the executable must have read and write access to the Orion Platform database.	
Microsoft SNMP Trap Service	Must be installed if you want real time change detection triggered through devices sending SNMP traps.	
Microsoft IIS	Version 8.0 or later. DNS specifications require hostnames to be composed of alphanumeric characters (A-Z, 0-9), the minus sign (-), and periods (.). Underscore characters (_) are not allowed. SolarWinds does not support installing SolarWinds SCM on the same server or using the same database server as a Research in Motion (RIM) Blackberry server.	
Microsoft ASP .NET 2.0 Ajax Extension	Version 1 or later If this is not found on the target computer, the setup program downloads and installs the component.	

TYPE	REQUIREMENTS
Microsoft .NET Framework	Version 4.6.2 If the required version is not found on the target computer, the installer downloads and installs it. Ensure that .NET is turned on in Windows Features.

Database server requirements

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

TYPE	REQUIREMENTS
Language	SolarWinds supports using SCM with database servers set up in the following languages: • English • German • Japanese • Chinese
SQL Server versions	• SQL Server 2017 • SQL Server 2016 and SQL Server 2016 with SP1 • SQL Server 2014 and SQL Server 2014 with SP1-SP4 • SQL Server 2012, with or without SP1 and SP2, Standard or Enterprise ⚠ **Deprecation notice**: Although you can use SQL Server 2012 with Orion Platform 2018.2 products, this version is deprecated and will not be supported on future versions of the Orion Platform. **SolarWinds strongly recommends that you upgrade to Microsoft SQL Server 2016, 2017, or later at your earliest convenience.** ⓘ SCM local SQL database uses SQL 2017 EE Advanced by default. You can use the following database select statement to check your SQL Server version, service pack or release level, and edition: `select SERVERPROPERTY ('productversion'), SERVERPROPERTY ('productlevel'), SERVERPROPERTY ('edition')`

SQL server collations	The following SQL server collations are supported: • English with collation setting SQL_Latin1_General_CP1_CI_AS • English with collation setting SQL_Latin1_General_CP1_CS_AS • German with collation setting German_PhoneBook_CI_AS • Japanese with collation setting Japanese_CI_AS • Simplified Chinese with collation setting Chinese_PRC_CI_AS
Authentication and protocols	Your database server must support mixed-mode authentication or SQL authentication and have the following protocols enabled: • Shared memory • TCP/IP • Named Pipes
x86 components	The following x86 components must be installed: • SQL Server System Common Language Runtime (CLR) Types • Microsoft SQL Server Native Client • Microsoft SQL Server Management Objects If the components are not found on the target computer, the setup program downloads and installs the components.
CPU	Quad core processor or better
Memory	8 GB minimum 16 GB recommended ⓘ The amount of memory needed by SCM depends on several variables in your environment. For best performance, SolarWinds recommends using at least 16GB of memory on the main Orion server and 32 GB per SQL Server if you plan to monitor over 1000 nodes.
Hard drive space	20 GB minimum 50 GB recommended ⚠ The amount of space needed by SCM depends on several variables in your environment. See the table below for more details.

Additional database space requirements

The amount of space required by SCM depends on the number of nodes being monitored, the frequency of changes, the number of configuration items being monitored, and the average size of a configuration item. Use the following examples to help determine your needs.

Number of nodes monitored by SCM	Number of configuration items per node	Average size of configuration item	Frequency of changes	Additional database space recommendation
1000	100	10.00 kB	Once per **week**, every item changes	52 GB
			Once per **day**, every item changes	365 GB
	50	10.00 kB	Once per **week**, every item changes	26 GB
		5.00 kB		13 GB

Port requirements

Port	Protocol	Service/Process	Direction	Description
22	SSH	SolarWinds Job Engine v2 IIS	Bidirectional	Port for accessing ASA devices through CLI
25	TCP	SolarWinds Alerting Service V2	Outbound	SMTP email default that Orion Platform products use for notification (If SSL/TLS encryption is set up on SMTP server, default port is 465)
53	UDP	SolarWinds Job Engine v2	Bidirectional	Resolving DNS queries
80	TCP	IIS	Inbound	HTTP default for the Orion Web Console
161	UDP	SolarWinds Job Engine v2	Outbound	SNMP statistics collection, the default for polling
162	UDP	SolarWinds Trap Service	Inbound	Trap messages listened for and received by the Trap Server
443	TCP	IIS	Inbound	Default port for HTTPS binding
445	TCP	File and Printer Sharing (SMB-In)	Bidirectional	Used to store firmware updates and configuration files remotely
465	TCP	SolarWinds Alerting Service V2	Outbound	The port used for SSL-enabled email alert actions

PORT	PROTOCOL	SERVICE/PROCESS	DIRECTION	DESCRIPTION
514	UDP	SolarWinds Syslog Service	Inbound	Syslog Service listens for incoming messages
587	TCP	SolarWinds Alerting Service V2	Outbound	The port used for TLS-enabled email alert actions
1434	UDP	SolarWinds Alerting Service V2 SolarWinds Administration Service SolarWinds Information Service SolarWinds Information Service V3 SolarWinds Orion Module Engine SQL Server Browse Service	Outbound	Communication with the SQL Server Browser Service to determine how to communicate with certain non-standard SQL Server installations. Required only if your SQL Server is configured to use dynamic ports.
1801	TCP	MSMQ	Bidirectional	MSMQ WCF binding (For more information see this article from Microsoft)
5671	TCP	RabbitMQ	Bidirectional	For encrypted RabbitMQ messaging (AMQP/TLS) into the main polling engine from all Orion servers
17777	TCP	SolarWinds Orion Module Engine SolarWinds Information Service SolarWinds Information Service V3	Bidirectional	Orion module traffic. Open the port to enable communication from your poller to the Orion Web Console, and from the Orion Web Console to your poller. The port used for communication between the Orion Web Console and the poller.
17778	HTTPS	SolarWinds Agent	Inbound to the Orion server	Required for access to the SWIS API and agent communication

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

Supported Web Console browsers

- Microsoft Internet Explorer version 11 or later with Active scripting

Do not enable Enterprise Mode on Internet Explorer. This setting forces Internet Explorer to emulate version 7, which is not supported.

- Microsoft Edge

Orion Platform products support two most recent versions of the following web browsers available at the release date:

- Firefox
- Chrome

Additional information

- SCM 1.0 supports monitoring on nodes running Windows Server 2008 R2 and newer.
- SCM requires read permissions to the monitored path for all file, parsed file, and registry profile elements.

Scalability

- SolarWinds SCM supports 1000 agent nodes and 150 changes/second per poller. To monitor files or registry entries on more than 1000 nodes, or if you expect to have more than 150 changes/second, you will need an Additional Polling Engine.

Installation and licensing

Installing SCM

As an Orion Platform product, SCM uses the SolarWinds Orion Installer.

Licensing

License Tier
Server Configuration MonitorSCM10 Nodes
Server Configuration MonitorSCM25 Nodes
Server Configuration Monitor SCM50 Nodes
Server Configuration Monitor SCM100 Nodes
Server Configuration Monitor SCM250 Nodes
Server Configuration Monitor SCM500 Nodes
Server Configuration Monitor SCM1000 Nodes

Node management

Supported nodes

Server Configuration Monitor supports monitoring on Windows-based devices. Monitoring profiles that include file or registry elements require the device be polled by the Orion Agent for Windows on Windows 2008 R2 or later. The out-of-the-box HW and SW inventory profiles require Asset Inventory, which can be enabled through List Resources on the Node Details page.

Add a node to SCM

To add servers already monitored by the Orion Platform to SCM, start configuration monitoring on the device.

To monitor servers using Server Configuration Monitor, you must first add them to the Orion Platform. There are several ways to add devices to the Orion Platform, but the following ways allow you to start SCM monitoring at the same time:

- Add a node through Network Discovery
- Add a node through the Add Node wizard

To learn more about adding nodes to the Orion Platform, see the Orion Platform Administrator Guide.

Add a node through Network Discovery

1. In the Orion Web Console menu, navigate to Settings > Network Discovery.
2. Follow the steps in the Network Discovery wizard.
3. After discovery has completed, select the devices to import and click Next.
4. Select the volume types to monitor. Click Next.
5. Select the server configuration profiles to monitor. Only out-of-the-box profiles can be added this way. Click Next.

   Selected profiles will be applied to all discovered nodes that are eligible for that type of monitoring. This eligibility is determined by the presence of specific files or registries on the node. For example, IIS configuration files must be present for the IIS profile to be applied. Note that the profiles other than the HW and SW inventories require polling via an Orion Agent for Windows.

6. Confirm all import information. Click Import.
7. Wait for the import to complete. Click Finish.

Add a node through the Add Node wizard

1. In the Orion Web Console menu, navigate to Settings > Manage Nodes.
2. Click Add Node.
3. Specify the node, and click Next.
   a. Provide the host name or IP address.
   b. Select the polling method, and provide credentials.

      > ⓘ Most SCM monitoring requires polling via an Orion Agent for Windows.

4. In the Choose Resources step, select the profiles you would like to monitor under Server Configuration. Click Next.

   > ⓘ Only out-of-the-box profiles can be assigned this way. To assign custom profiles, see Assign configuration profiles to a node.

5. Review and adjust the device properties. Click Ok, Add Node.

See monitored nodes

All users can see the nodes currently being monitored by SCM in the Server Configuration Nodes widget on the Server Configuration Summary page. The Server Configuration Summary page can be found under My Dashboards.

Users with the SCM Admin role can also see the Monitored Nodes section of Server Configuration Monitor Settings:

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings and selecting Server Configuration Monitor Settings under Product Specific Settings.
2. Click the Monitored Nodes tab in the upper left.

From here, you can assign and unassign profiles from the nodes that are already being monitored.

Monitor a node

ⓘ This assumes you have already added the node to the Orion Platform. See Add a node to SCM for details.

To begin monitoring server configurations, you must assign one or more configuration profiles to the server.

- Assign configuration profiles to a node
- Assign profiles based on suggestions

Assign configuration profiles

ⓘ This task is not available to all users. See User Roles for details.

To begin monitoring server configurations, you must assign one or more configuration profiles to the server. There are multiple ways to assign configuration profiles:

Through Server Configuration Monitor Settings

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor settings under the Product Specific Settings heading.
2. Pick either the Manage Profiles tab or the Monitored Nodes tab. If you need to assign profiles to a node that is not already in SCM, choose Monitored Nodes.
   a. From Manage Profiles:
      i. Select the profiles to assign.
      ii. Click Assign To in the ribbon.
      iii. Choose the nodes to assign the profiles to, then click Next.
   b. From Monitored Nodes:
      i. Select the node(s) to assign profiles to from the list of nodes already in SCM, then choose Assign Profiles.
      If you do not see the node you want to assign profiles to, click Set Up Configuration Monitoring to add a new node to SCM.
      ii. Select the profiles to assign, then click Next.
      iii. If monitoring a new node, select the node(s) to apply the profiles to.
3. Review the assignments on the summary page. Here you will see warnings if there are any potential polling issues detected, such as Asset Inventory being disabled on a node when assigning a profile that requires it. You can still assign profiles if a warning occurs, but SCM will

not start collecting that data until the conflict is resolved.

4. Click Confirm to finish the assignment.

Through List Resources

Out-of-the-box profiles can be assigned through a node's List Resources.

1. Navigate to List Resources for the server you would like to monitor. There are multiple ways to get to List Resources:
   - From the Node Details Summary page, click List Resources in the Management widget.
   - Click Settings > Manage Nodes. Select the node, then click List Resources in the Node Management toolbar.
2. Under Server Configuration, select the profiles you want to assign or unassign.

   > ⓘ Note that custom profiles are not included in List Resources.

3. Click Submit to save your changes.

From the Server Configuration Summary page

Custom and out-of-the-box profiles can be assigned from the Server Configuration Summary page.

1. Navigate to My Dashboards > Server Configuration Summary.
2. In the Server Configuration Nodes widget, click Assign Configuration Profiles.
3. Select the profiles you wish to assign, then click Next.
4. Select the nodes to which those profiles should be assigned, then click Next. The list of nodes can be filtered by node properties, including custom properties.
5. Review the profile assignments, then click Confirm to finish the profile assignment.

Unassign configuration profiles

> ⓘ This task is not available to all users. See User Roles for details.

There are two ways to unassign configuration profiles:

Through Server Configuration Monitor Settings

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. Switch to the Monitored Nodes tab.
3. Select the node(s) you want to unassign profiles from.

4. Click Unassign Profiles on the ribbon.
5. Select the profiles you want to unassign, then click Unassign.
6. You will be prompted with a question about keeping historical data. You can choose to keep the data SCM has collected from the unassigned profiles if you would like to see that information when looking at the configuration history. If you choose to delete the data, that history will be gone. Click either Keep Data or Delete Data to finish the unassignment.

Through List Resources

Out-of-the-box profiles can be unassigned through a node's List Resources. There is no option to keep the historical data if unassigning profiles this way.

1. Navigate to List Resources for the server you would like to monitor. There are multiple ways to get to List Resources:
   - From the Node Details Summary page, click List Resources in the Management widget.
   - Click Settings > Manage Nodes. Select the node, then click List Resources in the Node Management toolbar.
2. Under Server Configuration select the profiles you want to assign or unassign. Note that custom profiles are not included in List Resources.
3. Click Submit to save your changes.

You might want to assign the same profile(s) to multiple servers. Instead of doing each individually, you can assign and unassign profiles in bulk. There are two ways to do assignment, and one way to do unassignment:

See detected candidates for configuration monitoring

SCM will automatically detect servers that have been added to the Orion Platform that might be eligible for monitoring one or more of the out-of-the-box profiles. You can view a list of candidate servers on the SCM Summary page, which can be found under My Dashboards.

The Candidates for Server Configuration Monitoring widget lists servers that might be eligible for configuration monitoring but do not have an agent, and servers that are eligible for monitoring each out-of-the-box profile. From there, you can push agents or assign the suggested profiles using the links provided. The "Dismiss all" link will stop those nodes from being suggested again.

Whether a node is eligible for configuration monitoring is determined in the following ways:

SUGGESTED ACTION	ELIGIBILITY REQUIREMENTS
Push an agent	Any node running Windows Server 2008 R2 or later.

Assign HW/SW inventory profiles	Any node with AssetInventory enabled
Assign IIS profile	Any node monitored by AppInsight for IIS, or another SAM app templated tagged as 'IIS'

See recent configuration changes

To see the most recent configurations from all monitored nodes, find the Recent Configuration Changes widget on the Server Configuration Summary dashboard.

This widget shows all configuration changes in the selected time interval. Each row shows the name of the profile in bold, the node the change was made on, and the element name/path. The color to the left of each entry indicates the type of change: yellow for addition, blue for an update, and red for removal. Clicking a row will take you to a comparison between the two most recent versions (see Compare configurations over time).

> ⓘ The initial poll is not included in the list of all configuration changes. The initial data is not considered a change, since there was no previous data to compare to.

To see the most recent configuration changes on a particular node, see the Recent Configuration Changes widget on the Server Configuration page of Node Details.

Configuration profiles

SCM configuration profiles are collections of elements you want to monitor. Each profile element results in one or more configuration items (e.g. individual files or registry entries) being monitored. There are several out-of-the-box profiles for commonly monitored elements, or you can create custom profiles with exactly the elements you want to monitor.

Out-of-the-box profiles

SCM comes with several predefined configuration profiles for server inventory and commonly monitored applications. These out-of-the-box configurations are:

- HW Inventory
- SW Inventory
- IIS

Customizing

Out-of-the-box profiles cannot be edited directly. However, you can create a custom profile based on one of the out-of-the-box profiles, which can be edited.

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. Click the Manage Profiles tab, if it is not selected by default.
3. Select the profile you wish to copy, then click Copy. An "Add configuration profile" window will open.
4. Make the desired changes to the list of configuration elements, description, and profile name.
5. Click the Add button to save the new profile.

HW inventory

The HW inventory profile monitors changes to the server's hardware, including:

- Drivers
- Hard Drives
- Logical Drives
- Memory modules
- Network Interfaces
- OutOfBand Management
- Peripherals
- Processors

- Removable Media
- Storage Controllers
- Video Card

Monitoring this profile requires Asset Inventory be enabled on the server. To enable Asset Inventory:

1. Navigate to List Resources for the server you would like to monitor. There are multiple ways to get to List Resources:
   - From the Node Details Summary page, click List Resources in the Management widget.
   - Click Settings > Manage Nodes. Select the node, then click List Resources in the Node Management toolbar.
2. In the list that appears, check the box next to Asset Inventory.
3. Click Submit to save your changes.

SW inventory

The SW inventory profile monitors changes to:

- Firmware
- OS Updates
- Server Information
- Software Installed

Monitoring this profile requires Asset Inventory be enabled on the server. To enable Asset Inventory:

1. Navigate to List Resources for the server you would like to monitor. There are multiple ways to get to List Resources:
   - From the Node Details Summary page, click List Resources in the Management widget.
   - Click Settings > Manage Nodes. Select the node, then click List Resources in the Node Management toolbar.
2. In the list that appears, check the box next to Asset Inventory.
3. Click Submit to save your changes.

IIS

The predefined profile for IIS servers monitors the following configuration files. Descriptions of these elements are available:

PATH	DESCRIPTION
%WINDIR%\Microsoft.NET\**\machine.config	The machine.config for .NET Framework settings.

%WINDIR%\Microsoft.NET\**\web.config	The root web.config for .NET Framework settings.
%WINDIR%\System32\inetsrv\MBSchema.xml	The MetaBase schema definition used in IIS 6.0 instead of applicationHost.config.
%WINDIR%\System32\inetsrv\MetaBase.xml	This configuration file is used in IIS 6.0 instead of applicationHost.config.
%WINDIR%\System32\inetsrv\config\administration.config	This configuration file stores the settings for IIS management. These settings include the list of management modules that are installed for the IIS Manager tool, as well as configuration settings for management modules.
%WINDIR%\System32\inetsrv\config\redirection.config	IIS 7 and later support the management of several IIS servers from a single, centralized configuration file. This configuration file contains the settings that indicate the location where the centralized configuration files are stored.
%WINDIR%\System32\inetsrv\config\schema\*.xml	The full schema reference for config files, including default values for all properties in every section, their valid ranges, etc.
%WINDIR%\System32\inetsrv\config\applicationHost.config	Parsing applicationHost.config file to search for distributed configuration via web.config files specific for a particular IIS site, application or virtual directory and located within its directory.
All web.config files found from parsing applicationHost.config.	

Profile element types

File

The File element type is defined by a full path to a file. This path can use the wild character `*` for any part of the filename, the wild character `**` for any subdirectory, and system variables such as `%WINDIR%`.

For example:

- `%WINDIR%\Microsoft.NET\**\web.config`
- `%WINDIR%\System32\inetsrv\config\schema\*.xml`

Note: The use of wild characters can have a negative impact on performance if used to monitor too many files, or very large files.

File elements are polled every minute.

Registry

Registry elements are defined by a registry key path. No wild characters are allowed. All subtrees are monitored, which might affect performance if monitoring a large registry tree.

For example:

- `HKEY_CLASSES_ROOT\Installer\Features`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\Packages`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate`

Registry elements are polled in real-time.

Parsed File

ⓘ This element type is only available as part of out-of-the-box profiles.

A file parser reads a particular type of file and finds more configuration elements to monitored based on that file's contents.

PARSER	FILE PARSED	ELEMENTS PARSED OUT
IIS Web Config Parser	applicationHost.config	This parser reads an applicationHost.config file to find web.config files to monitor for all IIS sites, applications, and virtual directories within that applicationHost.config.

Internal Query

ⓘ This element type is only available as part of out-of-the-box profiles.

Internal Query elements are queries to the Orion database.

Custom profiles

ⓘ These tasks are not available to all users. See User Roles for details.

You can use custom profiles to create sets of files and directories you want to monitor that aren't covered by the out-of-the-box profiles.

If a custom profile contains an element that targets the same file or registry as another profile, that file or registry will be reported twice. For example, if one profile is monitoring C:\foo\*.config and another is monitoring the more specific path C:\foo\bar.config, then the file C:\foo\bar.config will be doubled in SCM.

Add a new custom profile

To add a new custom profile to SCM:

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. Click Add at the top of the list of profiles.
3. Enter a name for the profile and (optionally) a description.
4. Add configuration elements to the profile with the Add button in the configuration elements pane.
   a. Select an element type from the drop-down menu.
   b. Enter a path or registry key for the element. See Element types for more information on permitted characters.
   c. Optional: Define a display alias for this element. If an alias is given, the element will be referred to by the alias instead of the filename or registry key.
   d. Optional: Enter a description of the element.
5. Click Add at the bottom of the dialog to save the profile.

Copy an existing profile

To copy an existing configuration profile:

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. Click the Manage Profiles tab, if it is not selected by default.
3. Select the profile you wish to copy, then click Copy. An "Add configuration profile" window will open.
4. Click Add to save the new profile.

Edit a custom profile

To edit a custom configuration profile:

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. Click the Manage Profiles tab, if it is not selected by default.
3. Select the profile you wish to copy, then click Edit.
4. In the "Edit configuration profile" window that opens, make your desired changes. Note that the type and path of an element can't be edited in profiles that are already assigned to a node. If you need to change the type or path, add a new element with the desired properties and remove the old one.
5. Click Save to save your changes.

Delete a custom profile

Deleting a custom profile removes all polled data gathered by that profile, for all nodes. To delete a custom configuration profile:

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. Click the Manage Profiles tab, if it is not selected by default.
3. Select the profile(s) you want to delete, then click Delete on the menu bar.
4. A window will open informing you of any nodes the selected profile(s) are currently assigned to. Even with SCM Admin rights, it is possible you cannot see all the nodes a profile is assigned to due to user limitations. Check that the number of nodes the confirmation dialog shows is equal to the number of nodes you believe to be assigned to the profile. If you are sure you want to delete the profile(s), click Delete to confirm.

Enable or disable content downloading for an element

SCM downloads the contents of configuration elements for content comparison. For very large files or very large registry keys, you may want to disable downloading to save database space and prevent performance or network traffic issues. When content downloading is disabled, changes will still be detected and reported as usual, but line-by-line content comparison will be disabled for the element.

To toggle content downloading:

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. Click the Manage Profiles tab, if it is not selected by default.
3. Select the profile containing the element, then click Edit.

4. Select the element to change the content downloading setting on, then click Edit.
5. Change the Download Content switch to the desired state, then click Save.

If content downloading was enabled for an element but is later disabled, the previously downloaded content will still be kept according to the data retention settings.

Import and export profiles

Profiles can be imported and exported to facilitate collaboration with other SCM users. SCM profile files have the extension ".scm-profile". The direct editing of .scm-profile files is not recommended.

Import

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. In the Manage Profiles tab, click Import.
3. Find the .scm-profile file you want to import, then click Open.

If a profile with the same name already exists, you will be asked if you would like to import the profile as a copy.

Export

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. In the Manage Profiles tab, select the profile you want to export.
3. Click Export.

Compare configurations over time

You can use SCM to see which configuration items changed between any two points in time, and drill down even further to see line-by-line what changes were made.

See configuration changes between two points in time

SCM lets you see the difference between versions of a server's configuration. You can see which configuration elements were added, deleted, or modified. If content downloading is enabled for a particular element, you can also see which lines of that element were added, deleted, or modified.

See which configuration elements changed

To see which configuration elements were changed between two points in time:

1. From the Node Details page of the server you would like to monitor, navigate to the Server Configuration view in the left sidebar.
2. In the Configuration Management widget, click Compare Configuration.
3. In Configuration Comparison, you will be presented with two side-by-side panels showing the monitored configuration items for that node, organized by profile and element type.
   By default, this comparison is between the current configuration and the baseline. If no baseline is set, it is instead between the current configuration and 24 hours prior.
   a. To change the date and time displayed, click the datetime on either side and select a new date and time. If a baseline is set, you can select it quickly from the datetime selection pop-up.

See line-by-line changes

1. Follow the above steps, or find the Configuration Details widget on the Server Configuration view of the Node Details page.
2. Click the item you want to examine the contents of.

The Content Comparison page that opens shows a line comparison of the element's contents at the times specified on the previous page. Unchanged lines will be collapsed by default, but can be expanded by clicking on the number of unchanged lines.

Color-coding

There are two color-coding modes for the change comparison pages: simplified, and change-type-based. With simplified color-coding, all changes are highlighted in yellow. With change-type-based color-coding, additions are shown in green, deletions in red, and modifications in blue.

To switch color-coding modes, click the three dots in the upper right of either comparison page.

Character Encoding

By default, all items in the line-by-line comparison are displayed using UTF-8 encoding. You can change the encoding by clicking the three dots in the upper right of the Content Comparison page. Changing the encoding will only change the way the item is displayed, and will not alter the underlying data.

Changing the encoding for one item will change the encoding for all other configuration items created by the same profile element. For example, if you have a File element in a profile that uses a wildcard character to match all the files in a certain directory, changing the encoding for one of those files will change the encoding for all the files in the directory.

Define a baseline

Baselines can be set from the Compare Configurations page, or from the Configuration Details widget on the SCM subview of a Node Details page.

- When comparing two configurations, if you would like to set one of them as the baseline, click the three dots to the right of the datetime and choose "Set as baseline".
- From Node Details, if you would like to set the current configuration as the baseline, click "Set as baseline" in the upper right of the Configuration Details widget.

Once a baseline is set on a node, it cannot be removed, but it can be set to a different time using the same methods.

If a profile is assigned to a node after the baseline is defined, those configuration items are not included in the baseline.

What is a baseline?

Each node can have a snapshot of all configuration items from all profiles at a particular date set as its baseline configuration. A baseline is the ideal or standard configuration for that node. It is the configuration against which you want to judge that node going forward.

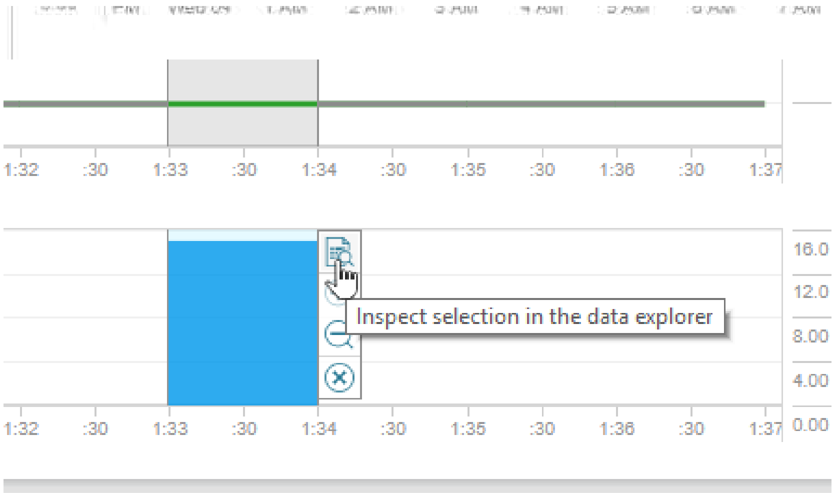
After you've set a baseline, you can be alerted when a node's configuration deviates from the baseline. For example, if a node is supposed to have only a particular set of software installed, you might assign the SW Inventory profile and set the baseline to a time immediately after all the software has been installed, then turn on "Server configuration differs from baseline" alert. If software is removed or additional software is installed, the alert will trigger and notify you something has changed.

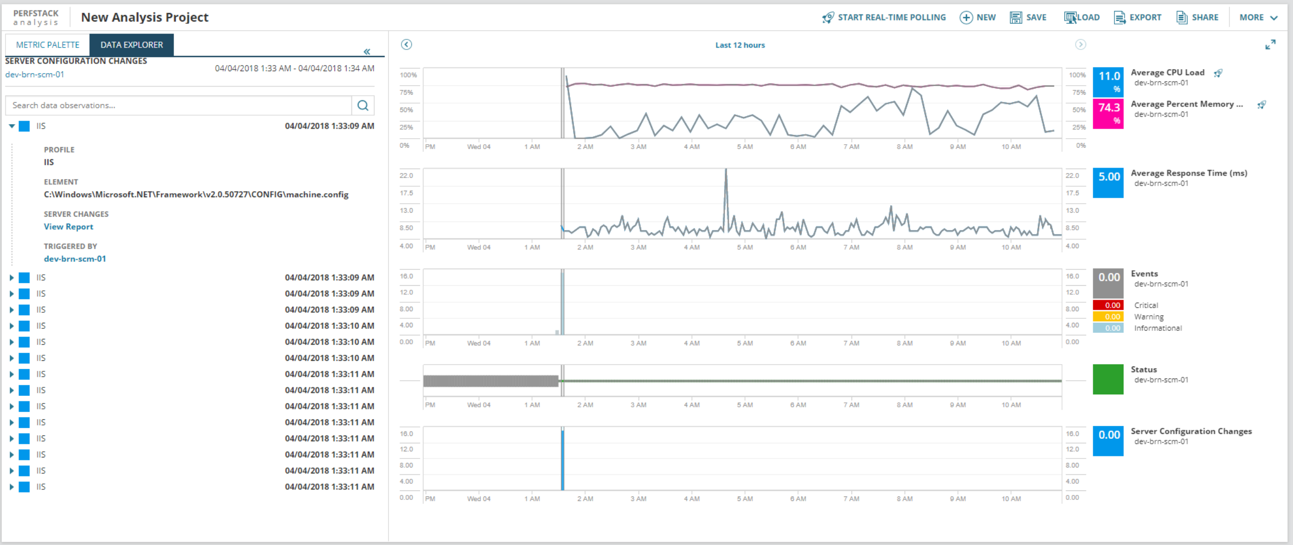
Correlate configuration changes to performance metrics

To see how a change in server configurations might have affected the server's performance, you can view changes on a timeline with performance metrics using the Performance Analysis Dashboard (PerfStack™).

1. Navigate to the Node Details Summary page for the node you want to examine.
2. In the Management widget, click Performance Analyzer.

Configuration changes will be shown at the bottom in blue. The X-axis shows time, and Y-axis of the SCM portion shows how many changes were made. To view configuration change details, hover over a column of changes and click the "Inspect selection in the data explorer" icon. Change details will be displayed in the Data Explorer to the left.





New Analysis Project

SERVER CONFIGURATION CHANGES
dev-brn-scm-01
04/04/2018 1:33 AM - 04/04/2018 1:34 AM

Search data observations...

IIS 04/04/2018 1:33:09 AM

PROFILE
IIS

ELEMENT
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config

SERVER CHANGES
View Report

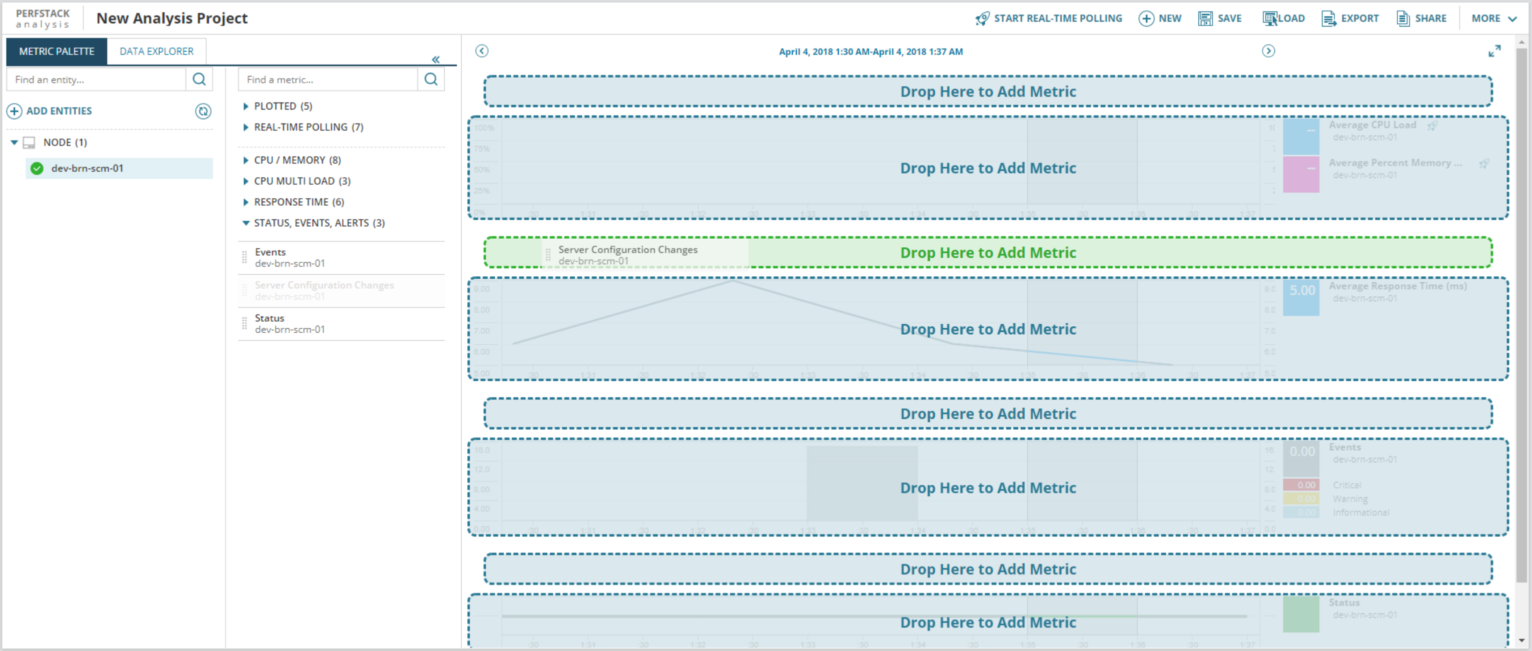
TRIGGERED BY
dev-brn-scm-01

IIS	04/04/2018 1:33:09 AM
IIS	04/04/2018 1:33:09 AM
IIS	04/04/2018 1:33:09 AM
IIS	04/04/2018 1:33:10 AM
IIS	04/04/2018 1:33:10 AM
IIS	04/04/2018 1:33:10 AM
IIS	04/04/2018 1:33:11 AM
IIS	04/04/2018 1:33:11 AM
IIS	04/04/2018 1:33:11 AM
IIS	04/04/2018 1:33:11 AM
IIS	04/04/2018 1:33:11 AM
IIS	04/04/2018 1:33:11 AM
IIS	04/04/2018 1:33:11 AM
IIS	04/04/2018 1:33:11 AM

11.0 %	Average CPU Load	dev-brn-scm-01
74.3 %	Average Percent Memory ...	dev-brn-scm-01
5.00	Average Response Time (ms)	dev-brn-scm-01
0.00	Events	dev-brn-scm-01
0.00	Critical	
0.00	Warning	
0.00	Informational	
🟩	Status	dev-brn-scm-01
0.00	Server Configuration Changes	dev-brn-scm-01

You can also manually add Server Configuration Changes to any custom PerfStack view.

1. Select a node in the Metrics Palette.
2. Find Server Configuration Changes under Status, Events, Alerts.
3. Drag and drop Server Configuration Changes into the PerfStack view.



Change how long configuration data is kept

This task is not available to all users. See User Roles for details.

SCM retains configuration data at three levels of granularity: detailed, hourly, and daily. Detailed data is every change detected for every configuration item. Hourly data is the most recent change detected within the hour for each configuration item. Daily data is the most recent change detected within a calendar day for each configuration item.

Data retention settings do not affect the data for a node's baseline configuration. Baseline information is kept forever.

By default, detailed data is kept for 7 days, hourly data is kept for 30 days, and daily data is kept for 365 days.

The default values for each level of granularity can be changed in SCM Settings:

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. Click the Data Retention tab.
3. Change the settings for each level of data as desired, then click Save Changes.

User restrictions

In order to make changes to profiles, profile assignments, and data retention settings in Server Configuration Settings, a user must have the SCM role "Admin" and node management rights. These permissions can be granted or revoked through Manage Accounts.

Events

You can view events in the Orion Web Console Message Center, found under Alerts & Activity, and in several widgets throughout the Orion Web Console. SCM fires the following events:

EVENT TEXT	DESCRIPTION
Server configuration baseline set to <datetime> on node '<node>'	The baseline has been set for the first time on a node.
Server configuration baseline reset to <datetime> on node '<node>'	The baseline has been set to a different datetime.
Server configuration differs from baseline on node '<node>'	Server's configuration has changed and no longer matches the baseline.
Server configuration matches the baseline on node '<node>'	Server's configuration that didn't match the baseline before has changed to match.

Alert on SCM data

Alerts can be enabled or disabled and configured through the Alert Manager , found under Alerts & Activity > Alerts > Manage Alerts.

SCM comes with the following out-of-the-box alerts:

ALERT NAME	DESCRIPTION
Server configuration has changed	Triggers the first time any of the server configuration items being watched are changed. To reduce noise if many changes happen at once, subsequent alerts are suppressed until the alert is cleared.
Server configuration differs from baseline	Triggers the first time a configuration item changes in a way that does not match that server's baseline configuration, where previously the configuration did match the baseline.

You can also create custom alerts using Server Configuration object fields and events, including the baseline status and when the last change was detected, as trigger conditions.

Report on SCM data

SolarWinds provides predefined reports for each Server Configuration Monitor product. You can use the reports as soon as there is data to be reported on.

View a list of predefined reports by clicking Reports > All Reports in the menu bar. Use the web-based interface to customize the predefined reports or create your own reports.

SCM comes with the following out-of-the-box reports:

NAME	DESCRIPTION	FIELDS
List of all configuration changes detected	All configuration changes that were detected in the last 24 hours.	• Node name • Node IP address • Profile name • Element type • Configuration item name • Change type • Change timestamp
List baseline mismatches	All configuration items that do not match the baseline configuration for the server, the last time a change was detected for that item, what kind of change was made, and a link to compare the item to the baseline.	• Node • Profile • Configuration item • Most recent change detected • Change type • Link to the change comparison page
Nodes with SCM profiles currently assigned	All nodes that have at least one SCM profile assigned, and which profiles are assigned.	• Node • Assigned profile

Troubleshooting SCM

The following are steps you can take to troubleshoot issues with your SCM deployment.

- If you aren't seeing any configuration data for a node, click Poll Now on the Node Details page. SCM may take up to an hour to poll data initially, but Poll Now should result in data appearing within a few minutes.
- If you're experiencing polling issues, try troubleshooting the Orion Agent
- If you're experiencing polling issues with only certain configuration items, make sure the system account on the node has permissions to the monitored file/registry path.
- Check that the Module Engine, SWIS, Job Engine, Collector Service, Agent and Website Orion services are running on your Orion server.

If the above steps don't resolve your issue, check the SCM logs for more information. By default, the relevant log files are located at:

- C:\ProgramData\SolarWinds\Logs\Agent\SolarWinds.Orion.SCM.AgentPlugin.log
- C:\ProgramData\Solarwinds\Collector\Logs\Collector.Service.log
- C:\ProgramData\Solarwinds\Logs\SCM\BL\BusinessLayer.log

Orion Platform Documentation

The following is information on the Orion Platform and Orion Web Console that is not specific to SCM, but is referenced throughout the SCM guide. For a comprehensive look at the platform, please see the online Orion Platform Administrator Guide.

Discover your network with the Discovery Wizard

Before you begin:

- Enable the networking devices you want to monitor for SNMP.
- Enable Windows devices for WMI.

The first time you discover your network, SolarWinds recommends adding a limited number of edge routers or switches, firewalls and load balancers (if you have them), and critical physical or virtual servers and hosts.

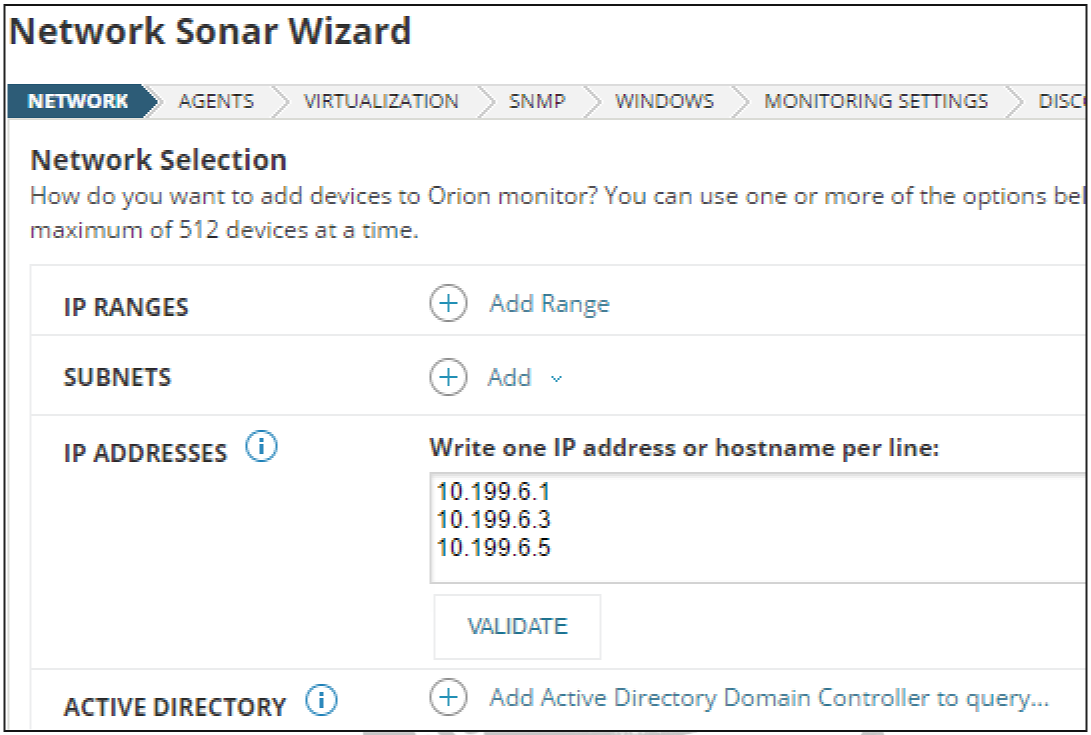
ⓘ Add nodes with high latency one at a time.

1. If the Discovery Wizard does not start automatically after configuration, click Settings > Network Discovery.
2. Click Add New Discovery, and then click Start.
3. On the Network panel, if this is your first discovery, add a limited number of IP addresses.

   As you scale your implementation, you can use the following scanning options.

OPTION	DESCRIPTION
IP Ranges	Use this option when you want Orion to scan one or more IP ranges. If you have many IP ranges to scan, consider adding multiple discovery jobs rather than including all ranges in a single job.
Subnets	Use this option to scan every IP address in a subnet. SolarWinds recommends scanning at most a /23 subnet (512 addresses max). Scanning a subnet returns everything that responds to ping, so we recommend only scanning subnets where the majority of devices are objects you want to monitor.
IP Addresses	Use this option for a limited number of IP addresses that do not fall in a range. Since a network discovery job can take a long time to complete, SolarWinds recommends using this option when you are first starting out.

Active Directory	Use this option to scan an Active Directory Domain Controller. Using Active Directory for discovery is particularly useful for adding large subnets because Orion can use the devices specified in Active Directory instead of scanning every IP address.


Network Sonar Wizard

Network Selection

How do you want to add devices to Orion monitor? You can use one or more of the options bel maximum of 512 devices at a time.

IP RANGES ⊕ Add Range

SUBNETS ⊕ Add ⌄

IP ADDRESSES ⓘ Write one IP address or hostname per line:

```
10.199.6.1
10.199.6.3
10.199.6.5
```

VALIDATE

ACTIVE DIRECTORY ⓘ ⊕ Add Active Directory Domain Controller to query...

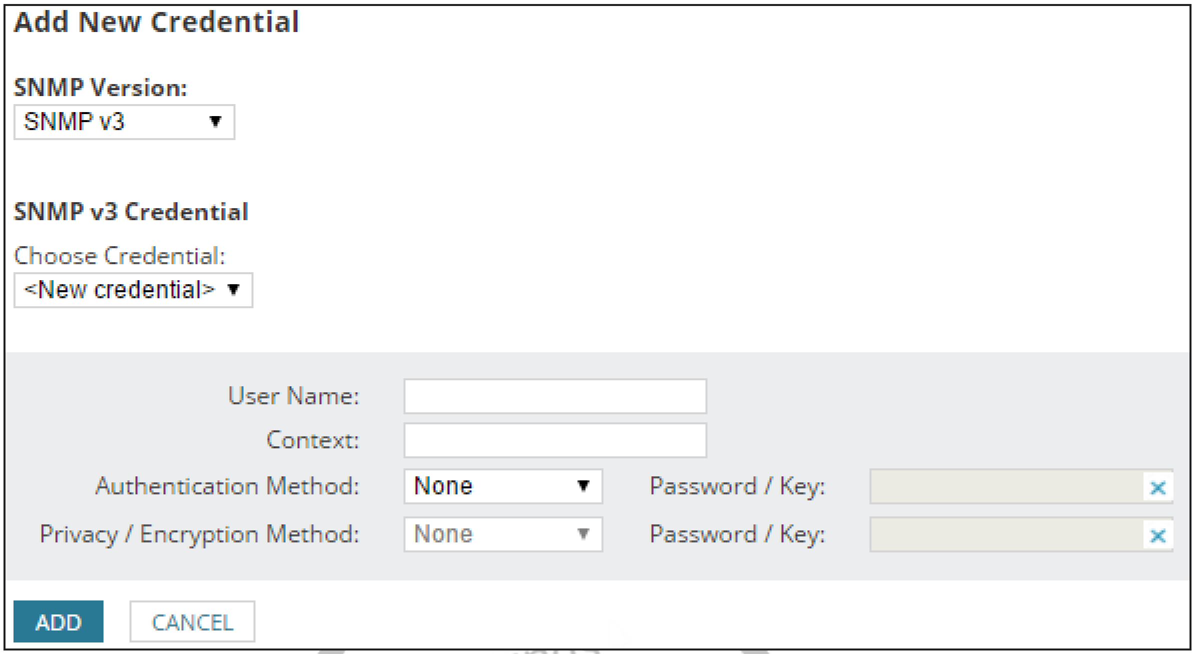
4. If the Agents panel appears, you enabled the Quality of Experience (QoE) agent during installation. The QoE agent monitors packet-level traffic. If there are any nodes using agents, select the Check all existing nodes check box.

   This setting ensures that any agents you deploy, including the one on your Orion server, are up-to-date. If there are no nodes using agents, you can leave this option unchecked.

5. On the SNMP panel:

   a. If all devices on your network require only the default SNMPv1 and SNMPv2 public and private community stings, click Next.

b. If any device on your network uses a community string other than public or private, or if you want to use an SNMPv3 credential, click Add Credential and provide the required information.



Add New Credential

SNMP Version: SNMP v3 ▼

SNMP v3 Credential

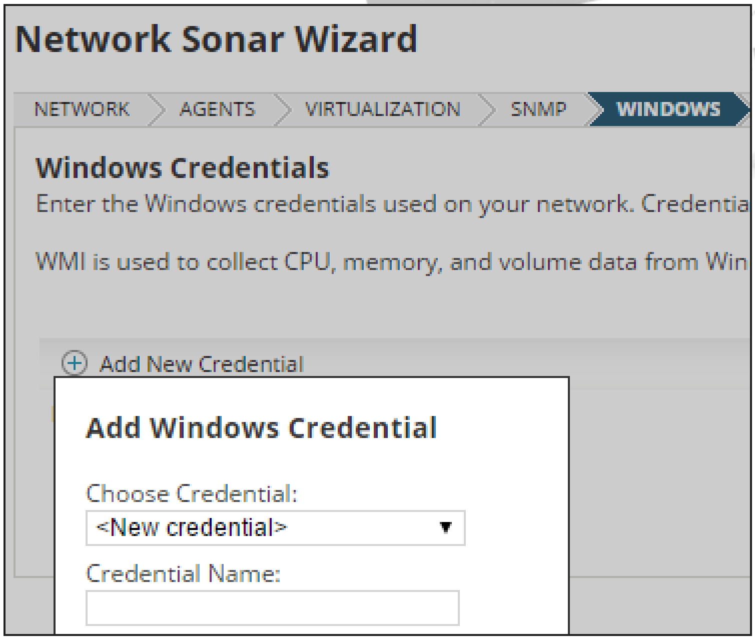
Choose Credential: <New credential> ▼

User Name:			
Context:			
Authentication Method:	None ▼	Password / Key:	×
Privacy / Encryption Method:	None ▼	Password / Key:	×

ADD CANCEL

6. On the Windows panel, to discover WMI or RPC-enabled Windows devices, click Add New Credential and provide the required information.

SolarWinds recommends that you monitor Windows devices with WMI instead of SNMP.



Network Sonar Wizard

Windows Credentials

Enter the Windows credentials used on your network. Credentia

WMI is used to collect CPU, memory, and volume data from Win

⊕ Add New Credential

Add Windows Credential

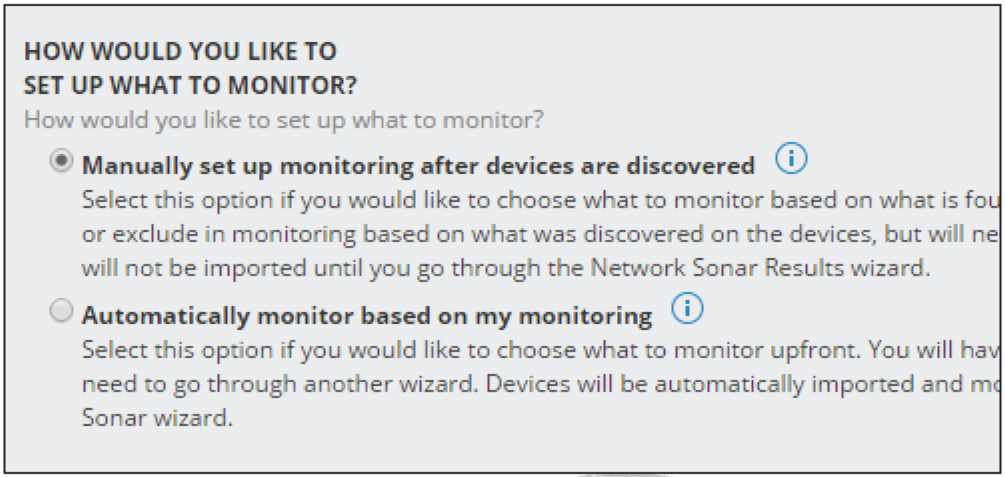
Choose Credential: <New credential> ▼

Credential Name:

7. On the Monitoring Settings panel, SolarWinds recommends manually setting up monitoring the

first time you run discovery. This allows you to review the list of discovered objects and select the ones you want to monitor.

When you scale monitoring, you can configure discovery to automatically start monitoring objects it finds.



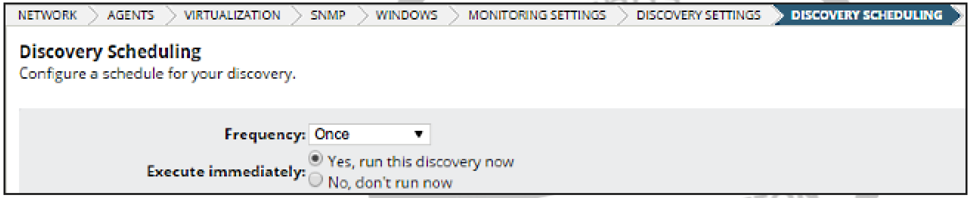
HOW WOULD YOU LIKE TO
SET UP WHAT TO MONITOR?

How would you like to set up what to monitor?

● **Manually set up monitoring after devices are discovered** ⓘ
Select this option if you would like to choose what to monitor based on what is fou
or exclude in monitoring based on what was discovered on the devices, but will ne
will not be imported until you go through the Network Sonar Results wizard.

○ **Automatically monitor based on my monitoring** ⓘ
Select this option if you would like to choose what to monitor upfront. You will hav
need to go through another wizard. Devices will be automatically imported and mo
Sonar wizard.

8. On the Discovery Settings panel, click Next.
9. Accept the default frequency and run the discovery immediately.

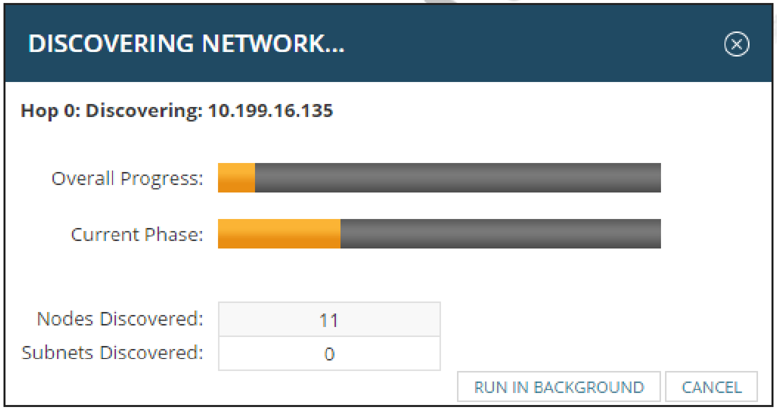


Discovery Scheduling
Configure a schedule for your discovery.

Frequency: Once

Execute immediately: ● Yes, run this discovery now
○ No, don't run now

Discovery can take anywhere from a few minutes to a few hours, depending on the number of network elements the system discovers.



DISCOVERING NETWORK...

Hop 0: Discovering: 10.199.16.135

Overall Progress:

Current Phase:

Nodes Discovered: 11

Subnets Discovered: 0

Add a single node for monitoring

As an alternative to using the Network Sonar Discovery wizard, you can add individual nodes for monitoring.

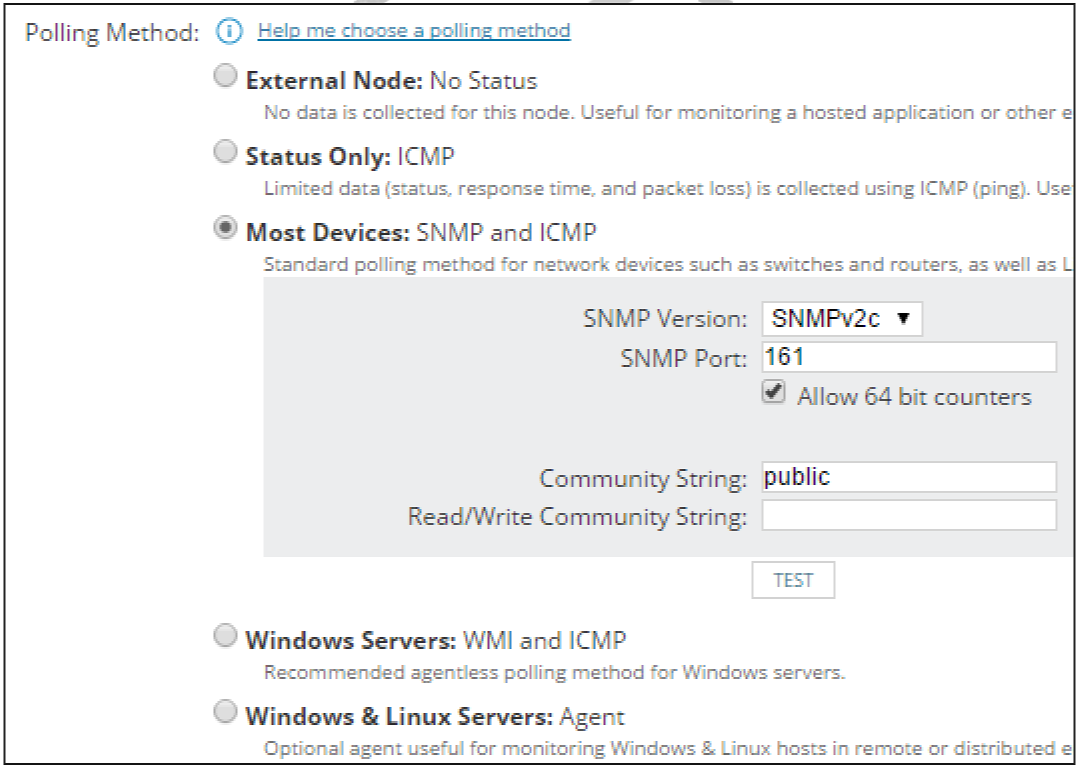
Adding a single node offers more detail in monitoring and is the recommended approach when you have a node with high latency. Do not include nodes with high latency in a discovery job.

As you add a single node for monitoring, you can:

- Select the statistics and resources to monitor.
- Add Universal Device Pollers.
- Identify how often the node status, monitored statistics, or topology details are updated.
- Add custom properties.
- Edit alert thresholds.

To add a single node for monitoring:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes, and then click Add a Node.
3. Specify the node, and click Next.
   a. Provide the host name or IP address.
   b. Select the polling method, and provide credentials.



Polling Method: Help me choose a polling method

○ **External Node:** No Status
No data is collected for this node. Useful for monitoring a hosted application or other e

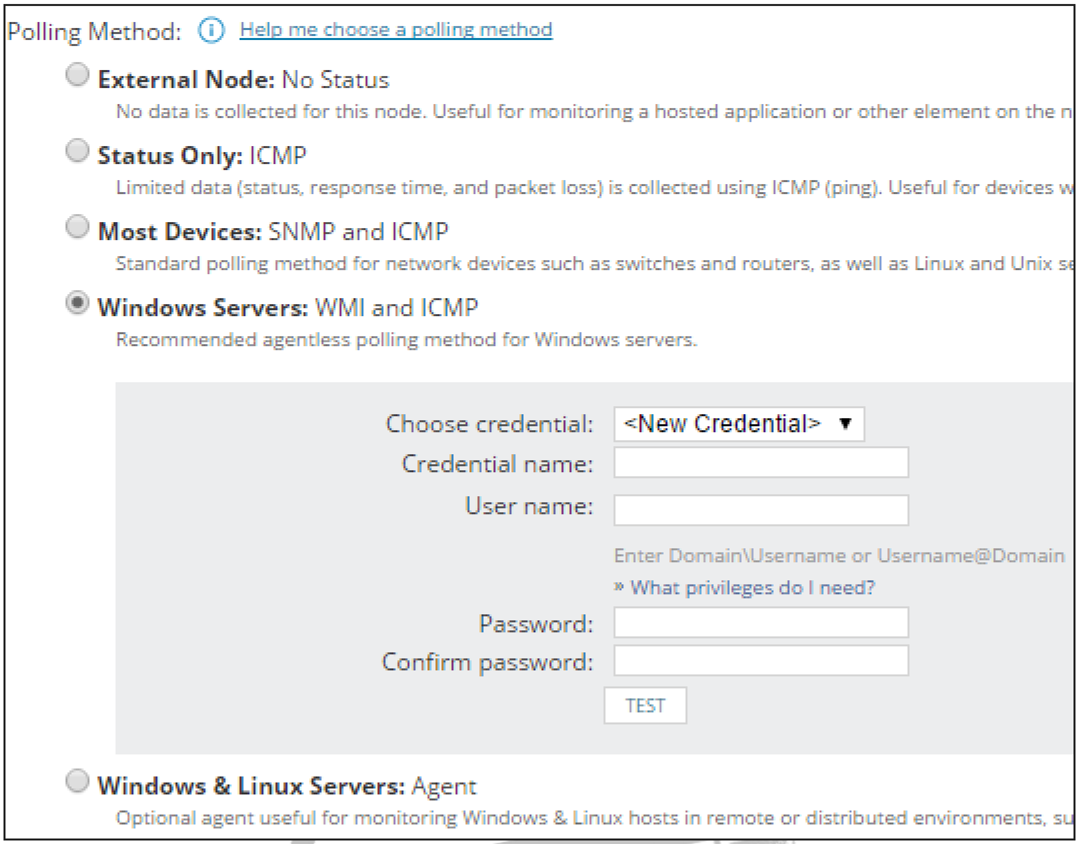
○ **Status Only:** ICMP
Limited data (status, response time, and packet loss) is collected using ICMP (ping). Use

● **Most Devices:** SNMP and ICMP
Standard polling method for network devices such as switches and routers, as well as L

SNMP Version: SNMPv2c
SNMP Port: 161
☑ Allow 64 bit counters
Community String: public
Read/Write Community String:

○ **Windows Servers:** WMI and ICMP
Recommended agentless polling method for Windows servers.

○ **Windows & Linux Servers:** Agent
Optional agent useful for monitoring Windows & Linux hosts in remote or distributed e



Polling Method: ⓘ Help me choose a polling method

○ **External Node:** No Status
No data is collected for this node. Useful for monitoring a hosted application or other element on the n

○ **Status Only:** ICMP
Limited data (status, response time, and packet loss) is collected using ICMP (ping). Useful for devices w

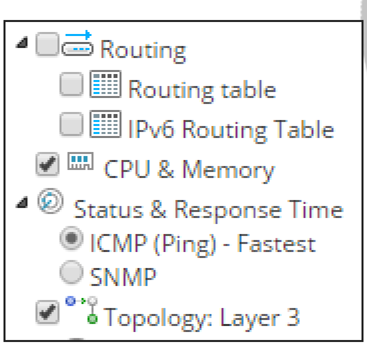
○ **Most Devices:** SNMP and ICMP
Standard polling method for network devices such as switches and routers, as well as Linux and Unix se

● **Windows Servers:** WMI and ICMP
Recommended agentless polling method for Windows servers.

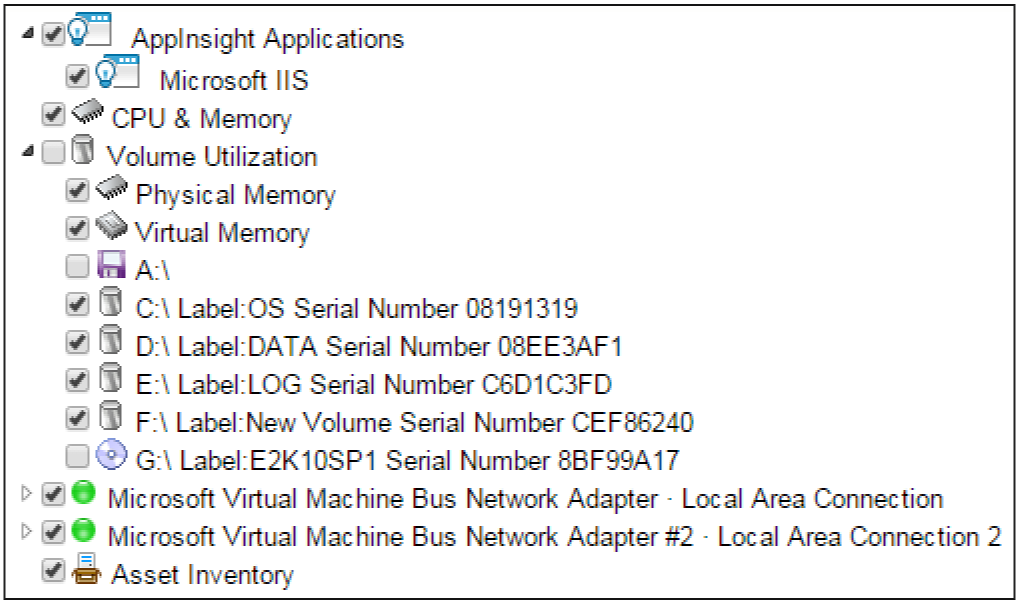
Choose credential: <New Credential> ▼
Credential name:
User name:
Enter Domain\Username or Username@Domain
» What privileges do I need?
Password:
Confirm password:
TEST

○ **Windows & Linux Servers:** Agent
Optional agent useful for monitoring Windows & Linux hosts in remote or distributed environments, su

4. Select the statistics and resources to monitor on the node, and click Next.

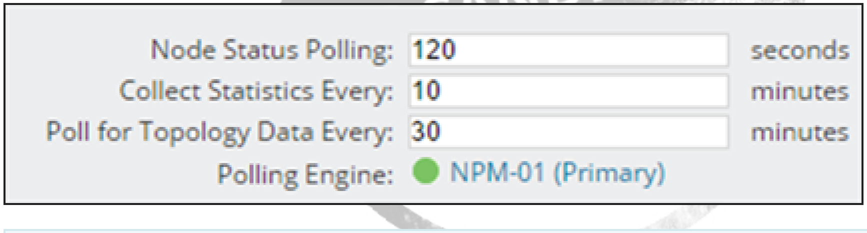


- □ Routing
  - □ Routing table
  - □ IPv6 Routing Table
- ☑ CPU & Memory
- Status & Response Time
  - ● ICMP (Ping) - Fastest
  - ○ SNMP
- ☑ Topology: Layer 3



- ☑ AppInsight Applications
  - ☑ Microsoft IIS
- ☑ CPU & Memory
- □ Volume Utilization
  - ☑ Physical Memory
  - ☑ Virtual Memory
  - □ A:\
  - ☑ C:\ Label:OS Serial Number 08191319
  - ☑ D:\ Label:DATA Serial Number 08EE3AF1
  - ☑ E:\ Label:LOG Serial Number C6D1C3FD
  - ☑ F:\ Label:New Volume Serial Number CEF86240
  - □ G:\ Label:E2K10SP1 Serial Number 8BF99A17
- ☑ ● Microsoft Virtual Machine Bus Network Adapter - Local Area Connection
- ☑ ● Microsoft Virtual Machine Bus Network Adapter #2 - Local Area Connection 2
- ☑ Asset Inventory

5. If you want to monitor a special metric on the node and have defined the metric using a custom poller, select the poller on the Add Pollers pane, and click Next.
6. Review and adjust the device properties.
   a. To edit the SNMP settings, change the values, and click Test.
   b. To edit how often the node status, monitored statistics, or topology details are updated, change the values in the Polling area.



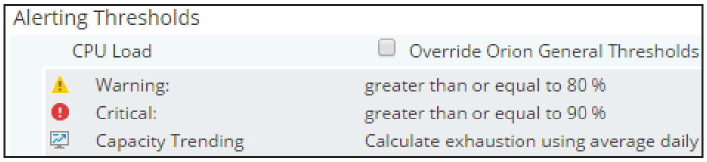
Node Status Polling: 120 seconds
Collect Statistics Every: 10 minutes
Poll for Topology Data Every: 30 minutes
Polling Engine: ● NPM-01 (Primary)

For critical nodes, you may need to poll status information or collect statistics more frequently than the default polling intervals.
Change the polling intervals if polling the nodes takes too long.

   c. Enter values for custom properties for the node.

   The Custom Properties area will be empty if you have not defined any custom properties for the monitored nodes. See "Add custom properties to nodes" in the SolarWinds Getting Started Guide - Customize.

   d. To adjust when the status of the node changes to Warning or Critical, edit alerting thresholds for the metric. Select the Override box and set thresholds specific for the node.



Alerting Thresholds

CPU Load	□ Override Orion General Thresholds
⚠ Warning:	greater than or equal to 80 %
● Critical:	greater than or equal to 90 %
Capacity Trending	Calculate exhaustion using average daily

7. Click OK, Add Node.

   The node will be monitored according to the options you set.

Restrict user access to network areas by applying limitations

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

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

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

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

> - Group limitations are not applied until after the group availability is calculated.
> - Because SolarWinds NetFlow Traffic Analyzer (NTA) initially caches account limitations, it may take up to a minute for account limitations to take effect in SolarWinds NTA.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the User Accounts grouping, click Manage Accounts.
4. Edit an individual or group account.
   a. Click Add Limitation in the Account Limitations section.
   b. Select the type of limitation to apply, and click Continue.
   c. Define the limitation, and click Submit.

      The limitation will be added to the Edit Account page.
5. Click Submit.

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

Patterns for limitations

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

> Patterns are not case sensitive.

You may also group operators using parentheses, as in the following example.

`(*foo* EXCEPT *b*) AND (*all* OR *sea*)` matches `seafood` and `footfall`, but not `football` or `Bigfoot`.

Create limitations based on custom properties

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

> ⓘ
> - Before you start, plan how you want to limit the user access, and create custom properties.
> - This procedure requires access to the computer that hosts the Orion server.

1. Click Start > All Programs > SolarWinds Orion > Grouping and Access Control > Account Limitation Builder.
2. Click Start on the splash screen.
3. Click Add Limitation.
4. Select a Custom Property. The fields are populated automatically based on your selection.
5. Choose a Selection Method.

   > ⓘ This is the selection format that will appear when you are choosing values for the account limitation in the Orion Web Console.

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

6. Click OK.

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

Poll devices with SolarWinds Orion agents

An agent is software that provides a communication channel between the Orion server and a Windows or Linux/Unix computer. Products install plugins on agents to collect the data that the agents send back. This can be beneficial in situations such as:

- Polling hosts and applications behind firewall NAT or proxies.
- Polling nodes and applications across multiple discrete networks that have overlapping IP address space.
- 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 main polling engine.

You can monitor servers hosted by cloud-based services such as Amazon EC2, Rackspace, Microsoft Azure, and other Infrastructure as a Service (IaaS).

After deployment, all communication between the Orion server and the agent occur over a fixed port. This communication is fully encrypted using 3072-bit TLS encryption. The agent protocol supports NAT traversal and passing through proxy servers that require authentication.

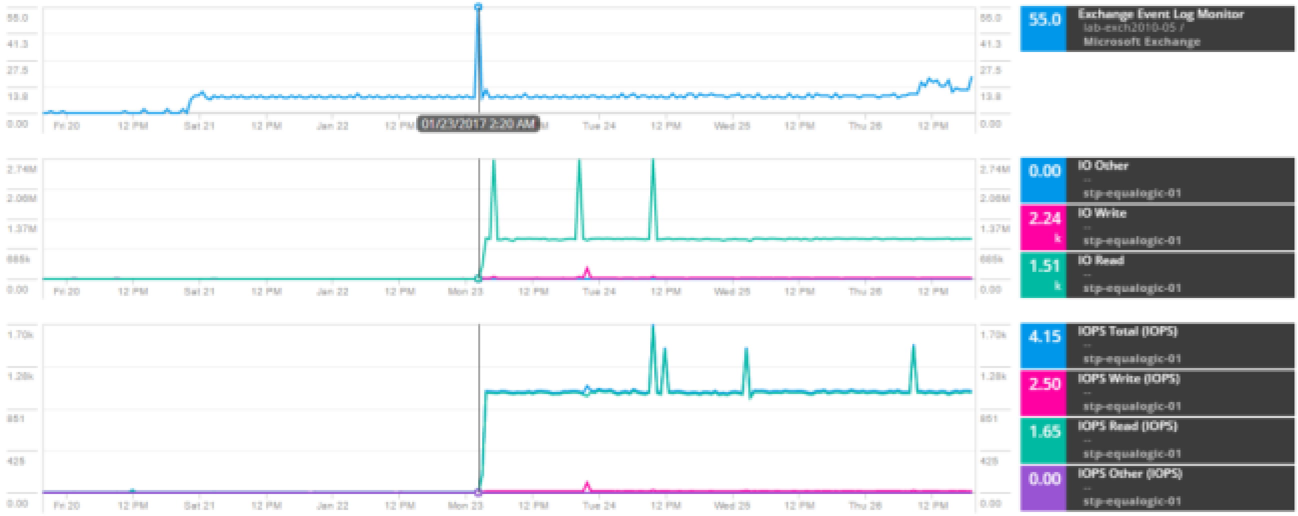
Troubleshooting environmental issues with Performance Analysis dashboards

Create analysis projects with the Performance Analysis (PerfStack™) dashboard. Analysis projects visually correlate time series data, both historical and current, from multiple SolarWinds products and entity types in a single view. This allows you to:

- Troubleshoot issues in real-time.
- Create ad-hoc reports.
- Identify root causes of intermittent issues.
- Make data-driven decisions on infrastructure changes.

Drag and drop performance metrics, events, and log data from multiple device types to a chart to perform deep analysis of what was going on in your environment when the issue occurred, including real-time polling for issues you're experiencing now. You can mix and match metrics from data collected across multiple SolarWinds products for both broad and in-depth insight to your infrastructure.

For example, you could identify an issue in your application that causes disk I/O to spike and slowdowns if you collect SRM and SAM data. After your project is built, share the troubleshooting project with other members of your team for remediation.



Compatible SolarWinds products

ⓘ Performance Analysis is most useful in correlating performance data when multiple SolarWinds products are installed.

Correlate data from the following SolarWinds products:

- NPM 12.3 or later
- SAM 6.6.1 or later
- VMAN 8.2.1 or later
- NTA 4.2.3 or later
- SRM 6.6 or later
- WPM 2.2.2 or later
- EOC 2.1 or later
- NCM 7.8 or later (Configuration changes)
- VNQM 4.5 or later (IPSLA operations)
- DPAIM 11.1 or later (DPA integrated with the Orion Platform)

If you have at least one of these products installed together on the same server, you can access Performance Analysis dashboards. However, you may not be able to use all collected metrics if you pull data from older product versions.

⚠ Some data are either not available or partially available in the Performance Analysis dashboard, such as data from the following:

- NetPath™

For a more complete list, see SolarWinds KB MT85165.

- Create analysis projects
- Update charts in real-time (Real-Time Polling)
- View the polled data for a plotted metric
- Modify the time range for all charts
- View more information for an entity
- Share analysis projects
- View your saved analysis projects
- Add saved analysis projects to views as a widget
- Delete analysis projects

Create analysis projects

The entities and metrics you can add to your analysis project depends on the SolarWinds products installed on your Orion server.

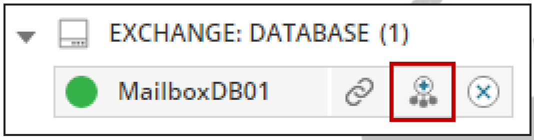
- The rocket ship next to a metric means that the Orion Platform can collect real-time data for the metric.
- The data line may not fully extend to the right of the chart because it is based on the last polling time.
- Depending on your account limitations, you may not have access to all available data, metrics, or entities. However, all users can create Performance Analysis troubleshooting projects.

Create analysis projects from the Performance Analysis dashboard

1. Click My Dashboards > Home > Performance Analysis.

   If you customize your dashboards, Performance Analysis might not be in the menu bar. Click Settings > All Settings > User Accounts > Edit and note what you use for HomeTab Menu bar. Click My Dashboards > Configure, and add Performance Analysis to the menu bar you used in HomeTab Menu bar.

2. Add entities.
   You can add a key entity and then add all other related entities. Hover over the entity in the metric palette and click the Add related icon.

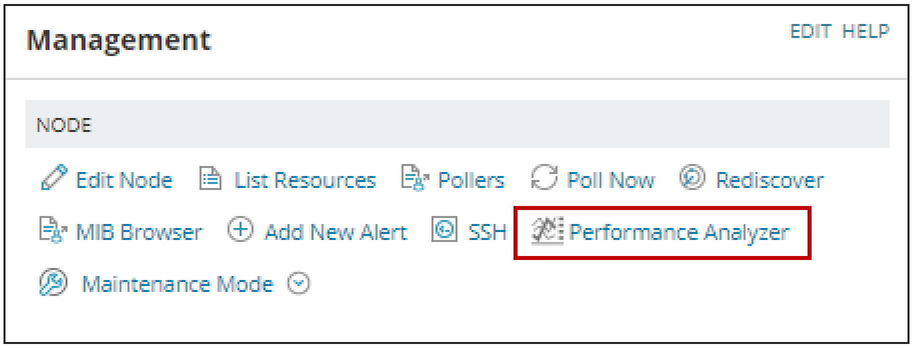


3. Select an entity and choose metrics to drag to the dashboard. You can also drag and drop an entity directly to the charts.

Create analysis projects from the entity details page

You can open an analysis project directly from the details page of nodes, interfaces, IPSLA operations, clusters, datastores, hosts, VMs, LUNs, SRM pools, storage arrays, volumes, cloud instances, and applications.

1. Open the details page to an entity.
2. Click Performance Analyzer on the Management widget.



This opens a project with relevant metrics from the entity already charted. For example, key metrics for node entities include:

- Average CPU Load
- Average Percent Memory Used
- Average Response Time
- Alerts
- Events
- Status

ⓘ Metrics that are not collected for an entity are not added.

You can add more metrics from related entities.

Update charts in real-time (Real-Time Polling)

Metrics denoted by a rocket ship icon can use high frequency polling, one second apart, to update their charts. You can have both real-time metrics and regular metrics in your project. You can only have 10 real-time pollable metrics in your project. If you have 11, Real-Time Polling cannot start. Your project has a 10 minute window of real-time metrics.

ⓘ

- You may not have the option to poll entities in real-time. This option is controlled through individual account settings and is based on the version of Orion Platform your installation runs on. Orion Platform version 2017.3 includes this option. EOC installations and DPA metrics do not have this option.
- You can poll up to 30 unique metrics across all user accounts in real-time. After this limit is reached, a warning message displays.
- When you stop Real-Time Polling, the metrics will continue to poll at the accelerated pace for two minutes before stopping.
- Real-Time Polling does not affect normal polling intervals.

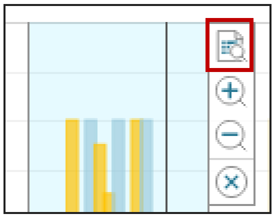
Click Start Real-Time Polling in the toolbar.

All real-time enabled metrics in your analysis dashboard begin to poll the entities approximately every second. When the rocket ship icon flashes, Real-Time Polling has started. The icon stops flashing when data from the first poll is returned.

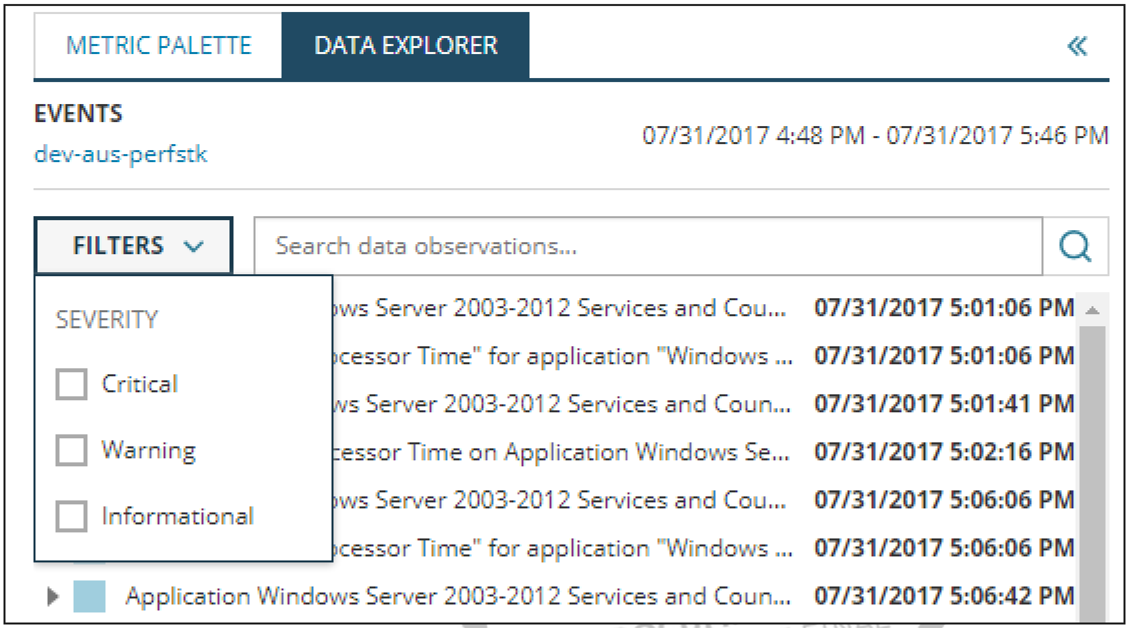
View the polled data for a plotted metric

ⓘ This is available for Syslog, SNMP Traps, Events, Alerts, and Configuration changes on installations running on Orion Platform version 2017.3.

Click and drag a selection on a chart, and click on the icon with the magnifying glass.



The Data Explorer tab opens with the data that for the chart within the time frame you select. Use the Filters menu or the search bar to further reduce the visible data.



EVENTS

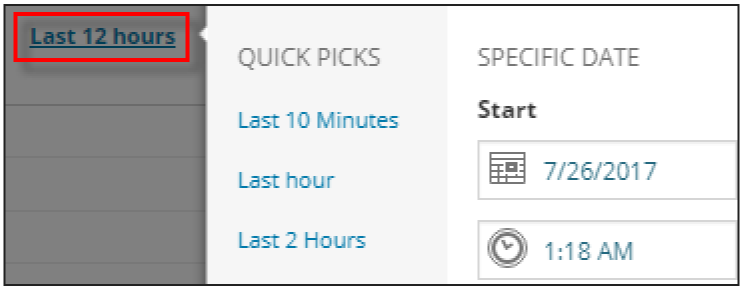
dev-aus-perfstk

07/31/2017 4:48 PM - 07/31/2017 5:46 PM

```
ows Server 2003-2012 Services and Cou...          07/31/2017 5:01:06 PM
ocessor Time" for application "Windows ...        07/31/2017 5:01:06 PM
ws Server 2003-2012 Services and Coun...          07/31/2017 5:01:41 PM
cessor Time on Application Windows Se...          07/31/2017 5:02:16 PM
ows Server 2003-2012 Services and Cou...          07/31/2017 5:06:06 PM
ocessor Time" for application "Windows ...        07/31/2017 5:06:06 PM
Application Windows Server 2003-2012 Services and Coun...   07/31/2017 5:06:42 PM
```

Modify the time range for all charts

You can set absolute, relative, or custom time ranges simultaneously across all charts in your troubleshooting project at the top of the dashboard.

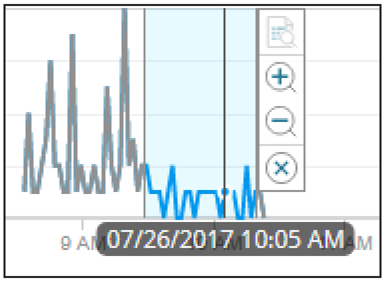


Start

7/26/2017

1:18 AM

Click and drag to select a time range on a chart and zoom in or out using the hover menu. Click the X button to cancel the selection and return focus to the entire chart area.



View more information for an entity

Open the entity details page directly from the analysis project to view more information, such as MAC addresses or model numbers. Hover over the entity in the metric palette and click the link icon.

Share analysis projects

Click the Share button in your analysis dashboard to copy the project's URL to your clipboard. Share the URL so others can:

- Use the projects as-is and have the same data to troubleshoot issues.
- Modify the project and sent the URL back to you.
- Save it to their own Performance Analysis dashboard by clicking More > Save As.
- Add the project to a menu bar.

For example, you may use a troubleshooting project to identify the root cause of an issue you are experiencing and send the URL in a help desk ticket for a technician to view, or you may share it with members of your team to refine your diagnoses or use as a troubleshooting tool.

You can send the URL to anyone with access to the Orion Web Console. When a person views the troubleshooting project, all node access limitations are applied.

View your saved analysis projects

Click Load at the top of the dashboard to open your most recently used projects, or search for your saved projects. You can only view projects that you have created or saved, and you cannot save a project with Real-Time Polling enabled. You must manually turn Real-Time Polling on when loading a project.

Add saved analysis projects to views as a widget

With a performance analysis project as a widget on a view, you can compare the project with other data on the view, or show the performance analysis data on a NOC view.

ⓘ Adding widgets on views requires an account with View Customization privileges.

1. Go to the Orion Web Console view.
   When adding the widget to a Node Details page, make sure limitations do not prevent the data from displaying.
2. Click the Pencil icon in the top left corner, and search for the Performance Analysis project in Available Widgets.

   > To find the widget, search for a string from the project's name.
   > You can also search in the Group by list in the following categories: Type > Charts, Features > Performance Analysis, or Classic > Performance Analysis.

3. Drag and drop the project to the view and click Done Adding Widgets.

Cannot find your project in Available Widgets?

You can only add saved performance analysis projects as a widget. If you haven't saved any projects, no performance analysis widgets are visible in Available Widgets.

Delete analysis projects

Click More > Delete to remove a project. You can only delete projects you have created. If a user creates a project and is removed from the SolarWinds user list, the projects that user saved are not removed from the server.

If you delete a troubleshooting project that you have shared with others, you are only deleting your copy.

Add a Performance Analysis Project to the menu

Create a link directly to frequently used PerfStack™ analysis projects directly in your global navigation. View and account limitations apply to the project.

1. In your analysis project, click Share. The project's URL is automatically copied to your clipboard.
2. Click My Dashboards > Configure.
3. Click Edit on the menu bar you want to add the project to.
4. Click Add under Available items.
5. Enter the name for the project you want to display in the menu.
6. Enter the URL copied from the analysis project, and click OK.
7. Move the new menu item to the Selected items column, and click Submit.

The menu has a link to the Performance Analysis project.

> Click on the full-screen ⤢ button on saved projects to have a non-interactive, full-screen view that you can use in NOCs.

Manage reports in the Orion Web Console

SolarWinds provides predefined reports for each Orion Platform product. You can use the reports as soon as there is data to be reported on.

View a list of predefined reports by clicking Reports > All Reports in the menu bar.

Use the web-based interface to customize the predefined reports or create your own reports.

ⓘ The Orion Web Console does not allow you to edit legacy reports created with the Orion Report Writer.