GETTING STARTED GUIDE

Server & Application Monitor

Version 6.8
GETTING STARTED GUIDE: SERVER & APPLICATION MONITOR

© 2018 SolarWinds Worldwide, LLC. All rights reserved.

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

Get started with Server & Application Monitor ................................................................. 6

- Who this guide is for ........................................................................................................... 6
- What's in this guide ............................................................................................................ 7
- Learn more ....................................................................................................................... 7
- Product terminology ........................................................................................................ 7
- Log into the Orion Web Console .................................................................................... 8
- Navigate your environment .............................................................................................. 9
- Explore SolarWinds SAM widgets .................................................................................. 10
  - Management actions for nodes, applications, and components ............................... 13
- Introduction to the AppStack environment ..................................................................... 14

**Discover your environment** .......................................................................................... 17

- What should I monitor? .................................................................................................... 17
- Discovery checklist .......................................................................................................... 18
- Monitoring overview ....................................................................................................... 19
  - Monitoring with Orion agents ..................................................................................... 19
  - Monitoring with SNMP ............................................................................................... 19
  - Monitoring with WMI ................................................................................................. 19
  - Deciding between SNPM and WMI ............................................................................ 20
- Discover your servers and applications ......................................................................... 21
- Add discovered servers and applications to SolarWinds SAM ...................................... 24

**Monitor your environment** .......................................................................................... 27

- How SAM works ............................................................................................................. 27
- Understand the relationship between applications and templates ............................. 28
- Monitor Internet Information Services (IIS) .................................................................... 30
  - Add AppInsight for IIS to a node ............................................................................... 30
  - View IIS application data ............................................................................................ 32
  - Navigate to the AppInsight for IIS details view ......................................................... 32
  - Navigate to the website details view .......................................................................... 32
Navigating to the application pools view ................................................................. 32
Navigating to the performance counter details view ................................................ 33
Expert knowledge for AppInsight performance counters ........................................... 33
Monitoring your operating system ........................................................................... 33
Before you begin ......................................................................................................... 34
Applying a template to a node .................................................................................. 34
Viewing the application data ..................................................................................... 36
Configuring hardware health monitoring ................................................................. 37
Monitoring hardware health .................................................................................... 38
Monitoring cloud instances and VMs ...................................................................... 40
Investigating application performance with Performance Analysis ....................... 42
Explore alerts and reports ....................................................................................... 47
How alerts work ......................................................................................................... 47
Managing and using alerts ...................................................................................... 49
List preconfigured, enabled alerts .......................................................................... 49
Enabling and disabling alerts .................................................................................. 50
Action types ............................................................................................................... 50
Configuring the default email action ....................................................................... 51
Managing active alerts ............................................................................................. 52
Creating a custom alert ............................................................................................ 55
How reports work ..................................................................................................... 57
Running a preconfigured report .............................................................................. 59
Enabling Asset Inventory data collection .................................................................. 59
Generating the report ............................................................................................... 60
Scheduling a report .................................................................................................... 61
Creating a SAM custom report ................................................................................ 61
Creating a custom property to identify nodes running IIS ........................................ 62
Creating the IIS application server issue rollup report ............................................... 64
Work with templates ............................................................................................... 70
Creating a template for an application ...................................................................... 70
Create a template to monitor file size ................................................................. 70
Apply the template to a node .............................................................................. 71
Import and export templates in SAM .................................................................. 72
Export a template ................................................................................................. 73
Import a template ................................................................................................. 74
Share application monitor templates on THWACK .............................................. 75
Export a template ................................................................................................. 75
Import a template ................................................................................................. 75

Set thresholds ....................................................................................................... 77
How thresholds work ............................................................................................. 77
Edit a global threshold .......................................................................................... 77
Edit a local node threshold .................................................................................... 78
Edit a local component monitor threshold .......................................................... 80
Edit an application template threshold ............................................................... 82

Understand agents ................................................................................................. 83
How agents work .................................................................................................... 83

Agent communication modes .............................................................................. 84
Server-initiated communication ........................................................................... 84
Agent-initiated communication ............................................................................. 85
Deploy an agent with the Add Node wizard ......................................................... 85
Agent resource consumption ............................................................................... 87
Agent settings ......................................................................................................... 87
Get started with Server & Application Monitor

This guide picks up right after the SAM installation process and walks you through the first steps you need to take to monitor applications, hardware health, asset inventory and operating performance in your environment.

- **Get started.** Plan your implementation, set up SAM, and collect data about your environment.
  - Understand the SAM environment and learn about the Application Stack
  - Discover applications, servers, cloud instances/VMs, and devices
  - Monitor applications, hardware health, assets, cloud instances/VMs, and more
  - Use **Performance Analysis (PerfStack)** to identify issues before customers call the help desk
  - Prepare alerts and reports

- **Customize.** Tailor SAM to your internal processes so you can more effectively respond to performance issues.
  - Create templates for custom applications
  - Create and assign custom properties to nodes
  - Create dependencies between applications and supporting infrastructure
  - Create custom pages
  - Create dashboard views and adjust user permissions
  - Create custom alerts and reports

**Who this guide is for**

<table>
<thead>
<tr>
<th>NEW SAM USERS</th>
<th>EXISTING SAM USERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>This guide is meant for you and is the best place to start with SAM.</td>
<td>You'll find more advanced information in the <a href="#">SAM Administrator Guide</a>. To upgrade SAM, see the <a href="#">SolarWinds Upgrade Guide</a>.</td>
</tr>
</tbody>
</table>

**Existing customers:** Follow recommendations in this guide to ensure your system capabilities are appropriate and your environment is sized correctly. Minimum system requirements used during evaluation are not sufficient for a production environment. Access your licensed software from the [SolarWinds Customer Portal](#). If you need implementation help, contact [Customer Support](#). See [Working with Support](#) to learn how to open a support case with the correct level of visibility.

**Evaluators:** If you are evaluating SolarWinds SAM, concentrate on the Get Started and Customize objectives described earlier. As you work through the guide, you will see some topics that provide information for production deployments. That information is included to provide a sense of what a production environment looks like. Download a free 30-day evaluation [here](#). For assistance during evaluation, contact [sales@solarwinds.com](mailto:sales@solarwinds.com).
What's in this guide

**Log into the Orion Web Console:** Access the Orion Web Console, which you'll use to do everything in SAM, from discovering applications to setting up alerts, thresholds, and application monitoring templates.

**Discover your environment:** Identify the servers and applications you want to monitor and add them to the Orion Web Console.

**Monitor your environment:** Learn about monitoring with templates, using AppInsight for IIS, monitoring your OS, tracking hardware health, working with your cloud infrastructure, and using PerfStack™.

**Explore alerts and reports:** Manage and use alerts, and then set up reports.

**Work with templates:** Create templates for custom applications and explore templates in the SolarWinds online IT community, THWACK.

**Set thresholds:** Learn how to set up global and local thresholds to automate monitoring.

**Understand agents:** Get to know agents and how they're used for SAM monitoring.

Learn more

- To install SAM, review the latest system requirements and release notes, and then use the SolarWinds Orion Installer.
- To get the latest version of SAM, use the SolarWinds Upgrade Guide.
- The SAM Administrator Guide provides an overview of product features and related technologies. In addition to details about configuring and using SolarWinds SAM, it contains recommendations on best practices, and troubleshooting information for common situations.
- To learn about features shared by SAM and other Orion Platform products, such as user accounts, views, dashboards, and alerts, see the Orion Platform Administration Guide.

The Orion Platform Administration Guide describes ways to fine-tune your SAM deployment by working with custom properties and groups, creating custom views, reducing alerting noise, and more.

- Visit the SolarWinds Success Center for product guides, training resources, and technical support articles.
- Check out the Server & Application Monitor product forum in our online IT community, THWACK, to connect with SolarWinds developers, product managers, and other SAM users. Download templates, reports, scripts and more to customize and extend SAM.

Product terminology

**Orion Platform:** The common backend platform used by the Solarwinds Orion suite of products, including NPM, SAM, NCM, NTA, WPM, and more. The Orion Platform is the backbone for navigation, settings, and common features like alerts and reports. It also provides a consistent look-and-feel across products, giving you a "single pane of glass" for your Orion monitoring tools.
**Orion Web Console:** The web interface you see when you log into the Orion Web Console that is used to view, configure, and manage all of your monitored objects.

**Orion server:** A Microsoft Windows server that hosts the Orion Web Console and collects data from monitored objects. Also called the Orion Main Poller or Main Polling Engine.

**Orion database server:** A Windows SQL server that is hosted on a dedicated server in a production environment, separate from the Orion Application Server. It stores Orion configuration data plus collected performance and Syslog data.

**Polling engine:** A polling engine controls polling job scheduling, data processing, and queries your monitored devices for performance metrics like CPU, memory, and up/down status. Additional Polling Engines (APEs) can be licensed to provide additional scalability and capacity. By default, the Orion Server provides one polling engine, that is often called the "main polling engine."

**Node:** A node is considered to be any endpoint of a given network. For example, any application, server, device, or computer on a network is considered a node.

**Template:** A template is the blueprint for an application. It is a collection of component monitors designed to monitor a server or application. You can customize numerous templates using only the component monitors you need for a specific environment. For a list of out-of-the-box templates, see the [SAM Template Reference](#).

**Application:** An application or application monitor in SAM monitors a specific application or server using a collection of component monitors.

**Component Monitor:** A component monitor is the fundamental element of an application. Component monitors return the current status or value of a monitored service or process. All component monitors return at least one value or one status condition. For a full list of component monitors, see [SAM Component Monitor Types](#).

**Log into the Orion Web Console**

As with all Orion Platform products, you can access SAM by logging into the Orion Web Console to do everything from adding devices to discovering applications for monitoring, and setting up alerts.

In a web browser, navigate to `http://hostnameOrIPAddress:port` where:

- `hostnameOrIPAddress` is the hostname or IP address of the Orion server where SAM is installed.
- `port` is the Orion Web Console port defined for the website. This is configurable during installation. The default port is 8787.
You'll see the Orion login page:

If your SAM environment is new, you can log in as the default admin user with no password.

SolarWinds recommends setting up users with the Account Manager to ensure your data and network remain in your control. The Orion Platform supports different permissions for users, including administrator-level users that can access to all key features and configurations.

Navigate your environment

SolarWinds SAM includes many views and widgets (formerly called "resources") that you can use to manage and troubleshoot an environment. A widget is a building block that displays on a view as a box and provides information about different aspects of monitoring, usually in a chart or table. Some widgets are intended for use on summary views, some are suitable for detail views, and some can be useful on both view types.

The following figure shows several widgets in a single summary view, including a widgets with gauges that displays statistics for multiple components:
Some widgets and views are not visible by default and can be added by editing settings.

Explore SolarWinds SAM widgets

Most widgets (formerly called "resources") in the SAM environment are actionable. For example, drilling down to and clicking an individual node in the All Nodes widget on the Summary page takes you to the Node Details page. The Node Details page contains widgets that provide information about this node.

The following example shows the Management widget, which is one of many widgets available on the Node Details page.
Clicking Manage Nodes in the All Nodes widget opens the Manage Nodes page where you can take action on multiple nodes.

Use the All Applications widget on the Summary page to drill down to individual applications and component monitors of an application. The Application Details page provides details about the individual application and actions you can perform on that application. This allows you to manage templates and applications to node assignments, or "unmanage" (that is, stop managing) multiple applications at one time.
Clicking Manage Applications in the All Applications widget takes you to the Manage Applications page where you can troubleshoot and resolve issues on multiple applications.

Expand an application name to show all component monitors associated with that application. Click a component monitor to access the Component Monitor details page to view detailed information and perform additional actions.
Management actions for nodes, applications, and components

The Orion Platform provides many options to manage nodes, applications, and components, similar to how Windows Task Manager works.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Node</td>
<td>Edit the properties of a node and the polling method used.</td>
</tr>
<tr>
<td>List Resources</td>
<td>Display resources that indicate what is being monitored.</td>
</tr>
<tr>
<td>Unmanage</td>
<td>Suspend polling and collecting statistics for a set period of time.</td>
</tr>
<tr>
<td>Poll Now</td>
<td>Reschedules a job to run immediately. If the job scheduler is at capacity, the job may not execute immediately, but it will execute before the next scheduled poll cycle.</td>
</tr>
<tr>
<td>Rediscover</td>
<td>Update node data such as machine type, system name, or location.</td>
</tr>
<tr>
<td>Add New Alert</td>
<td>Create a new alert for a node.</td>
</tr>
<tr>
<td>Real-Time</td>
<td>Stop, start, and select processes to monitor.</td>
</tr>
<tr>
<td>Process Explorer</td>
<td>Stop, start, and restart services.</td>
</tr>
<tr>
<td>Service Control</td>
<td>Stop, start, and restart services.</td>
</tr>
<tr>
<td>Manager</td>
<td></td>
</tr>
<tr>
<td>Real-time Event</td>
<td>Display a list of system events and start monitoring events.</td>
</tr>
<tr>
<td>Log Viewer</td>
<td></td>
</tr>
<tr>
<td>Reboot</td>
<td>Restart the remote computer.</td>
</tr>
</tbody>
</table>

These controls are available on the Details page of the node, application, or component in the Management widget.
Introduction to the AppStack environment

SolarWinds SAM provides an Application Stack (AppStack) with an interactive visual map that displays a detailed view of your environment, helping to identify the root cause of performance and availability issues. Use AppStack to assess the overall health of your environment and to troubleshoot specific and related problems.

An AppStack view is also available at the application layer that only shows the relationships for that application. This view is called the Mini-Stack.

AppStack provides a more thorough analysis of root cause problems in your environment if combined with Storage Resource Manager, Virtualization Manager, and Web Performance Monitor.

To access the AppStack Environment page:

1. Click My Dashboards > Environment.

The AppStack environment generates categories that show the status of objects in your IT environment. Objects on the left are the highest priority.
2. Click an object to highlight related objects and gray out unrelated objects.

3. Click Spotlight to remove unrelated objects.

4. To investigate further, click the selected object.
The relevant Details page appears.
Discover your environment

After you install SolarWinds SAM, you can identify the devices you want to monitor, and add them to the SolarWinds Orion database.

- To automatically discover and add a larger number of devices across your enterprise, use the Network Sonar Discovery and Network Sonar Results Wizards.
- To add individual objects for monitoring, add single nodes using Node Management in the Orion Web Console.

After adding application servers, review the following topics in this guide:

- What should I monitor?
- Discover your servers and applications
- Add discovered servers and applications to SolarWinds SAM

To learn about the following topics, see the Orion Platform Administrator Guide:

- Add nodes using Active Directory
- Choose polling methods
- Import nodes
- Manage scheduled discovery results
- Minimize SNMP processing load during Discovery
- Group objects and mirroring network dependencies

What should I monitor?

*Discovery* is a term used to describe the process SolarWinds Orion uses to identify network elements. During discovery, SolarWinds Orion scans the network for application servers and applications that you can add to the SolarWinds Orion database for monitoring.

SolarWinds SAM can monitor an application, or you can configure SAM to monitor a custom collection of application components, process monitors, and performance counters. Depending on your needs, SAM can assess the status of every aspect of your application, and the health of the application as a whole.

SAM also monitors Amazon Web Services (AWS) cloud instances and Microsoft Azure VMs. With access to your cloud services account, SAM can poll cloud service APIs for cloud metrics and status. This data aggregates and displays through the Orion Web Console to monitor, manage, and troubleshoot issues in your cloud environment. See Manage your cloud infrastructure for details.

SolarWinds recommends adding a limited number of applications and servers to begin monitoring and gauging performance, including Microsoft Exchange, IIS, SQL, Linux, and Unix. After monitoring, alerts, and reports are set up, continue adding more applications and servers to expand your infrastructure monitoring.
Discovery checklist

When you run the Discovery Wizard, you will be asked to provide IP addresses and credentials for the devices you want to monitor. SolarWinds recommends that you gather this information before running the Discovery Wizard.

- Determine the devices to monitor.
- Determine the protocol used to monitor your devices: SNMP or WMI. See Monitoring overview for details.
- Gather IP ranges or individual IP addresses you want the system to scan as it discovers your network.
- Collect SNMP v1/2c community strings and SNMP v3 community strings and credentials of the devices you want to monitor.
- Obtain login credentials for each monitored device, including
  - VMware host credentials. The system requires read-only permissions.
  - Windows credentials: domain or local admin.
- For AWS cloud monitoring, add an AWS IAM user account (up to 10) and Account Access Key ID and Secret Access Key for access. The account should include the following permissions:
  - ec2:DescribeInstances
  - ec2:DescribeAddresses
  - ec2:DescribeVolumes
  - ec2:DescribeVolumeStatus
  - cloudwatch:GetMetricStatistics
  - autoscaling:DescribeAutoScalingInstances
  For additional management actions, add the following permissions to the AWS IAM user account:
  - ec2:StartInstances
  - ec2:StopInstances
  - ec2:RebootInstances
  - ec2:TerminateInstances
  To set up permissions and AWS cloud accounts, see Learn more about Amazon EC2 credentials for cloud monitoring.
- For Microsoft Azure cloud monitoring, configure Azure to interact with the Orion Platform before adding an Azure cloud account to the Orion Web Console. Each account requires sufficient Azure Active Directory (AD) and subscription permissions to add an AD app in the Azure Portal so the Orion Platform can retrieve status and metrics for VMs. IAM permissions must also be set up.
  Visit the SolarWinds Success Center and review Configuring Microsoft Azure for cloud monitoring in the Orion Platform for details.
Monitoring overview

You can configure an application or template to collect data through a preferred polling method as agent or agentless.

Monitoring with Orion agents

An agent is software that provides a communication channel between the Orion server and a Windows or Linux computer. Products install plugins on agents to collect the data that the agents send back. Orion agents are available for Windows and Linux. For requirements and information, see Monitoring with Orion agents in SAM.

Monitoring with SNMP

To monitor devices using SNMP, you must enable SNMP on those devices because it is not enabled by default. SNMP is primarily used to monitor network devices, for example, routers, firewalls, and switches. To enable SNMP, consult the device vendor documentation.

When configuring SNMP-enabled network devices for monitoring, note these details:

- Steps to enable SNMP communications differ by device; consult the documentation provided by your device vendor.
- For correct device identification, monitored devices must allow access to the SysObjectID.
- Unix-based devices should use the version of Net-SNMP (5.5 or later) that is specific to the Unix-based operating system in use.
- If SNMPv2c is enabled on a device, NMPv2c is used to poll the device for performance details by default. To poll with SNMPv1, disable SNMPv2c on the device to be polled.
- SolarWinds SAM can monitor VMware ESX and ESXi Servers versions 4.0 and later.
- Linux/Unix servers are generally monitored with SNMP and SSH Script Monitors that require user credentials.

VMware Tools is not required on virtual machines (VMs) running on monitored ESXi and ESX servers, but additional details such as IP addresses are made available if VMware Tools is installed on VMs hosted by monitored ESXi and ESX Servers.

Monitoring with WMI

If monitoring Windows servers, use Windows Management Instrumentation (WMI), which is usually enabled on Windows devices by default. Capable of gathering more data than SNMP, WMI is the preferred polling method because some SolarWinds SAM features are not available if you use SNMP.

Agentless monitoring using WMI is not recommended when the poller and the device are separated by a firewall. To overcome this limitation, SolarWinds provides an optional agent that allows you to securely monitor Windows servers and applications by WMI. If you want to use SNMP for Windows, then you must install and configure an SNMP agent.
Deciding between SNPM and WMI

SNMP is typically used to monitor servers and network devices without agents. For Windows servers, WMI usually provides better metrics than can be obtained through SNMP monitoring alone. For many Windows-based servers and applications, agentless monitoring via the WMI gateway provides strong monitoring capabilities.

The availability of some features depends on which Orion Platform modules are in your environment, as well as which product versions you're using. For example, NPM supports polling via WMI, SNMP, and agents. However, interface polling via WMI and Agent is not supported unless you have a SAM license. You must use SNMP as a polling method to obtain interface data in an NPM-only installation. For details, see Polling methods used by Orion.

The following table describes the pros and cons of monitoring with SNMP vs. WMI:

<table>
<thead>
<tr>
<th></th>
<th>SNMP</th>
<th>WMI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth, CPU, memory usage on the host/poller</td>
<td>✔</td>
<td>⚠️ Uses more bandwidth, CPU, and memory than SNMP per poll.</td>
</tr>
<tr>
<td>Monitoring across firewall/NAT-ed WAN connection</td>
<td>✔</td>
<td>⚠️ Requires an agent for secure monitoring over one port.</td>
</tr>
<tr>
<td>Windows mount points and application metrics</td>
<td>✖ Cannot collect Windows mount point statistics or application level metrics.</td>
<td>✔</td>
</tr>
</tbody>
</table>

To learn more, see the following the SolarWinds Success Center articles:

- Feature availability based on monitoring methods
- How do I choose a polling method to use in SAM?
- WMI vs. SNMP polling
Discover your servers and applications

Check out this video about discovering your servers and applications.

*Discovery* is a term that describes the process SolarWinds Orion uses to identify application servers and applications. Before you begin:

- Ensure that you determine what to monitor.
- Enable Windows devices for WMI.
- Enable the networking devices you want to monitor for SNMP.

The first time you run the Discovery Wizard, SolarWinds recommends adding a limited number of application servers, including Exchange, IIS, SQL, Linux, and Unix. The examples in this guide focus on monitoring IIS and the operating system of your application server, but the same steps are applicable to monitoring any application.

After discovery, if the status of a node is Unknown, you may need to check settings in SolarWinds SAM. See Troubleshoot Unknown Nodes for details.

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Ranges</td>
<td>Use this option when you want Orion to scan one or more IP ranges.</td>
</tr>
<tr>
<td></td>
<td>If you have many IP ranges to scan, consider adding multiple discovery jobs</td>
</tr>
<tr>
<td></td>
<td>rather than including all ranges in a single job.</td>
</tr>
<tr>
<td>Subnets</td>
<td>Use this option to scan every IP address in a subnet. SolarWinds recommends</td>
</tr>
<tr>
<td></td>
<td>scanning at most a /23 subnet (512 addresses max).</td>
</tr>
<tr>
<td></td>
<td>Scanning a subnet returns everything that responds to ping, so we recommend</td>
</tr>
<tr>
<td></td>
<td>only scanning subnets where the majority of devices are objects you want to</td>
</tr>
<tr>
<td></td>
<td>monitor.</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>Use this option for a limited number of IP addresses that do not fall in a</td>
</tr>
<tr>
<td></td>
<td>range. Since a network discovery job can take a long time to complete, SolarWinds recommends using this option when you are first starting out.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Use this option to scan an Active Directory Domain Controller.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
4. The Agents panel appears. The QoE agent monitors packet-level traffic. If there are any nodes using agents, select the Check all existing nodes.

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 Virtualization panel, to discover VMware vCenter or ESX hosts on your network, enter the credentials, and click Next.

6. On the SNMP panel, to monitor an SNMP-enabled device, enter the credentials, and click Next.

7. 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.
8. 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.


10. Accept the default frequency and run the discovery immediately.

Discovery can take anywhere from 5 minutes to several hours, depending on the number of application servers involved.
Add discovered servers and applications to SolarWinds SAM

After the Network Sonar Wizard discovers your network, the Network Sonar Results Wizard opens, allowing you to import network elements into SolarWinds SAM. Discovered elements do not count against your license count; only elements that you import into the Orion database count against your license.

When you run discovery manually, the system automatically selects all network elements to be monitored. You must clear the check boxes for elements you do not want monitored. This example highlights Windows devices with IIS.

Before you begin, ensure that you Discover your servers and applications.

If discovering your network for the first time, SolarWinds recommends monitoring a small number of critical servers.

1. Make sure that only the device types you want to monitor are selected, and click Next.

2. Ensure the interfaces you want to monitor are selected, and click Next.

SolarWinds recommends that you do not monitor WAN, QoS, multi-port, and virtual NIC interfaces.
1. SolarWinds SAM only discovers interfaces on WMI nodes.

<table>
<thead>
<tr>
<th>List of Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected (Available)</td>
</tr>
<tr>
<td>2 (of 2)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Node Name</th>
<th>Interface Description</th>
<th>Interface Alias</th>
<th>Port Mode</th>
<th>Monitoring type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Area</td>
<td>LAB-APM-</td>
<td>Microsoft Virtual Machine Bus Network</td>
<td>Local Area Connection</td>
<td>WMI</td>
<td></td>
</tr>
<tr>
<td>Connection</td>
<td>DEMO(2)</td>
<td>Adapter</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Area</td>
<td>LAB-APM-</td>
<td>Microsoft Virtual Machine Bus Network</td>
<td>Local Area Connection</td>
<td>WMI</td>
<td></td>
</tr>
<tr>
<td>Connection</td>
<td>DEMO(2)</td>
<td>Adapter</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Ensure the volume types you want to monitor are selected, and click Next.
   SolarWinds recommends that you do not monitor compact disks and removable disks.

<table>
<thead>
<tr>
<th>Network Sonar Results Wizard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume Types to Import</td>
</tr>
</tbody>
</table>

- Count  Volume Type
- 2      RAM
- 2      Virtual Memory
- 2      Floppy Disk
- 2      Fixed Disk
- 4      Compact Disk

3. Select the applications to monitor, and click Next.
   In this example, Microsoft IIS is selected and will be configured for monitoring.
5. Review the list of elements to be imported, and click Import.

6. On the Results tab, click Finish.

7. Click My Dashboards > SAM Summary.

The SAM Summary view widgets may take several minutes to populate with data.
Monitor your environment

This section includes instructions on how to configure monitoring:

- Understand the relationship between applications and templates
- Monitor Internet Information Services (IIS)
- Monitor your operating system
- Configure hardware health monitoring
- Monitor hardware health
- Monitor cloud instances and VMs
- Investigate application performance with Performance Analysis

How SAM works

Using UDP, TCP, SNMP, and WMI calls to your environment and application servers, SAM provides real-time feedback about applications and trends through statistics stored in the Orion database. Thanks to the SolarWinds common components infrastructure, there are no agents installed on your servers and no remote software to maintain. All calls are made in real time and displayed in the Orion Platform accessible from any supported browser.

As a standalone product, SAM operations can be visualized with the following flowchart:
Installed as a module in your family of SolarWinds products, SAM can be visualized with the following flowchart:

![Flowchart of SAM operation]

- SAM requests performance data based on defined monitors and targets respond.
- Orion Server or Additional Poller schedules SAM Poll and Job Requests.
- Orion Module Engine receives the data and requests statistics from the Orion Database.
- Orion Database sends requested data to the Module Engine.
- Module Engine writes statistics to and requests statistics from the Orion Database.
- Returned Statistics are displayed on the Network Engineer viewing Web Console.
- Orion Module Engine processes the data.
- Orion Module Engine sends the data back to Orion Server or Additional Poller.

**Tip:** SAM includes many features that are common to all Orion Platform products, including user accounts, views, alerts, and reports. To learn more, see the Orion Platform Administration Guide.

**Understand the relationship between applications and templates**

In SolarWinds SAM, an application is a collection of component monitors inherited from a template. A component monitor queries for values returned by a process, counter, status, or script. SolarWinds SAM uses the data received to display vital statistics concerning the health of the system.
Templates provide blueprints for the applications to be monitored. You can customize templates, and use only the component monitors you need to monitor a specific environment. SolarWinds SAM provides the following types of templates:

- **AppInsight application templates** are preconfigured templates that provide detailed information. If you have business-critical Exchange, Microsoft IIS, or Microsoft SQL instances, use the AppInsight templates to monitor these applications. These templates have their own mechanism of discovering elements of an application dynamically. They also have special licensing.
- If you have other business-critical applications, apply one of the many preconfigured application templates that ship with SolarWinds SAM. SolarWinds recommends deploying a single template, making necessary edits to customize it to your environment, and then deploying the edited template on all similar applications. You can also obtain a template from the thwack community for an application not shipped with SAM.
- If you have a custom, homegrown application that you need to monitor, you can build a custom template.

The following illustration explains the template and application relationship. If you make a change at the template level, the applications based on that template will be affected. Conversely, if you make a change at the application level, only the individual application will be affected.

This inheritance relationship is beneficial if you need to make a lot of changes. For example, rather than making one change to 100 applications (and therefore 100 changes), you can change one item that will affect all 100 applications based on that template.
Monitor Internet Information Services (IIS)

SolarWinds SAM includes AppInsight Applications that provide a level of detail beyond what other templates can provide, allowing you to monitor virtually every aspect of your application. The AppInsight for IIS application provides:

- Control over web sites and application pools
- Separate, detailed metrics on each website or pool, instead of just a summary level
- Monitoring log space usage on each website individually, ASP.NET requests monitoring
- SSL expiration monitoring

If the system did not scan for AppInsight for IIS during discovery, you can add it to monitored servers running IIS.

This example shows how to apply the AppInsight for IIS application template to a Windows node.

Add AppInsight for IIS to a node

1. In the Orion Web Console, navigate to the Node Details page of any WMI node running IIS.

   ![Management widget](Image)

   You must know which nodes are running IIS.

2. From the Management widget, click List Resources.

3. Select Microsoft IIS to enable AppInsight for IIS data collection, then click Submit.

   List Resources shows all monitorable features of a node.
4. Click the All Applications widget to verify the addition by clicking the Applications.

5. Enter your IIS credentials when prompted, and click Configure Server.

For troubleshooting information, see Troubleshooting ApplInsight for IIS.
View IIS application data

SolarWinds SAM displays IIS data in views. The type of view determines the level of detail. For example, the AppInsight for IIS details view provides a rollup of information about that IIS server, including statistics about all the sites on the server, application pools, and connections.

Navigate to the AppInsight for IIS details view

1. In the Orion Web Console, locate the All Applications widget by clicking My Dashboards > Home.
2. Expand the AppInsight for IIS tree by clicking >.
3. Click an IIS application to view.

From the AppInsight for IIS details view you can view the status and details for Sites, Applications Pools, and Performance Counters by clicking elements in each of these widgets.

Navigate to the website details view

From the AppInsight for IIS details view, click a website in the Sites widget. The Sites widget shows every site hosted by that server.

Navigate to the application pools view

From the AppInsight for IIS details view, click an application pool in the Application Pool widget. The Application Pool widget show the memory and CPU usage of each site on the server.
Navigate to the performance counter details view

From the AppInsight for IIS details view, click a performance counter in any widget. For example, click ASP.NET > Requests Rejected.

![Image of ASP.NET performance counter](image)

Expert knowledge for AppInsight performance counters

General information is provided for a selected counter, in addition to possible problems and troubleshooting steps, where applicable. Find expert knowledge on the performance counter details page.

**Expert Knowledge**

**Description:**
This displays the number of milliseconds that the most recent request was waiting in the queue.

**Information:**
This does not include any time spent waiting in application queues. The threshold for this counter is 1,000.

**Possible problems:**
If this indicator is greater than 1,000 ms, the performance of the IIS server is suffering.

AppInsight for IIS can help you monitor and troubleshoot IIS. However, a software monitoring solution cannot detect failed hardware issues, such as insufficient RAM or a failed cooling fan. To detect hardware issues, you also need to enable hardware health monitoring.

Monitor your operating system

SolarWinds SAM provides a number of out-of-the-box application templates that you can use to monitor business-critical applications. You can assign these templates as-is to nodes, or create copies to modify settings or add and modify component monitors.
SolarWinds recommends deploying a single template, making necessary edits to customize it to your environment, and then deploying the edited template on all similar applications. To find and add additional templates, import templates shared by other users through THWACK. SAM provides import options for THWACK exports and directly from files.

The following example shows how to apply the Windows Server 2016 Services and Counters template to monitor a Windows 2016 OS with the component monitors:

- Service: Distributed Transaction Coordinator
- Service: Security Accounts Manager
- Service: Remote Registry
- Total Available Memory (MB)
- Page File Usage
- Disk Queue Length
- Virtual Memory
- % Processor Time
- Service: Server
- Service: Plug and Play
- Pages per second
- Logical Disk: Average Disk Queue Length
- Physical Disk: Average Disk Queue Length

Before you begin

Ensure you have Remote Procedure Call (RPC) and Windows Management Instrumentation (WMI) access to the target server, plus Windows Administrator credentials for the server.

Windows Performance Counters use RPC for communication which uses TCP port 445. If testing fails after assigning the template to a node, use the WMI protocol.

Apply a template to a node

1. In the Orion Web Console, click Settings > All Settings > SAM Settings.
2. Under Application Monitor Templates, click Manage Templates.
3. Locate the template and click Assign to Node.

4. Select the Windows nodes you want to monitor for the operating system on the left pane, click the green arrow to move it to the right pane, and click Next.
5. Choose the credentials, and click Assign Application Monitors.

6. On the Finish panel, click Done.
   It will take several minutes for the initial poll to complete and widgets to display data.

View the application data

Click My Dashboards > SAM Summary to view the All Applications widget. The All Applications widget is an excellent method for at-a-glance monitoring with hover-over information and icons status to provide a quick overview of data. When software has been ruled out as the problem, check the hardware health.
Configure hardware health monitoring

SolarWinds SAM monitors hardware health information such as fan, power supply, memory, CPU, and so on, on the following types of hardware:

- VMware hosts
- HP ProLiant™
- Dell PowerEdge™
- IBM X-Series™
- HP C7000 and HP C3000 BladeSystems
- Dell M1000e Blade Enclosure

For SolarWinds SAM to monitor hardware health information, the Hardware Monitoring Agent, provided by the software manufacturer, must be installed, configured, and enabled on each system. Once enabled server-side, you must either:

- Run a discovery so that SolarWinds SAM can detect that the Hardware Monitoring Agent has been enabled. SolarWinds recommends this approach if you have multiple nodes where the Hardware Monitoring Agent has been enabled, or if you are not already monitoring those nodes.
- Go to the Node Details page, select List Resources, then check the Hardware Health option.

To configure hardware health monitoring:

1. In the Orion Web Console, click My Dashboards > Home.
2. In the All Nodes resource, click the node you want to monitor.

3. On the Management resource, click List Resources.
4. Select Hardware Health Sensors, and click Submit.

Monitor hardware health

SolarWinds SAM monitors hardware health information such as fan, power supply, memory, CPU, and so on, on the following types of hardware:

- VMware hosts
- HP ProLiant™
- Dell PowerEdge™
- IBM X-Series™
- HP C7000 and HP C3000 BladeSystems
- Dell M1000e Blade Enclosure

For SolarWinds SAM to monitor hardware health:

- The Hardware Monitoring Agent, provided by the software manufacturer, must be installed, configured, and enabled on each system.
- You complete the steps outlined in Configure hardware health monitoring

You may need to log in with an administrator account to perform this action.

1. In the Orion Web Console, click My Dashboards > Home, and then locate the Hardware Health Overview widget.
2. To view a status, click its label.

3. Click the node you want to review.

4. Review the Current Hardware Health widget. Sensors listed as Critical should be investigated.
Monitor cloud instances and VMs

This section provides an overview about monitoring your cloud infrastructure. See the Orion Platform Administrator Guide for more information.

Cloud service platforms provide on-demand computing resources to third-party organizations over the Internet. As organizations migrate systems to the cloud to distribute workloads, deliver applications, and expand resources for growing databases, infrastructure can become difficult to map in sprawling environments, leading to lost resources or hidden instances.

To support hybrid environments, the Orion Platform can retrieve data from the Amazon Web Services (AWS) and Microsoft Azure cloud service platforms to track availability, performance, applications, and more for instances and VMs. Examples of data gathered include status, storage capacity, memory usage, and IP addresses.

After configuring cloud accounts, you can use the Cloud Infrastructure Monitoring feature to:

- Manage hybrid environment metrics and status through a single console so you can compare performance, locate bottlenecks, and better plan capacity and resource allocation.
- Track end user and business context for performance by gathering extended metrics that provide visibility into cloud and on-premises systems.
- Dynamically monitor cloud instances and VMs to better handle resource churn during provisioning. Instances and VMs can be removed as needed to support expanding environments or performance peaks.
- Determine usage trends and troubleshoot issues. Captured metrics over time provide historical references to track trends for resource consumption (such as CPU spikes and lulls) and help determine when those trends become issues.
- Use cloud monitoring data, Orion alerts, and the Performance Analysis dashboard (PerfStack) to review historical performance and pinpoint when significant usage changes began to trigger issues.

For example, add a series of EC2 cloud instances for an AWS account for the east coast. Select My Dashboards > Cloud to review overall AWS infrastructure data and cloud details. Use the Cloud Instances Status Summary and Cloud Server Infrastructure widgets to review status and health at-a-glance. To quickly review cloud status, metrics, and node management details, hover over any cloud instance name in the Orion Web Console.

The tooltip provides quick information for the cloud service and status.
When managed as a node, the tooltip provides enhanced data.

Cloud instances encountering issues display in the following widgets with linked instances and nodes to investigate:

- Active Cloud Alerts lists all active alerts affecting monitoring and managed cloud instances.
- Cloud Applications with Problems lists all applications with issues on cloud instances managed as nodes in SAM.

Select a cloud instance or VM to view its Details page. Exceeded thresholds are highlighted in warning and critical values, charts, and graphs with hover-over points to compare collected data and linked alerts.

The following widgets provide important data to determine issues, as well as track performance and usage trends:

- Active Alerts lists all active alerts affecting the cloud instance.
- Min/Max/Average of Average CPU load displays average CPU load collected and calculated for the cloud instance.
- Min/Max/Average of Network Utilization provides a chart of the minimum, maximum, and average bits per second transmitted and received over a cloud instance for a custom period of time.
Investigate application performance with Performance Analysis

With complex networks consisting of cloud, hybrid IT, virtualization, storage area networks, and so on, multi-faceted IT issues can be difficult to pinpoint and diagnose. When an issue surfaces, for example a badly performing application or server, the investigation can take significant time to locate the core issue. The problem could be in storage, network connectivity, user access, or a mix of resources and configurations.

To investigate the issue, create troubleshooting projects with the Performance Analysis (PerfStack™) dashboard that visually correlate historical and real-time data from multiple SolarWinds products and entity types in a single view.

With Performance Analysis dashboards, you can do the following:

- Compare and analyze multiple metric types in a single view, including status, events, and statistics.
- Compare and analyze metrics for multiple entities in a single view, including, nodes, interfaces, volumes, applications, and more.
- Correlate data from across the Orion Platform on a single, shared time line.
- Visualize hybrid data for on-premises, cloud, and everything in between.
- Share a troubleshooting project with your teams and experts to review historical data for an issue.

For SAM, the possibilities are endless for application analysis and hybrid environments:

- Visually walk through historical data for applications in your environment
- Verify resource allocation issues in hybrid environments for a specific application
- Correlate application data from templates, component monitors, hardware health, and more into a single view
The following example shows you how to identify a root cause for a Windows Server 2012 application performance issue. In this scenario, the application performance has degraded to the point where users encounter slower responses and access. As you review the Windows Server 2003-2012 template dashboard, you find triggered alerts. These alerts notified your application owner, who escalated the issue to system and network administrators.

Rather than digging into the alerts and multiple Node Details pages to troubleshoot the issue, create a new troubleshooting project to investigate the issue.

1. In the Orion Web Console, select My Dashboards > Home > Performance Analysis.
   This opens the Performance Analysis, or PerfStack, dashboard to build charts and graphs using metrics pulled from monitored applications and servers in the Metric Palette. Each chart can hold multiple metrics to directly correlate data.

2. In the New Analysis Project, click Add Entities.
   Entities include all monitored and managed servers, applications, devices, services, and more in the Orion Platform.

3. Select Entities and click Add selected items.
   To get started, you need to locate and add the Windows 2012 application in distress. In the search field, enter Windows to get a list of all monitored nodes, component monitors, and more with Windows in the name or type. Expand and select Types or Status to filter the list.

From the list, we find the application monitor watching Windows Server 2003-2012 Services and Counters. Select and add to the dashboard Metric Palette.
Interested in all associated nodes, applications, servers, and more to this selected node? Click the related entities icon. All related entities display in the Metric Palette providing more options for metrics possibly causing issues.

4. Select the Windows 2012 node to view and select metrics to drag and drop onto the dashboard. You can drag them into the same chart to compare values between metrics.

To start investigating, pull a series of metrics for the IOPS throughput for the server. For this scenario, add the following metrics to investigate latency and connectivity:

- Logical Disk Average: Disk Queuing
- Average IOPS Read
- Maximum IOPS Write
- Maximum IOPS Read
- Average IOPS Write
- IO Latency Write
- IO Latency Read
- IOPS Total
The charts and graphs display with data and alerts for the Last 12 hours of metrics.

5. Add more metrics from the virtual and storage layers to investigate and confirm any bandwidth spikes.

For example, add metrics for the IO latency from the virtual and storage layers to locate issues:

- IO Latency Write
- IO Latency Read
- IOPS Total
- Throughput Total
Analyzing the data, the issue looks to be a noisy neighbor. Basically, another server, service, or application is consuming higher bandwidth, disk I/O, CPU, and other resources causing issues for this specific application.

This information gives your network and system administrators a direction for further investigation and resolving latency issues. To resolve, they can reallocate resources or move the high-consumption application to another location.

6. Click Save and give the project a name.

The project saves as a dashboard with the selected metrics in the set date and time range.

When saved, the URL becomes a sharable link. Copy and share the link to the saved dashboard in tickets or emails sent by the system and network administrators and the product owner. They can access the link to review the gathered data and troubleshoot.

`yourSolarWindsdomain/ui/perfstack/PSTK-50A2738DF0FEF6B74607A68FA812250A67EFH89`

After reallocating resources and making network changes, reopen the dashboard to verify changes and new usage trends for polled metrics.
Explore alerts and reports

This section includes information on working with preconfigured alerts and reports:

- How alerts work
- Manage and use alerts
- How reports work
- Run a preconfigured report
- Create a custom alert
- Create a SAM custom report

How alerts work

An alert is a notification that there is a problem with a monitored element. Orion comes with hundreds of predefined alerts for common problems such as a node or application going down, SSL certificate expiration, website failures, and many other problems.

Many predefined alerts are enabled by default, so if there are problems, you are alerted as soon as you Discover your servers and applications and Add discovered servers and applications to SolarWinds SAM.

SolarWinds recommends that you identify who will receive warning or critical alerts.

- **Alerting on an application**: SolarWinds SAM provides many preconfigured application alerts that notify you if the status of an application has changed (for example: up, down, or unknown) based on whether a component monitor has reached a warning or critical threshold. One alert can notify you about a warning, critical, down, or unknown state for the application.

- **Alerting on a component**: If you create an alert for each component monitor in your application template, you will receive one alert for each component that exceeds a threshold. Alerting on a component monitor can be beneficial if you have custom scripts where you must be notified if the output of the script crosses a specific threshold.
By default, alerts appear in the Active Alerts widget on the Orion Home page.

To see all alerts, you can click the All Active Alerts button in the Active Alerts widget, or you can click Alerts & Activity > Alerts. On this page, you can:

- Acknowledge an alert that you are working on
- Click on any alert to go to the Alert Details page for more information
- Click Manage Alerts to enable/disable, add or edit any alert.

You can create your own alerts, either by duplicating and editing a predefined alert, or by creating a custom alert. Alerting is very powerful and can be complex, with multiple trigger conditions, reset conditions, and actions.
Manage and use alerts

SAM includes out-of-the-box alerts with preconfigured triggers, actions, and settings to automatically start monitoring and triggering against events. These alerts provide immediate notifications through the Orion Web Console as SAM monitors applications, servers, and other nodes.

These alerts allow you to configure additional options for actions including sending an email with event and alert information and resetting manually or automatically according to specific settings. You can also create copies of preconfigured alerts to customize and add triggers, conditions, actions, and more.

List preconfigured, enabled alerts

SolarWinds SAM ships with 21 preconfigured, enabled alerts, and a number of disabled alerts that you can enable and make operational as needed.

To see the list of preconfigured, enabled alerts:

1. Click Alerts & Activity > Alerts
2. Click Manage Alerts.
3. In the Group by field, select Enabled.
4. In the Type field, sort by Out-of-the-box.
5. Review the list of preconfigured, enabled alerts.

Enable and disable alerts

To enable or disable alerts, on the Manage Alerts page, click On or Off in the Enabled column.

Action types

You can configure an alert to trigger one or more actions, such as:

- Send an email
- Send a page
- Manage a virtual machine (for example, power on/off)
- Log the alert to send a file

A complete list of alert actions is available on the Add Action dialog box that you see when you configure an alert.
Configure the default email action

A common alert action is to send an email. To send an email, Orion requires a designated SMTP server that you configure.

1. Click Settings > All Settings, and in the Alerts & Reports section, click Configure Default Send Email Action.

2. In the Default Recipients section, enter recipient email addresses, separated by a semicolon.

3. Under the Default Sender Details heading, provide the default Name of Sender and the default Reply Address.

4. Under the Default SMTP Server section:
   a. Provide the Host name or IP Address of the SMTP Server and the designated SMTP Port Number.
      For example, 192.168.10.124, port 25.
   b. If you want to use SSL encryption for your alert emails, select Use SSL. Selecting 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 the credentials.

d. Click Use as Default.

Manage active alerts

When an alert triggers, any associated alert actions also trigger, and the alert appears on the All Active Alerts page and in the SAM Summary Page. Through the Orion Web Console, you can view the details of alert, the monitored element that triggered the alert, and take action.

1. To view the alert details, click the alert.

The Active Alert Details page appears.
2. To view the details of the network object that triggered the alert, click an object.

The details page of the selected object appears.
3. To acknowledge an alert:
   a. Click Acknowledge.

   ![Acknowledged by]
   ![Acknowledged time]
   ![Acknowledge][Not yet...]
   ![Acknowledge][Not yet...]

   b. Enter a note and click Acknowledge.

   When acknowledged, the alert will not trigger again.
Create a custom alert

Alerts give you the ability to trigger actions and notifications according to monitored events and metrics. In this example, an alert is configured to trigger and send an email to an IIS Administrator when an IIS application goes into a warning or critical state.

1. In the Orion Web Console, click Settings > All Settings > Manage Alerts.
2. Select an alert, and click Duplicate & Edit.

3. On the Properties panel, enter a name and any other properties, and click Next.
   In this example, a group of IIS administrators is identified as the responsible team.

4. On the Trigger Conditions panel, select an object to alert on, and then complete the trigger condition fields.
   In this example, the first trigger condition tests for node status (Down), the second and third conditions test for application thresholds, and the fourth condition specifies the applications to alert on (indicated by 5 Objects).
5. On the Trigger Actions panel, click Add Action.
6. Select send an Email/Page, and click Configure Action.
7. Modify the alert to email the IIS administrators.

   This is an example of creating a custom alert, as opposed to using a predefined default alert that comes with SolarWinds SAM. You can define additional alerts that can be customized to email specific users or email groups.

   8. You can optionally add and configure an action to log the event to the NetPerfMon event log.

   9. Enter the required information for each action, click Next, then continue through the wizard.

   10. Edit the Reset Actions to send an email to the default recipients, then click Next.

    11. Continue through the wizard, review the Summary, then click Submit.

        The Manage Alerts page indicates the alert was created successfully.

   **How reports work**

   Reports provide a bridge between detailed views (which provide point-in-time information) and alerts (which tell you there is a problem). Reports can contain detailed, current state information, or they can contain historical data.
You can run an ad-hoc report, or schedule reports to be sent to you automatically, as a PDF, a web page, or email. For example, use a schedule when you want to receive the Asset Inventory report every Monday morning.

SolarWinds recommends that you identify who needs to receive performance or status reports, and how often they should receive them.

Reports populate when:

- You [Discover your servers and applications](#) and [Add discovered servers and applications to SolarWinds SAM](#).
- There is enough data to include in the report. Depending on the polling interval and data type, some reports do not populate immediately. For example, it takes two weeks for baseline reports to populate.

SolarWinds provides predefined reports for each Orion module. Click Reports > All Reports to see the available predefined reports.

### All Reports

<table>
<thead>
<tr>
<th>GROUP BY:</th>
<th>VIEW REPORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Origin</td>
<td><img src="#" alt="Report Title" /></td>
</tr>
<tr>
<td>All (157)</td>
<td><img src="#" alt="90/95/99th Percentile Traffic Rate - Last 7 Days" /></td>
</tr>
<tr>
<td>Web-based (62)</td>
<td><img src="#" alt="90/95/99th Percentile Traffic Rate - Last Month" /></td>
</tr>
<tr>
<td>Report Writer (95)</td>
<td><img src="#" alt="90/95/99th Percentile Traffic Rate - This Month" /></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Agent Inventory" /></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Agent Plugin Version" /></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="All Active Alerts" /></td>
</tr>
</tbody>
</table>
On the All Reports page, click a report to view it.

You can create your own custom reports by either editing an existing report or creating a report from scratch. Reports can combine any number or type of Orion widgets, including charts, tables, and gauges. You can customize the size of the report, the layout, and add a logo and a footer.

Run a preconfigured report

This example shows how to run and schedule the Asset Inventory preconfigured report. The Asset Inventory dashboard allows you to maintain a current and detailed inventory of your environment's hardware and software. Automatic inventory data collection benefits those interested in tracking asset depreciation, gathering information for insurance purposes, or managing and maintaining your infrastructure.

Enable Asset Inventory data collection

You must enable Asset Inventory data collection before you generate the Hardware Asset Inventory report.

1. In the Orion Web Console, click Settings > Manage Node.
2. Click Add Node.
3. On the Choose Resource panel, click Asset Inventory.

Generate the report

The following example illustrates how to generate an asset inventory report.

1. In the Orion Web Console, click Reports > All Reports.
2. Locate the report, and click the report title.

The system generates the report.
Schedule a report

1. In the Orion Web Console, click Reports > All Reports.
2. Click Manage Reports.

   ![Schedule Report Options]

4. Configure the properties, frequency, and actions as needed in the wizard.
5. When completed, review the summary, and click Create Schedule.

Create a SAM custom report

You can combine any Orion Web Console widget or chart into a report. In this example, a custom report for IIS servers is created by modifying a predefined report, then adding a few more widgets for a complete picture of your IIS servers. To create this custom report, you will first need to create a custom property to identify nodes running IIS.
This report provides information about:

- IIS servers with disks approaching 100%
- Capacity for all disk volumes from the last seven days
- The percentage of disk space used for all disk volumes from the last seven days
- IIS instances with problems
- Availability of IIS Nodes
- Nodes with problems

Create a custom property to identify nodes running IIS

1. In the Orion Web Console, click Settings > All Settings > Manage Custom Properties.
2. Click Add Custom Properties.
3. On the Select Object panel, select Nodes, and click Next.
4. On the Choose Properties panel, in the Property Name field, enter Type.
5. In the Format field, select Text.
6. Select Restrict values, and in the Value 1 field, enter IIS.

You can enter more values to identify other server types. This example uses just the IIS server type.
7. For Usage, select everything except Asset Inventory, and click Next.

8. On the Assign Values panel, click Select Nodes.

9. Select the nodes to which you want to assign the property, and click Add.

10. In the list of Selected Nodes, click Select All, then click Select Nodes.
11. Select IIS from the drop down menu, and click Submit.

![Image of Select IIS from drop down menu]

Create the IIS application server issue rollup report

1. In the Orion Web Console, click Reports > All Reports > Manage Reports, and locate Disks Approaching 100% Capacity - This Month.

![Image of Disks Approaching 100% Capacity - This Month]

2. Select the report, and click Duplicate & Edit.

3. Enter the report name, for example, IIS Application Server Issue Rollup.

4. For the widget in the first default row, click Edit Chart, rename the chart to IIS Servers with Disks Approaching 100% Capacity, and click Submit.

5. In the From field, select Last 7 Days.

6. Click Edit.

![Image of IIS Servers with Disks Approaching 100% Capacity chart]

---

page 64
7. Click the plus sign (+), and click Add Simple Condition.

8. Click Select Field, and then locate and select Node > Nodes Custom Properties > Type.

9. Click Add Column.
10. Select IIS from the drop-down menu, ensuring the query reads **Type** is equal to IIS.

![Query screenshot with IIS selected](image1)

11. Add another simple condition, and locate and select Percent Used under Volume Current Statistics.

12. Click Add Column.

![Add Column screenshot](image2)

13. Select the is greater than operator and enter 70.

The query should read: **Percent used is greater than 70.**
14. Click Add to Layout.

![Basic Selector and Advanced Selector](image)

15. For the widget in the second default row, in the From field, select Last 7 Days.

![Percent Disk Used (Custom Table)](image)

16. Click Add Content.

17. In the Group By field, select Classic category.


19. Click Select and Continue.
20. On the Layout Builder panel, click Edit Resource, and in the Title field, enter IIS Instance with Problems.

21. Add the following SWQL filter: Application.Name='Microsoft IIS'

22. Click Submit.

23. Click Add Content > Classic Category > Summary Reports > Availability of Each Node.

24. Click Select and Continue.

25. Click Edit Resource, and in the Select a Time Period field, select Last 7 Days.

26. In the Filter Nodes (SQL) field, enter: type='IIS'.

27. Click Submit.
When complete, your report should look similar to the following:

![IIS Application Server Issue Rollup](image)
Work with templates

This section guides you in creating and sharing templates:

- Create a template for an application
- Share application monitor templates on THWACK

Create a template for an application

SolarWinds SAM provides pre-built templates that allow you to monitor over 200 applications. You can use the pre-built templates as is, you can modify them, or you can create a template.

Creating a template allows you to monitor uncommon components or applications that are not included in the pre-built application templates provided with SolarWinds SAM.

You have two options for creating templates:

- Create a new template and add component monitors as needed
- Create a copy of an existing template

The following example shows how to create and assign a template that contains the file size component monitor. You can add as many component monitors to a template as you need.

Create a template to monitor file size

1. In the Orion Web Console, click Settings > All Settings.
2. In the Product specific settings group, click SAM Settings.
3. Click Create a New Template, and enter a name.
4. Click Add Component Monitors > Manually add Component Monitors.
5. Select the File Size Monitor component, and click Add.

![1 COMPONENT SELECTED](image)

6. Enter the path and the file to monitor.

![File Path](image)

7. Enter warning and critical threshold values, and click Submit.

![Statistic Threshold](image)

Apply the template to a node

1. In the Orion Web Console, click Settings > All Settings.
2. In the Product specific settings group, click SAM Settings.
3. Click Manage Templates, select the template, and click Assign to Node.

4. Select the node from the left pane, click the green arrow to move it to the right pane, and click Next.

5. Choose the credentials, click Assign Application Monitor, and click Done.

Import and export templates in SAM

SAM integrates with the SolarWinds online IT community site, THWACK, so SAM customers can share templates. You can export custom templates created for applications and custom scripts to THWACK to help other customers. Exporting templates creates an XML file with an .apm-template extension and adds the template to a repository accessed by SAM.

SAM automatically connects with THWACK to list all available templates for import. You need a THWACK account to download and install templates into SAM.
Export a template

> Templates can take about 5 minutes to export to THWACK. If exporting multiple templates, allow time for SAM to complete the export.

1. In the Orion Web Console, click Settings > All Settings > SAM Settings, and click Manage Templates.
2. Browse or select for a template in the list.
3. Click Import Export > Export to THWACK.

4. Enter your THWACK account credentials when prompted.
   If you need an account, click Create Account and follow the steps.

A message displays with the template exporting to THWACK. The template packages into an XML file with an extension .apm-template.
Import a template

1. In the Orion Web Console, click Settings > All Settings > SAM Settings, and click Manage Templates.
2. Click the Shared Templates on THWACK tab.
3. Search or browse the templates. Select a template file and click Import.
   To view details about a template, click the link for the content exchange area on THWACK.

4. Enter your THWACK account credentials when prompted.
   If you need an account, click Create Account and follow the steps.

5. The template imports into the Orion Web Console. In the dialog box, click View Imported Templates.
A list displays of all imported templates.

- If you import a template with the same name as an existing template, the name of the imported template is modified by appending \( n \) to the name, where \( n \) is an integer.

## Share application monitor templates on THWACK

If you create a template that you think might be useful to other SolarWinds users, you can share it via our online IT community, THWACK.

Want THWACK points? Uploading a template to THWACK awards 50 points with an additional five points awarded every time you download a template.

You need a THWACK account to export and import templates into SAM. To share a template, create a user account at THWACK.solarwinds.com.

Check your organization’s policy about sharing company information publicly before posting to THWACK.

## Export a template

You can export custom templates you create for applications and custom scripts THWACK to help other customers. Exporting templates creates an XML file with an .apm-template extension and adds the template to a repository accessed by SAM.

Templates can take about 5 minutes to export to THWACK. If exporting multiple templates, give SAM time to complete the export.

1. Click Settings > All Settings > SAM Settings, and click Manage Templates.
2. Browse or select for a template in the list.
3. Click Import Export > Export to THWACK.
4. Enter your THWACK account credentials when prompted.

   SAM exports the template to THWACK as an XML file with an .apm extension.

## Import a template

SAM automatically connects with THWACK to list all available templates for import. Browse and review the descriptions of available templates to find exactly the ones you need for your monitored applications.
1. Click Settings > All Settings > SAM Settings, and click Manage Templates.

2. Click the Shared Templates on THWACK tab.
   
   A page opens and populates with templates posted in THWACK.

3. Search or browse the templates. Select a template file and click Import.
   
   To view any details provided by the author, click the link for content exchange area on THWACK.

4. Enter your THWACK account credentials and click Log In.

5. After the template is uploaded, click View Imported Templates.

   If you import a template with the same name as an existing template, the name of the imported template is modified by appending (n) to the name, where n is an integer.
Set thresholds

This section provides guidelines for editing thresholds:

- How thresholds work
- Edit a global threshold
- Edit a local node threshold
- Edit a local component monitor threshold
- Edit an application template threshold

How thresholds work

Alerts are triggered when a monitored value exceeds a threshold. Orion comes with predefined static thresholds for most statistics, but you can override these thresholds and customize them on a per-object basis.

Orion provides two threshold levels: critical and warning. A value that crosses a warning threshold appears yellow, and a critical threshold appears red.

If you want to change the predefined value for a threshold, you can add a static threshold or let the system calculate a dynamic baseline threshold.

- **Static threshold.** a constant value that you set for your threshold. For example, the warning threshold for response time might be 500 ms, and the critical value might be 1000 ms. You should be familiar with the performance of that object to know what a reasonable value for a static threshold is.

- **Dynamic baseline threshold.** data for a statistic are collected for a week, and then used to calculate mean and standard deviation. The warning and critical threshold values are defined as 2 and 3 standard deviations above the mean, respectively. For example, if the mean value for packet loss for a specific node is 0%, the warning threshold for packet loss would be 3% (+2 standard deviations) and the critical threshold would be 4% (+3 standard deviations). Dynamic baseline thresholds are the most accurate way to define thresholds for a specific device.

Baselines are calculated once, after data has been collected for a week. You can recalculate baselines on demand.

Edit a global threshold

Alerts are triggered when a monitored value exceeds a threshold. Orion comes with predefined static thresholds for most statistics, but you can override these thresholds and customize them on a per-object basis.

The following statistics have built-in global thresholds, which is a threshold that applies to every monitored node in Orion:
- Average CPU load
- Disk Usage
- Percent memory Used
- Percent Packet Loss
- Response Time

To edit a global threshold:

1. In the Orion Web Console, click Settings > All Settings.
2. In the Thresholds & Polling group, click Orion Thresholds.

![Orion General Thresholds](image)

**Edit a local node threshold**

Alerts are triggered when a monitored value exceeds a threshold. Orion comes with predefined static thresholds for most statistics, but you can you can override global thresholds on a per-node basis. For example, one node might have a lower response time requirement than another, so you can set the threshold values accordingly.

The following example shows how to modify the Memory Usage threshold.

2. In the Alerting Threshold section, click the Override Orion General Thresholds check box.
3. Change the threshold values:
   a. If you are entering a static threshold, type the Warning and/or Critical values.
   b. If you are using a dynamic threshold, click Use Latest Baseline Thresholds.

   ![Memory Usage Thresholds](image)

   c. To understand the baselines calculated, click Latest Baseline Details.
   d. Click Apply thresholds.

   ![Latest Baseline Details](image)

You can edit multiple thresholds simultaneously by opening to the Manage Nodes page, multi-selecting the nodes you want, clicking Edit, and changing the thresholds.
Edit a local component monitor threshold

Alerts are triggered when a monitored value exceeds a threshold. Each component monitor has its own predefined thresholds that are inherited from the template that was used to create it. You can override these thresholds on each individual component monitor, and use either static thresholds or dynamic baseline thresholds instead.

1. Go to the Application Details widget, and click Edit Application Monitor.
2. Expand the component monitor whose threshold you want to change.
3. Click the Override Template button.
4. Change the threshold values:
   a. If you are entering a static threshold, enter the Warning and/or Critical values.
   b. If you are using a dynamic threshold, click Use Latest Baseline Thresholds.
c. To understand the baselines calculated, click Latest Baseline Details.

d. Click Apply thresholds.

![Latest Baseline Details (Statistic Data)](image)

A value of 24.92
Work Days: 215.00 x
Evenings and Weekends: 254.00 x
All hours: 469.00 x

### Latest Baseline Statistics (Statistic Data)

<table>
<thead>
<tr>
<th>TIME PERIOD</th>
<th>MIN</th>
<th>MAX</th>
<th>STD DEV (σ)</th>
<th>-3σ</th>
<th>-2σ</th>
<th>-1σ</th>
<th>MEAN</th>
<th>1σ</th>
<th>2σ</th>
<th>3σ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Days</td>
<td>20</td>
<td>26</td>
<td>1</td>
<td>23</td>
<td>24</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>26</td>
<td>27</td>
</tr>
<tr>
<td>Evenings</td>
<td>22</td>
<td>24</td>
<td>1</td>
<td>23</td>
<td>24</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>26</td>
<td>27</td>
</tr>
<tr>
<td>All hours</td>
<td>20</td>
<td>26</td>
<td>1</td>
<td>23</td>
<td>24</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>26</td>
<td>27</td>
</tr>
</tbody>
</table>

You can edit multiple thresholds simultaneously by multi-selecting component monitors, clicking Multi Edit, and changing the thresholds.
Edit an application template threshold

Alerts are triggered when a monitored value exceeds a threshold. Each component monitor has its own predefined thresholds that are inherited from the template that was used to create it. You can override these thresholds on each individual component monitor, or you can edit the thresholds on the application template. Changes you make to a template threshold propagate to all component monitors that the template is applied to.

1. In the Orion Web Console, click Settings > All Settings.
2. In the Product Specific Settings group, click SAM Settings.
3. In the Application Monitor Templates group, click Manage Templates.
4. Select a template, and click Edit.
5. Expand the component monitor that you want to change.
6. Change the threshold values:
   a. If you are entering a static threshold, type the Warning and/or Critical values.
      
      ![Physical Memory Threshold](image)

      You can edit multiple thresholds simultaneously by multi-selecting the component monitors, clicking Edit, and then changing the thresholds.
Understand agents

This section includes information on deploying agents:

- **How agents work**
- **Agent resource consumption**

To use custom properties to suppress alerts from being triggered when an object goes down, you can set up a [Do Not Alert alert](#).

### How agents work

An agent is a software application that provides a communication channel between the Orion server and a monitored computer. Agents are used as an alternative to WMI or SNMP to provide information about selected devices and applications. These agents provide the following advantages:

- Polling hosts and applications behind firewall NAT or proxies.
- Polling node 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 are established.
- Full, end-to-end encryption between the monitored host and the main poller.

After deployment, all communication between the Orion server and the agent occur over a fixed port, using 2048-bit TLS encryption. The agent protocol supports NAT traversal and passing through proxy servers that require authentication.

If an agent is used, all SAM application data is collected by the agent. You can override this behavior at both the application and template level to use another polling method. For example, if you assign an application template that uses a User Experience Monitor and you do not want to measure response time locally from the server where the application is installed, you can switch the application to poll without using an agent.
Agent Communication can be deployed as either Agent Initiated or Orion Server initiated:

- **Agent initiated communication**: The agent initiates communication with the server on the default port of 17778. This port must be opened on the server firewall so the agent can connect. No change to the agent firewall is required.

- **Orion Server initiated communication**: The agent waits for requests from the server on the default port of 17790. This port must be opened on the firewall of the agent computer so the server can connect. No change to the server firewall is required.

The following reports are configure for use with Orion agents:

- Agent Inventory
- Agent Plugin Version

**Tip**: Use Orion Server-initiated communication in DMZ environments or cloud scenarios such as Azure. Use agent-initiated communication with a proxy to poll multiple computers within a single Azure cloud service.

---

**Agent communication modes**

Communication modes determine how the agent and the Orion server communicate. This is frequently influenced by where the device you want to monitor is on your network.

**Server-initiated communication**

This communication method is also known as a passive agent.
Any communication between your Orion server or additional polling engines and the agent is initiated by the Orion server itself. To allow communication from the Orion server, the firewall service running on the monitored device or the network firewall must allow incoming connections through port 17790. If the agent is configured to use another port, update the firewall rules to allow incoming connections from the other port.

Agent-initiated communication

This communication method is also known as an active agent. In active mode, there are no listening ports on the agent.

Any communication between your Orion server or additional polling engines and the agent service is initiated by the agent service itself. Update your firewall rules to allow outgoing connections through port 17778 to enable communication between the agent and the Orion server. Open port 17791 if the agent is on Windows 2008 R2.

You cannot use agent-initiated communication through a proxy using NTLM authentication if the agent is running on a Linux/Unix-based device.

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.

Deploy an agent with the Add Node wizard

This is the recommended method to deploy an agent to a node. The Orion server deploys the agent software to the target node, installs the software using the credential you select, and adds the node to the Orion server as a monitored node. After the agent is installed, it operates under a local account.
The Orion server must be able to communicate with the remote node. To monitor Linux-based devices, TCP port 22 (outbound) must be open on the Orion server or additional polling engine and open (inbound) on the device you want to monitor.

1. Click Settings > All Settings in the menu bar.
2. Under Node & Group Management, click Manage Nodes.
3. Click Add Node.
4. In the Polling hostname or IP address field, enter the IP address or fully qualified domain name (FQDN) of the device you want to manage.
5. Select Windows & Linux Servers: Agent as the Polling Method.
6. Select the operating system type of the remote computer.
7. Choose a credential from the list, or enter new credentials, and then click Next.
   - These credentials are only used to connect to the remote computer and install the agent software. After the agent is deployed, the credentials may change with no impact to the deployed agent.
   - The credentials must have administrator or root-level privileges. On Linux-based devices you can connect with one credential set and then use another credential to use `su` or `sudo` for package installation. Most Linux distributions require the user’s password when using `sudo`. Other distributions, such as SUSE, may require the root password. Depending on your Linux distribution, enter the required credential for the Include Credentials with Elevated Privileges to install the package.
   - For Linux-based nodes, you can choose to add SNMP credentials to collect SNMP data for Asset Inventory and Hardware Health from the remote node.
8. Click Start Install on the Install Agent Software window.
9. Choose the resources to monitor on the agent, and click Next.
10. Add application monitors on the agent, and click Next.
11. Change properties or keep the defaults, and click OK, Add Node.

When installation is successful and communication between the agent and the Orion server is successful, the agent is listed on the Manage Agents page.
Agent resource consumption

An agent is a software application that provides a communication channel between the Orion server and a Windows or Linux computer. Agents are used as an alternative to WMI or SNMP to provide information about your selected key devices and applications.

A single polling engine can support up to 1,000 agents. The following table details agent resource consumption.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Consumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>0.24% on average under normal operating condition</td>
</tr>
<tr>
<td>Memory</td>
<td>Between 10 and 100 MB depending upon the number and types of jobs</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>The agent consumes roughly 20% (on average) of the bandwidth consumed by the WMI protocol for transmission of the same information</td>
</tr>
<tr>
<td></td>
<td>For example, Agent: 1.3 KBPS versus WMI at 5.3 KPB</td>
</tr>
<tr>
<td>Storage</td>
<td>100 MB</td>
</tr>
</tbody>
</table>

Agent settings

The Agent Settings page provides access to all of the settings and tools needed to install and manage agents. Additional agent settings can be found in the Control Panel.

In the Orion Web Console, click Settings > All Settings > Agent Settings.

- **Manage Agents**: Opens the Manage Agents page so you can add a new agent, edit, update, or reboot an existing agent.
- **Download Agent Software**: Opens the Agent Downloads page so you can mass deploy or manually install an agent.
- **Define Global Agent Settings**: Opens the Global Agent Settings page so you can allow automatic agent registration or allow automatic agent updates.