Orion Platform

Version 2019.4
© 2019 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

Orion Platform features ........................................................................................................... 11
  Pre-installation hints ............................................................................................................ 11
  Common features .................................................................................................................. 11
How Orion Platform products work ...................................................................................... 14
  SolarWinds Orion Platform requirements ............................................................................ 14
  SolarWinds Orion agent requirements .................................................................................. 26
  Multi-module system guidelines for the Orion Platform ....................................................... 32
License Orion Platform products in the Orion Web Console .................................................. 42
  Evaluate Orion Platform products ....................................................................................... 42
  Activate licenses for Orion Platform products ...................................................................... 44
  Upgrade licenses in the Orion Platform ................................................................................ 46
  Assign licenses for Orion Platform products to a server ..................................................... 46
  Migrate Orion Platform licenses from one server to another ............................................. 47
  Synchronize licenses in the Orion Platform .......................................................................... 49
Discover and add network devices to the Orion Platform ....................................................... 50
  Discover your network for the Orion Platform with the Discovery wizard ......................... 50
  Add nodes to the Orion Platform using Active Directory .................................................... 54
  Credentials for Active Directory discovery in the Orion Platform ..................................... 55
  Automatically add discovered nodes to the Orion Platform ............................................... 56
  Advanced discovery in the Orion Platform .......................................................................... 57
  Add discovered devices to the Orion Platform ..................................................................... 60
  Add a single node for monitoring to the Orion Platform ..................................................... 62
  Choose the polling method to use in the Orion Platform .................................................... 64
  Import nodes to the Orion Platform from a list of IP addresses .......................................... 67
  Manage scheduled discovery results in the Orion Platform ................................................ 68
  Minimize SNMP processing load during discoveries in the Orion Platform using the Discovery Ignore List ........................................................................................................ 68
  Manage devices in the Orion Web Console ......................................................................... 68
Group objects and mirror network dependencies in the Orion Web Console ........................................ 87

**View events, alerts, traps, and syslogs in the Orion Web Console Message Center** ................................ 95

- Filter the displayed logged events in the Web Console ................................................................. 95
- Remove events from the Web Console ............................................................................................. 95

**Monitor hardware health** .................................................................................................................. 97

- Monitored Hardware Sensors ........................................................................................................... 97
- Enable hardware health monitoring .................................................................................................. 97
- Enable, disable, or adjust hardware health sensors ........................................................................... 98
- Edit hardware health thresholds ....................................................................................................... 100
- Change the MIB used for polling hardware health statistics ............................................................ 101
- Change hardware health temperature units ....................................................................................... 101

**Monitor Hardware Health for Nutanix appliances** .......................................................................... 103

- Nutanix Hardware Health monitoring requirements ........................................................................ 104
- Set up Hardware Health monitoring for Nutanix appliances ............................................................ 104
- Manage alerts and reports for Nutanix appliances .......................................................................... 107
- Troubleshoot Nutanix Hardware Health monitoring ....................................................................... 108

**Monitor Cisco UCS devices in the Orion Platform** ........................................................................... 110

- UCS device monitoring requirements .............................................................................................. 110
- Set up monitoring for UCS devices .................................................................................................. 111
- Add nodes for devices connected to UCS controllers to the Orion Platform .................................... 112
- Manage alerts and reports for UCS devices in the Orion Platform .................................................. 113
- Troubleshoot UCS device monitoring in the Orion Platform ............................................................ 114

**Monitor cloud instances and VMs** .................................................................................................. 117

- Cloud monitoring recommendations ................................................................................................. 118
- Cloud monitoring requirements ......................................................................................................... 118
- Cloud metrics vs. OS metrics ............................................................................................................ 119
- Learn more ....................................................................................................................................... 119
- Add the first cloud account to the Orion Platform .......................................................................... 119
- Explore cloud instances and VMs on the Cloud Summary page ...................................................... 123
- Configure cloud accounts for the Orion Platform ............................................................................ 124
Cloud service polling overview ................................................................. 127
Throttling overview ................................................................................. 137
Manage your cloud infrastructure .......................................................... 139

**Monitor container services in the Orion Platform** .................................. 165
- Container lifespans and the Orion Platform ........................................... 166
- Container service monitoring requirements .......................................... 166
- Container service monitoring and licensing ......................................... 166
- Manage container services ................................................................. 167
- Add a container service ..................................................................... 167
- Delete a container service .................................................................. 170
- Supported container environments ...................................................... 171

**Monitor virtual infrastructure** ............................................................ 177
- Prerequisites to monitoring virtual infrastructure ............................... 177
- Create ESX server credentials for SolarWinds Orion products ............. 177
- Enable SNMP on VMware ESXi and ESX servers ............................... 177
- Change VMware credentials in the Orion Web Console ...................... 178
- Add virtual servers for monitoring ...................................................... 178
- Assess the status of the virtual environment ....................................... 179
- View ESX host details ....................................................................... 180

**Monitor Quality of Experience metrics** .............................................. 181
- How SolarWinds Packet Analysis Sensors work ................................. 182
- Limitations to Packet Analysis Sensors .............................................. 182
- Common Packet Analysis Sensor deployment scenarios ..................... 183
- Monitor QoE applications and nodes ................................................. 192
- Advanced sensor configuration .......................................................... 199

**Poll devices with SolarWinds Orion agents** ........................................ 202
- Modify global agent deployment and update settings ...................... 202
- Agent communication modes ............................................................ 203
- Deploy agents to nodes ..................................................................... 204
- View agent connections and status, update agents, or manage agents ... 224
Agent polling method ........................................................................................................................................... 235

View logs and events with the Orion Log Viewer ................................................................................................. 239
  OLV installation scenarios ....................................................................................................................................... 239
  OLV feature comparison ........................................................................................................................................... 240
  Evaluate Log Analyzer .............................................................................................................................................. 241
  OLV licensing model ................................................................................................................................................. 243
  Explore the Orion Log Viewer ............................................................................................................................... 245

Monitor Syslog messages ...................................................................................................................................... 261
  Before you begin ....................................................................................................................................................... 261
  View Syslog messages in the Orion Web Console .................................................................................................... 261
  View syslog messages in the Syslog Viewer ............................................................................................................. 263
  Syslog message priorities ......................................................................................................................................... 269

Monitor SNMP traps .............................................................................................................................................. 271
  Before you begin ....................................................................................................................................................... 271
  View SNMP traps in the Orion Web Console .......................................................................................................... 271
  View current traps in the Trap Viewer ..................................................................................................................... 272
  Search for traps in the Trap Viewer ......................................................................................................................... 272
  Configure the Trap Viewer ..................................................................................................................................... 273
  Configure Trap Viewer filters and alerts ................................................................................................................... 273
  Available trap alert actions ...................................................................................................................................... 274
  What is a Trap Template? ......................................................................................................................................... 276

Alert Integrations in the Orion Platform ................................................................................................................. 277
  Configure the integration ......................................................................................................................................... 277
  Configure the instance ............................................................................................................................................... 277
  Operational states ...................................................................................................................................................... 277
  Configure SolarWinds Service Desk to be integrated to the Orion Platform ......................................................... 278
  Integrate an Orion Platform product with ServiceNow ............................................................................................ 279
  Configure web proxy settings in the Orion Platform ............................................................................................... 286

Troubleshooting environmental issues with Performance Analysis dashboards .................................................... 288
  Compatible SolarWinds products ............................................................................................................................ 288
Create analysis projects ................................................................. 289
Update charts in real-time (Real-Time Polling) .................................. 291
Use Display Transform algorithms to visually transform chart data .......... 292
View the polled data for a plotted metric ........................................... 294
Modify the time range for all charts .................................................. 295
View more information for an entity .................................................. 295
Share analysis projects ................................................................. 295
View your saved analysis projects .................................................... 296
Add saved analysis projects to views as a widget ................................. 296
Delete analysis projects ................................................................. 296
Add a Performance Analysis Project to the menu ............................... 296
Troubleshooting Analysis Projects .................................................. 297

Use alerts to monitor your environment with the Orion Platform 299
Alert preconfiguration tasks in the Orion Platform ................................ 299
Configure the default information in the email action for Orion Platform alerts ........................................ 300
Best practices and tips for alerting in the Orion Platform ....................... 300
Navigate to the Alert Manager in the Orion Platform ............................ 301
Add an SMTP server in the Orion Platform ........................................ 301
Create new alerts to monitor your environment with the Orion Platform ........ 302
Reduce alerting noise in the Orion Platform ....................................... 310
Commonly created alerts in the Orion Platform .................................... 320
View triggered Orion Platform alerts in the Orion Web Console ............ 323
Remove alerts from the Active Alerts list in the Orion Platform ............... 323
Test alert triggers and actions in the Orion Platform ............................ 323
Modify multiple alerts or share alerts in the Orion Platform ................. 324
Build complex conditions in the Orion Platform .................................... 326
Manage alert actions in the Orion Platform ........................................ 329
Alert actions available in the Orion Platform ...................................... 330
Defunct alert variables in the Orion Platform ...................................... 355
Share Orion Platform alerts with other SolarWinds products ............... 355
Manage Orion Web Console user accounts in the Orion Platform ............................................ 356
Default accounts ................................................................................................. 356
Create users in the Orion Platform .................................................................. 356
Change account passwords in the Orion Platform .......................................... 359
Enable Orion Platform users to authenticate through LDAP ......................... 360
Authenticate Orion Platform users with SAML v2 ........................................ 360
Define what users can access and do in the Orion Platform ....................... 367
Restrict user access to network areas by applying limitations in the Orion Platform .......... 370
Set default menu bars and views for users in the Orion Platform .................. 372
Limit users to specific network areas in the Orion Platform ......................... 373
Configure automatic login in the Orion Platform ......................................... 373
Manage Orion Polling Engines in the Orion Platform ..................................... 379
Use additional polling engines to balance polling in the Orion Platform .... 379
Use an Additional Web Server .......................................................................... 382
Calculate node availability in the Orion Platform .......................................... 385
Assign credentials to virtual servers in the Orion Platform ......................... 385
Set the node warning level in the Orion Platform ........................................... 386
Delete polling engines in the Orion Platform ................................................. 386
Administrative functions of the Orion Web Console in the Orion Platform ........ 388
Orion Web Console administration in the Orion Platform ............................ 388
View secure data in the Orion Platform .......................................................... 391
Handle counter rollovers in the Orion Platform .............................................. 391
Configure web proxy settings in the Orion Platform .................................... 392
Maintain the SolarWinds Orion database in the Orion Platform .................. 393
Security enhancements and exceptions for SolarWinds Orion Platform products ........................................................... 396
Update polling settings in the Orion Platform ................................................. 402
Manage the Orion Web Console for your Orion Platform ............................ 410
Log in to the Orion Web Console .................................................................... 410
Customize the Manage Nodes / Entities view in the Orion Platform ............. 410
Thresholds in the Orion Platform ..................................................................... 414
Filter nodes in Orion Platform widgets using SQL queries ................................................................. 422
Custom properties in the Orion Platform .................................................................................................... 423

**Customize the Orion Web Console look, views, settings, charts, and maps in the Orion Platform** ..433
Customize the Orion Web Console look for the Orion Platform ................................................................. 433
Add custom properties to node popovers in the Orion Platform ............................................................. 439
How custom views work in the Orion Platform .......................................................................................... 440
Orion Web Console and chart settings for the Orion Platform ................................................................. 455
Customize charts in the Orion Web Console for the Orion Platform ....................................................... 458

**View monitored objects on Open Street map or on Network Atlas maps in the Orion Platform** ...465
Display the Worldwide Map of Orion nodes in the Orion Platform ........................................................... 465
Network Atlas for the Orion Platform ......................................................................................................... 469
Display Network Atlas maps in the Orion Web Console ........................................................................... 495

**Orion Maps for Orion Platform products** ............................................................................................ 497
Orion Map types ........................................................................................................................................ 497
Auto-generated Orion Maps ........................................................................................................................ 497
Custom Orion Maps ................................................................................................................................... 499
What can you do with Orion Maps? ............................................................................................................ 504
View details for Orion Platform entities on Orion Maps ............................................................................. 505
Work with entities in auto-generated Orion Maps in the Map subview .................................................... 511
Adjust auto-generated Orion Maps in the Orion Platform ....................................................................... 515
Understand connections on Orion Maps in the Orion Platform ............................................................... 516
Create and edit Orion Maps ....................................................................................................................... 521
Add Orion Maps to views as a widget ......................................................................................................... 525
Use Orion Maps in alerts and reports ......................................................................................................... 527

**Manage and view reports in the Orion Platform** ............................................................................... 532
Predefined reports in the Orion Platform ................................................................................................. 532
Modify an existing web-based report for the Orion Platform .................................................................. 532
Create a web-based report in the Orion Platform .................................................................................... 533
Customize a web-based report layout in the Orion Platform ................................................................. 536
Add content to a web-based report in the Orion Platform ........................................................................ 536
Add a custom chart or table to a web-based report in the Orion Platform ........................................ 537
Restrict who can access reports in the Orion Platform ................................................................. 540
Generate reports in the Orion Platform on a schedule ................................................................. 543
Export and import reports in the Orion Platform ......................................................................... 546

Create custom monitors in the Orion Platform ........................................................................... 548
Management Information Base (MIB) in the Orion Platform ...................................................... 549
Monitor custom statistics based on OIDs with Universal Device Pollers in the Orion Platform ...... 549
Manage unique devices on the network with the Orion Platform .................................................. 564

Access remote nodes in the Orion Platform ................................................................................. 574
Use Integrated Remote Desktop in the Orion Platform ................................................................. 574
Access nodes using HTTP, SSH, and Telnet in the Orion Platform ................................................ 574

High Availability in SolarWinds products .................................................................................. 576
How does SolarWinds High Availability work? ............................................................................ 576
How failovers work .......................................................................................................................... 577
When do I use a VIP or a virtual hostname? .................................................................................. 578
Which IP address is used as the source when using a VIP? ............................................................ 579
SolarWinds High Availability requirements .................................................................................. 580
High Availability deployment walk-through .................................................................................. 584
Disable or delete HA pools, force a failover, or update an HA pool for Orion Platform products ...... 594
Orion Platform features

The Orion Platform is the core of the SolarWinds IT Management Portfolio. It provides a stable and scalable architecture that includes data collection, processing, storage, and presentation. The Orion Platform provides common features, such as user accounts and groups, views, dashboards, reporting, alerting, and more that you can use across all Orion Platform products and access from the Orion Web Console.

Pre-installation hints

Before you install your Orion Platform products, review the following details:

Orion Platform requirements

Hardware, software, and port requirements for the Orion Platform server and SolarWinds Orion database.

Licensing

Licensing differs among Orion Platform products. Activate, add, upgrade or assign licenses with the License Manager in the Orion Web Console.

Installation or upgrade

Use the SolarWinds Orion Installer to easily install or upgrade multiple Orion Platform products simultaneously.

While installing your Orion Platform products, you might need to configure SSL for the Orion Web Console, enable FIPS, or review directories to be excluded from antivirus protection.

Common features

The following features are available in Orion Platform products.

Learn Orion Platform basics

Log in to your Orion Platform product in a web browser and meet the Orion Web Console.

Review Events, syslogs, or SNMP traps to know what's going on.

Get alerts about issues in your environment.

Generate reports to present the status of the monitored environment.

Review Performance Analysis dashboards, also known as PerfStack™.

Create, edit, and maintain Orion Web Console user accounts - set user rights, reset passwords, limit access to network segments, and enable authentication with Active Directory.

View monitored objects on Orion Maps in the Orion Web Console.
View other map options in the Orion Web Console - display objects with their location specified in the OpenStreet format in a widget, or create maps the Network Atlas tool and display them in the Orion Web Console.

Add devices for monitoring and manage monitored devices

Specify which devices to monitor and the information you need, then select the way you get this information. See Discover and add devices.

Add single nodes, use Active Directory domain controllers to add nodes, or discover devices on your network automatically.

Available polling methods include ICMP, WMI, SNMP, or agents deployed on Windows, Linux, and UIX devices.

Manage monitored devices - edit properties, set the polling method for monitored devices, toggle monitoring on and off, or mute alerts for nodes.

Customize your Orion Web Console

Customize Orion Web Console - customize dashboards, colors, logo, views, widgets and charts. Learn how to limit what objects users see on views, or specify what you want to see on views for specific device types.

Create custom properties - create custom fields to associate with monitored network objects and display custom information for monitored devices.

Create groups and dependencies - organize how monitored data is presented in the Orion Web Console. Set up dependencies to better represent the relationships between network objects and account for constraints on the network.

Set thresholds - specify thresholds for monitored metrics. Customize general thresholds or use baselines.

Monitor additional metrics and devices

Monitor hardware health - get insight into hardware issues on the network. Monitor hardware health based on hardware sensors, such as fan status, power supply status, or temperature.

Monitor virtual environments - monitor your virtual networks (VMware® ESX and ESXi servers, VMware vCenter®) in the Orion Web Console.

Quality of Experience - use packet analysis sensors to see packet-level traffic information about key devices and applications on your network.
Expand the Orion Platform functionality or scale your deployment

Use SolarWinds High Availability (HA) to provide failover protection for your Orion server and additional polling engines to reduce data loss.

Do you need to scale your deployment? See Scalability Engine Guidelines.

Review the tips for optimizing your deployment.

Balance the load on polling engines by specifying nodes to be polled by individual polling engines.

Manage Additional Polling Engines.

Troubleshoot your SolarWinds Orion database.

Extend monitoring to include non-standard devices using custom pollers.
How Orion Platform products work

Orion Platform products monitor the health and performance of your network through ICMP, SNMP, WMI, API, and Syslog communication and data collection.

A simple centralized Orion Platform deployment includes at least two servers:

- The Main Orion server where you install your Orion Platform products. The primary server includes the Main Polling Engine and the Orion Web Console.
- A separate server to install the SolarWinds Orion database.

The polling engine requests real-time statistics (through the selected polling method, such as SNMP or WMI) from monitored devices in your environment.

Polled data is further processed and stored in the SolarWinds Orion SQL database.

Data is requested from the database and displayed in Orion Web Console.

See Orion Scalability Engine guidelines for information about scaling your Orion Platform product.

SolarWinds Orion Platform requirements

Requirements depend on various variables, such as:

- Orion Platform deployment in the cloud vs on-premise.
- Size of the environment to be monitored. This topic provides requirements for small, medium, large and extra large deployments, based on NPM license levels.
- Orion Platform products to be deployed. This document provides minimum requirements for a single Orion Platform product. If you plan to deploy more SolarWinds products from the Orion Platform family, see Multi-module system guidelines.
• Review your product Administrator Guides and release notes for the exact product requirements beyond these minimums.
• SolarWinds recommends reviewing the Orion Platform 2019.4 Release Notes.

Cloud Deployment

Orion Platform products support the following cloud solutions:

- Amazon Web Service
- Microsoft Azure

Amazon Web Service

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Small SL100, SL250, SL500</th>
<th>Medium SL2000</th>
<th>Large SLX</th>
<th>XL (up to 400,000 elements)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orion server</td>
<td>m4.large</td>
<td>m4.xlarge</td>
<td>m5d.2xlarge</td>
<td>m5.2xlarge</td>
</tr>
<tr>
<td>SolarWinds Orion database using Amazon RDS</td>
<td>db.r4.large</td>
<td>db.r4.xlarge</td>
<td>db.r4.2xlarge</td>
<td>db.r4.8xlarge</td>
</tr>
<tr>
<td>SolarWinds Orion database deployed on an Amazon VM</td>
<td>m4.large</td>
<td>r4.xlarge</td>
<td>r4.2xlarge</td>
<td>r5d.8xlarge Recommended: r5d.16xlarge</td>
</tr>
<tr>
<td>Additional Polling Engines</td>
<td>Only relevant for environments that monitor over 12,000 elements.</td>
<td></td>
<td></td>
<td>m5.xlarge</td>
</tr>
</tbody>
</table>

Microsoft Azure

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Small SL100, SL250, SL500</th>
<th>Medium SL2000</th>
<th>Large SLX</th>
<th>XL (up to 400,000 elements)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orion server</td>
<td>A4_v2</td>
<td>DS12_v2</td>
<td>DS4_v2</td>
<td>DS4_v2</td>
</tr>
<tr>
<td>Requirements</td>
<td>Small SL100, SL250, SL500</td>
<td>Medium SL2000</td>
<td>Large SLX</td>
<td>XL (up to 400,000 elements)</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------</td>
<td>---------------</td>
<td>-----------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>SolarWinds Orion database using Azure SQL DB</td>
<td>All installed products must run on Orion Platform 2019.2 or later. Time zone setting of the Orion Server must be in the same time zone as Azure SQL DB time zone (UTC). When deploying Azure SQL and creating a new user in the Configuration wizard, SA account credentials are required in the Configuration wizard.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DTU Standard Tier S3 or better vCore General Purpose Tier 2 or better</td>
<td>DTU Standard Tier S3 or better vCore General Purpose Tier 2 or better</td>
<td>DTU Standard Tier S4 or better vCore General Purpose Tier 2 or better</td>
<td>DTU Standard Tier S9 (up to 100k elements), S12 (up to 400k elements) or better vCore General Purpose Tier 16 (up to 100k elements), 30 (up to 400k elements) or better</td>
<td></td>
</tr>
<tr>
<td>SolarWinds Orion database using Azure SQL Database managed instance</td>
<td>Gen5 4 vCores</td>
<td>Gen5 8 vCores</td>
<td>Gen5 16 vCores</td>
<td>Gen5 40 vCores</td>
</tr>
<tr>
<td>SolarWinds Orion database deployed in an Azure VM</td>
<td>A4_v2</td>
<td>DS4_v2 Standard</td>
<td>E8s_v3</td>
<td>E32-8s_v3</td>
</tr>
</tbody>
</table>
On-premise

To deploy a single Orion Platform product locally, on a server, review the following recommendations.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Small SL100, SL250, SL500</th>
<th>Medium SL2000</th>
<th>Large SLX</th>
<th>XL (up to 400,000 elements)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimum / Recommended</strong></td>
<td>Quad core processor or better</td>
<td>Quad core processor or better</td>
<td>Quad core processor or better</td>
<td>CPUs with a total combined PassMark score of 7,000 or higher</td>
</tr>
<tr>
<td></td>
<td>6 GB/8 GB RAM</td>
<td>8 GB/16 GB RAM</td>
<td>16 GB/32 GB RAM</td>
<td>16 GB/32 GB RAM</td>
</tr>
<tr>
<td></td>
<td>10 GB/20 GB HD</td>
<td>15 GB/40 GB HD</td>
<td>30 GB/40 GB HD</td>
<td>40 GB/50 GB HD</td>
</tr>
<tr>
<td></td>
<td><strong>More details</strong></td>
<td><strong>More details</strong></td>
<td><strong>More details</strong></td>
<td><strong>Read/Write I/O:</strong></td>
</tr>
<tr>
<td><strong>Orion server hardware</strong></td>
<td>Windows Server 2016</td>
<td>Windows Server 2019</td>
<td></td>
<td><strong>800 IOPS</strong></td>
</tr>
<tr>
<td><strong>Orion server software</strong></td>
<td>Desktop OS's only for evaluations; NOT recommended for production environments</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**More details**
<table>
<thead>
<tr>
<th>Requirements</th>
<th>Small SL100, SL250, SL500</th>
<th>Medium SL2000</th>
<th>Large SLX</th>
<th>XL (up to 400,000 elements)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SolarWinds Orion database server</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>![Notice] The Orion server and the SolarWinds Orion database must use separate servers. If you install on a virtual machine, you must maintain your SQL Server database on a separate, physical drive.</td>
<td>SQL Server Standard or Enterprise 2014 and later</td>
<td>SQL Server Standard or Enterprise 2014 and later</td>
<td>SQL Server Standard or Enterprise 2014 and later</td>
<td>SQL Server Enterprise 2014 and late</td>
</tr>
<tr>
<td></td>
<td>Quad core processor or better</td>
<td>Dual quad core processor or better</td>
<td>Dual quad core processor or better</td>
<td>CPUs with a total combined PassMark score of 32,000 or higher</td>
</tr>
<tr>
<td></td>
<td>8 GB/16 GB RAM</td>
<td>16 GB/64 GB RAM</td>
<td>64 GB/128 GB RAM</td>
<td>256 GB/512 GB RAM</td>
</tr>
<tr>
<td></td>
<td>20 GB/40 GB HD</td>
<td>50 GB/100 GB HD</td>
<td>100/400 GB HD</td>
<td>500 GB/1 TB HD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Read/Write I/O:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>30,000 IOPs / 190,000 IOPS or better</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>recommended</td>
</tr>
<tr>
<td><strong>Additional Polling Engines</strong></td>
<td>Only relevant for environments that monitor over 12,000 elements.</td>
<td></td>
<td></td>
<td>4-core processor or better</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16 GB RAM</td>
</tr>
<tr>
<td><strong>Ports to open</strong></td>
<td>Outbound: 22, 25, 465, 587, 1433, 1434,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inbound: 80, 162, 443, 514, 17778</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bi-directional: 53, 135, 161, 1801, 5671, 1777</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Account privileges</strong></td>
<td>SolarWinds recommends that SolarWinds Orion administrators have local administrator privileges on the Orion server to ensure full functionality of local SolarWinds tools.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SolarWinds Orion user accounts limited to the Orion Web Console do not require local administrator privileges.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
More information on hardware recommendations for the Orion Server

Use the recommended hardware configuration to avoid potential performance issues caused by a heavy load or custom configurations such as increased data retention or more frequent polling intervals.

**RAID recommendations** only apply to **physical environments**. If you have your Orion Platform server installed on a virtual machine, these recommendations do not apply to your environment.

**Processor speed**

Use processors that work at 2.4 GHz or faster.

**CPU**

Do not enable Physical Address Extension (PAE).

**HD**

Two 146 GB 15K (RAID 1/Mirrored Settings) hard drives are recommended with a dedicated drive for the server operating system and SolarWinds installation.

Some common files may need to be installed on the same drive as your server operating system. You may want to move or expand the Windows temporary directories.

More information on software requirements for the Orion Server

⚠️ Do not install Orion Platform products on the same server as SolarWinds Access Rights Manager (ARM).

The following table lists software requirements and recommendations for a SolarWinds installation on both physical and virtual computers.

<table>
<thead>
<tr>
<th>Software Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating system</strong></td>
</tr>
<tr>
<td>- Windows Server 2016</td>
</tr>
<tr>
<td>- Windows Server 2019</td>
</tr>
</tbody>
</table>

Desktop operating systems, such as Windows 10, 64-bit Pro or Enterprise, are supported for evaluation environments only. To make a smooth transition from your evaluation to production deployment, SolarWinds recommends that you avoid installing evaluations on desktop operating systems.

**Support differences between Orion Agents and Orion Platform products**

- You cannot install Orion Platform products on domain controllers.  
  **Exception**: You can install Orion Agents on domain controllers.

- You cannot install Orion Platform products or any scalability engines on Microsoft SharePoint, Microsoft Exchange, or BlackBerry servers.  
  **Exception**: You can install Orion Agents on the same server as a Microsoft SharePoint, Microsoft Exchange or Research in Motion (RIM) BlackBerry server.
### Operating system languages
- English (UK or US)
- German
- Japanese
- Simplified Chinese

<table>
<thead>
<tr>
<th>IP address version</th>
<th>IPv4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IPv6</td>
</tr>
<tr>
<td></td>
<td>Dual stack</td>
</tr>
</tbody>
</table>

- CIDR notation is not supported for IPv6 addresses.

### Web server
If you are **not** using Windows Authentication, make sure the Anonymous Authentication is enabled for the SolarWinds NetPerfMon website. Anonymous Authentication is used with the default forms-based authentication.

- IIS is installed by the SolarWinds installer. You can install this software manually to reduce your installation time.

### .NET Framework
- .NET 4.8

Run the same version of .NET on your primary server and any Additional Polling Engines or Additional Web Servers in the environment.


- If your Orion Platform runs on an operating system that does not support .NET 4.8, consider upgrading your environment to be able to use the new features provided by Orion Platform 2019.4.

### Services
If you are using the Syslog or SNMP Traps feature of the Orion Platform, make sure the following services are running after installation is complete to collect syslog messages and traps:

- SolarWinds Syslog Service
- SolarWinds Trap Service
Web console browser

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

- Firefox
- Chrome

Orion Platform products also support the following browsers:

- Microsoft Internet Explorer 11 with Active scripting
- Microsoft Edge

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

Microsoft Edge

More details on requirements for the Orion Database Server

SQL Server versions

Use Express, Standard, or Enterprise versions of the following:

- SQL Server 2014
- SQL Server 2014 SP1
- SQL Server 2014 SP2
- SQL Server 2014 SP3
- SQL Server 2016
- SQL Server 2016 SP1
- SQL Server 2016 SP2
- SQL Server 2017 (including installations on Linux)

ℹ️ Which SQL Server version to use?

- For XL environments, use only Enterprise versions
- Use Express only for evaluations, very small environments, or EOC.

Recommendations

- Use the Simple database recovery mode to ensure best performance.
- Use 64-bit version of SQL Server.
- You can set the database recovery model to Full Recovery if your Orion Database is hosted on a SQL Cluster or if you use Always On Availability. However, you must back up your database regularly and ensure that volume you store your transaction log has free space that is at least equal to or greater than the size of your Orion database. Your transaction logs will continue to grow indefinitely until a database backup is performed and the transactions committed to the database. We recommend daily database backups when you use the Full Recovery model.
The Orion Platform does not support case-sensitive databases.

The Orion Platform supports CI database on a CS SQL Server.

- English with collation setting SQL_Latin1_General_CP1_CI_AS
- English with collation setting SQL_Latin1_General_CP1_CS_AS
- German with collation setting German_PhoneBook_CI_AS
- Japanese with collation setting Japanese_CI_AS
- Simplified Chinese with collation setting Chinese_PRC_CI_AS

Server roles and permissions

**Required server roles:**

- dbcreator
- public
- securityadmin

**Permissions:**

- You need **read permissions** to the master database.
- You **don't need dbcreator permissions** if you are installing an Orion Platform product with a pre-existing blank database.

Hard drive space

The following recommendations apply to **physical environments only**. If you have your SolarWinds Orion database installed on a virtual machine, these recommendations do not apply to your environment.

- Due to intense I/O requirements, a RAID 1+0 drive is strongly recommended for the SolarWinds database, data, and log files with a dedicated drive for the server operating system and tempdb files.
- Other RAID configurations can negatively affect your SQL Server's performance.
- Mirrored drives for the OS and RAID 1+0 for database data files are recommended.
- Solid state drives (SSD) are recommended for all components.

Some common files may need to be installed on the same drive as your server operating system. You may want to move or expand the Windows or SQL temporary directories.

**Database hardware recommendations for large environments**

For large environments with a physical SQL Server, SolarWinds recommends the following hard drive configuration.

- A hardware RAID Controller with a battery backed-up write back cache
- Disk Subsystem 1 Array 1: 2x 146 GB 15K disks RAID 1 (mirroring) for the OS
- Disc Subsystem 2 Array 2: 2x 146 GB 15K disks RAID 1 (Pagefile + Extra Storage)
- Disk Subsystem 3 Array 3: with 6x 15k 146 GB or 300 GB disks configured in a RAID 1+0 array for your SQL MDF and FILEGROUPS.
- Disk Subsystem 4 Array 4: with 4x 15k 146 GB or 300 GB disks configured in a RAID 1+0 array for your SQL LDF Transaction LOG file
- Disk Subsystem 5 Array 5: with 4x 15k 146 GB or 300 GB disks configured in a RAID 1+0 array for your tempdb data file
- Disk Subsystem 6 Array 6: with 4x 15k 146 GB or 300 GB disks configured in a RAID 0 array for your tempdb log file

Authentication

Either mixed-mode or Windows authentication. If you require SQL authentication, you must enable mixed mode on your SQL server.

Other software

SolarWinds recommends you install the SQL Server Management Studio component on your Orion database server.

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

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

ℹ️ You cannot share the SolarWinds Orion database with Microsoft SharePoint, Microsoft Exchange, and Research in Motion (RIM) BlackBerry servers.

Server port requirements

- Ports 4369, 25672, and 5672 are opened by default on the main server for RabbitMQ messaging. These ports can be blocked by the firewall. When running SolarWinds High Availability, ensure ports 4369 and 25672 are open.
- RPC ports > 1024 (TCP, bidirectional) is used by the Job Engine v2 process to communicate with Windows nodes.
<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Service/Process</th>
<th>Direction</th>
<th>Description</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-defined, default: 22</td>
<td>SSH</td>
<td>SolarWinds Job Engine v2</td>
<td>Outbound</td>
<td>Port for accessing ASA devices through CLI</td>
<td>Device-based</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>TCP</td>
<td>SolarWinds Alerting Service V2</td>
<td>Outbound</td>
<td>SMTP port for non-encrypted messages</td>
<td>n/a</td>
</tr>
<tr>
<td>53</td>
<td>UDP</td>
<td>SolarWinds Job Engine v2</td>
<td>Bi-directional</td>
<td>Resolving DNS queries</td>
<td>n/a</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>IIS</td>
<td>Inbound</td>
<td>Default additional web server port. If you specify any port other than 80, you must include that port in the URL used to access the web console. For example, if you specify an IP address of 192.168.0.3 and port 8080, the URL used to access the web console is <a href="http://192.168.0.3:8080">http://192.168.0.3:8080</a>. Open the port to enable communication from your computers to the Orion Web Console. The port might also be used for Cisco UCS monitoring.</td>
<td>n/a</td>
</tr>
<tr>
<td>135</td>
<td>TCP</td>
<td>Microsoft EPMAP (DCE/RPC Locator service)</td>
<td>Bi-directional</td>
<td>Required for devices polled via WMI. Used to initiate communication with the remotely managed host.</td>
<td></td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>SolarWinds Job Engine v2</td>
<td>Bi-directional</td>
<td>Send and receive SNMP information</td>
<td>SNMP v1 and v2 are unencrypted. SNMP v3 uses AES and 3DES encryption.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SolarWinds Cortex</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>162</td>
<td>UDP</td>
<td>SolarWinds Trap Service</td>
<td>Inbound</td>
<td>Receive trap messages</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SNMP Informs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Service/Process</td>
<td>Direction</td>
<td>Description</td>
<td>Encryption</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>-----------------------------------------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>IIS</td>
<td>Inbound</td>
<td>Default port for https binding.</td>
<td>SSL</td>
</tr>
<tr>
<td>465</td>
<td>TCP</td>
<td>SolarWinds Alerting Service V2</td>
<td>Outbound</td>
<td>SMTP port used to send TLS-enabled email alert actions</td>
<td>SSL</td>
</tr>
<tr>
<td>514</td>
<td>UDP</td>
<td>SolarWinds Syslog Service</td>
<td>Inbound</td>
<td>Receive syslog messages</td>
<td>n/a</td>
</tr>
<tr>
<td>587</td>
<td>TCP</td>
<td>SolarWinds Alerting Service V2</td>
<td>Outbound</td>
<td>SMTP port used to send TLS-enabled email alert actions</td>
<td>TLS</td>
</tr>
<tr>
<td>1433</td>
<td>TCP</td>
<td>SolarWinds Alerting Service V2</td>
<td>Outbound</td>
<td>Communication between the Orion server and the SQL Server.</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SolarWinds Administration Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SolarWinds Information Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SolarWinds Information Service V3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SolarWinds Orion Module Engine</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1434</td>
<td>UDP</td>
<td>SolarWinds Alerting Service V2</td>
<td>Outbound</td>
<td>Communication with the SQL Server Browser Service to determine how to</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SolarWinds Administration Service</td>
<td></td>
<td>communicate with certain non-standard SQL Server installations. Required</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SolarWinds Information Service</td>
<td></td>
<td>only if your SQL Server is configured to use dynamic ports.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SolarWinds Information Service V3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SolarWinds Orion Module Engine</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SQL Server Browse Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1801</td>
<td>TCP</td>
<td>MSMQ</td>
<td>Bidirectional</td>
<td>MSMQ WCF binding</td>
<td>WCF</td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Service/Process</td>
<td>Direction</td>
<td>Description</td>
<td>Encryption</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>-----------------</td>
<td>-----------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>5671</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>Bi-directional</td>
<td>For encrypted RabbitMQ messaging (AMQP/TLS) into the main polling engine from all Orion servers (additional polling engines, HA servers, or additional web servers). Sending messages to RabbitMQ.</td>
<td>TLS 1.2</td>
</tr>
<tr>
<td>17777</td>
<td>TCP</td>
<td>SolarWinds Orion Module Engine</td>
<td>Bi-directional</td>
<td>Communication between services and SolarWinds Orion module traffic. Communication between the Orion Web Console and the polling engines. Communication between the main server and pool members.</td>
<td>RSA handshake, AES 256 communication using WCF TLS 1.2 with Cortex</td>
</tr>
<tr>
<td>17778</td>
<td>HTTPS</td>
<td>SolarWinds Agent</td>
<td>Inbound to the Orion server</td>
<td>Required for access to the SWIS API and agent communication</td>
<td>SSL</td>
</tr>
</tbody>
</table>

**SolarWinds Orion agent requirements**

Agent software is free. Licensing occurs through your product and is usually based on the number of monitored elements.

- Windows agents run as a service.
- Linux/Unix agents run as a service daemon.

Before you deploy agents to a target computer, review the following system requirements.
<table>
<thead>
<tr>
<th>Type</th>
<th>Windows</th>
<th>Linux/Unix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>• Windows Server 2008</td>
<td>• Amazon AMI, 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2</td>
<td>• CentOS 6.x, 32-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 SP1</td>
<td>• CentOS 6.x, 7.x, 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012</td>
<td>• IBM AIX 7.x</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2</td>
<td>• Oracle Linux 6.x, 7.x, 8.x, 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2016</td>
<td>• Raspbian Jessie 8.0</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2019</td>
<td>• Red Hat Enterprise Linux 5.11, 6.x, 86-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows 7</td>
<td>• Red Hat Enterprise Linux 5.11, 6.x, 7.x, 8.x, 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows 7 SP1</td>
<td>• SUSE Linux Enterprise Server 11.x - 15.x, 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows 8</td>
<td>• SUSE Linux Enterprise Server 11.x, 86-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows 8.1</td>
<td>• Ubuntu 14.x - 16.x, 86-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows 10</td>
<td>• Ubuntu 14.x - 18.x, 64-bit</td>
</tr>
</tbody>
</table>

⚠️ **Only Pro, Enterprise, and Ultimate workstation operating systems editions are supported.**

In a TLS 1.2 only environment, the target agent operating system must support TLS 1.2.

| Hard drive space   | Approximately 100 MB of hard drive space on the target computer. |
The following software packages are installed by the agent installer if necessary:

- Microsoft Visual C++ 2013 Redistributable Package for 32-bit or 64-bit

.NET Framework support

- On operating systems that support .NET Framework 4.8, all Windows Agent Plugins are migrated to .NET 4.8.
- Upon upgrade to 2019.4, .NET 4.8 is deployed automatically to operating systems that support .NET 4.8.
- .NET Framework 4.5 is deployed for Windows Server 2012 with no .NET Framework installed
- .NET Framework 4.0 is deployed automatically when installing Agents on Windows Server 2008 R2 or earlier or Windows Core

For Linux, you may need to install the following manually:

- Python 3

Starting with Orion Platform 2019.4, Python 3 is deployed automatically to Linux agents. During upgrades, all Linux Agent plugins are migrated to Python 3.

- The bash shell

For AIX:

- You don't need to install Python manually. Required packages are distributed and deployed automatically with the agent plugins.
- Bash or korn shell is required.

Security

The VeriSign Root Certificate Authority (CA) must be current. This is required because the agent software is signed using a VeriSign certificate. To install a certificate, see Certificates and the agent in the Orion Platform.

After the agent is installed, it runs as a Local System account and does not require administrative permissions to function.

Account Privileges

If you want to deploy agents from the Orion server, the following requirements must be met.

<table>
<thead>
<tr>
<th>Type</th>
<th>Windows</th>
<th>Linux/Unix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other software</td>
<td>The following software packages are installed by the agent installer if necessary:</td>
<td>For Linux, you may need to install the following manually:</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Visual C++ 2013 Redistributable Package for 32-bit or 64-bit</td>
<td>- Python 3</td>
</tr>
<tr>
<td></td>
<td><strong>.NET Framework support</strong></td>
<td>Starting with Orion Platform 2019.4, Python 3 is deployed automatically to Linux agents. During upgrades, all Linux Agent plugins are migrated to Python 3.</td>
</tr>
<tr>
<td></td>
<td>- On operating systems that support .NET Framework 4.8, all Windows Agent Plugins are migrated to .NET 4.8.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Upon upgrade to 2019.4, .NET 4.8 is deployed automatically to operating systems that support .NET 4.8.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- .NET Framework 4.5 is deployed for Windows Server 2012 with no .NET Framework installed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- .NET Framework 4.0 is deployed automatically when installing Agents on Windows Server 2008 R2 or earlier or Windows Core</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>The VeriSign Root Certificate Authority (CA) must be current. This is required because the agent software is signed using a VeriSign certificate. To install a certificate, see Certificates and the agent in the Orion Platform.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>After the agent is installed, it runs as a Local System account and does not require administrative permissions to function.</td>
<td></td>
</tr>
<tr>
<td>Latency</td>
<td>Agents can tolerate up to 500 ms of latency between the remote computer and the Orion server.</td>
<td></td>
</tr>
</tbody>
</table>
Windows

- The account used for remote deployment must have access to the administrative share on the target computer: \\<hostname_or_ip>\admin$\temp.
- User Account Control (UAC) must either be disabled on the target computer, or the built-in Administrator account must be used.

> You may need to disable UAC remote restrictions.
Other remote or mass deployment methods do not have the same requirements.

Linux/Unix

- An account that can connect remotely through SSH.
- An account that can install software and create a user and group.

See [Credentials and privileges used on Linux/Unix-based computers](#) for more information.

> To deploy a Linux/Unix agent via pull deployment, make sure that the following conditions are met:
- Orion Web Console must be accessible from the target Linux computer.
- Pull deployment uses wget, curl, or perl to download the installation files from the chosen polling engine.

Agent port requirements

The following ports need to be open both to deploy and to update Orion Agents:

- **Target computer** where the agent is deployed
- **Server hosting the Orion Platform polling engine**

Target computer

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Service/Process</th>
<th>Direction</th>
<th>Communication method</th>
<th>OS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>sshd</td>
<td>Inbound</td>
<td>Either</td>
<td>Linux/Unix</td>
<td>Used to install the agent on Linux/Unix computers through SSH and SFTP or SCP.</td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Service/Process</td>
<td>Direction</td>
<td>Communication method</td>
<td>OS</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>-----------------</td>
<td>-----------</td>
<td>----------------------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>135</td>
<td>TCP</td>
<td>Agent installer</td>
<td>Inbound</td>
<td>Either</td>
<td>Windows</td>
<td>(DCE/RPC Locator service) Microsoft EPMAP. This port must be open on the target computer for remote deployment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>WMI is only needed for deploying the agent to a Windows server with the Add Node or Add Agent wizard. If you do not want to open WMI ports required for software deployment, you can use another deployment method for the Agent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>WMI also uses any random TCP port greater than 1024. See WMI portocalypse on THWACK.</td>
</tr>
<tr>
<td>445</td>
<td>TCP</td>
<td>Agent installer</td>
<td>Inbound</td>
<td>Either</td>
<td>Windows</td>
<td>Microsoft-DS SMB file sharing. This port must be open on the target computer (inbound) for remote deployment.</td>
</tr>
<tr>
<td>17778</td>
<td>TCP</td>
<td>SolarWinds Agent</td>
<td>Outbound</td>
<td>Agent-initiated</td>
<td>All</td>
<td>Used continuously by the agent to communicate back to the Orion server. Also used to deploy the agent.</td>
</tr>
<tr>
<td>17790</td>
<td>TCP</td>
<td>SolarWinds Agent</td>
<td>Inbound</td>
<td>Server-initiated</td>
<td>All</td>
<td>Used to communicate with the Orion server.</td>
</tr>
</tbody>
</table>

**Orion server**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Service/Process</th>
<th>Direction</th>
<th>Communication method</th>
<th>OS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>n/a</td>
<td>Outbound</td>
<td>Either</td>
<td>Linux/Unix</td>
<td>Used to install the agent on Linux/Unix computers through SSH and SFTP or SCP.</td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Service/Process</td>
<td>Direction</td>
<td>Communication method</td>
<td>OS</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>-----------------</td>
<td>------------</td>
<td>---------------------</td>
<td>-----</td>
<td>--------------</td>
</tr>
<tr>
<td>17778</td>
<td>TCP</td>
<td>Orion Module Engine</td>
<td>Inbound</td>
<td>Agent-initiated</td>
<td>All</td>
<td>Used continuously by the agent to communicate back to the Orion server. Also used to deploy the agent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SolarWinds Agent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17790</td>
<td>TCP</td>
<td>Orion Module Engine</td>
<td>Outbound</td>
<td>Server-initiated</td>
<td>All</td>
<td>Used to communicate with the Orion server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SolarWinds Agent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Agent resource consumption

Agent resource consumption is variable and depends on what information is collected and how often the information is collected. This is the same as when the data is polled agentlessly, because in most cases, Agents use the same methods for collecting data as agentless polling.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Consumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Under normal operating conditions, Agent monitoring consumes less than 1% more resources than what would be consumed by monitoring the same node agentlessly.</td>
</tr>
<tr>
<td>Memory</td>
<td>10 - 100 MB, depending on the number and types of jobs.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Roughly 20% (on average) of the bandwidth consumed by the WMI protocol for transmission of the same information. For example, agents use approximately 1.3 kB/s versus WMI at 5.3 kB/s.</td>
</tr>
</tbody>
</table>

A single polling engine can support up to 1,000 agents.

Some Linux distributions, such as CentOS, log all cron jobs, including jobs that ensure the agent service is still up and responding. The log file can become large quickly. If your distribution logs all cron jobs, ensure that you use a tool such as logrotate to keep your log files to a manageable size.

Certificates and the agent in the Orion Platform

The Verisign Root Certificate Authority (CA) must be current. This is required because the agent software is signed using a Verisign certificate. If your certificate is not current, you must download the Root CA certificate and install it to the Local Computer\Trusted Root Certification Authority store on the server hosting the agent.
Multi-module system guidelines for the Orion Platform

This topic provides recommendations for deploying multiple Orion Platform products. These are guidelines only. You can choose to use more or less hardware, but your performance may vary depending on your deployment scenario.

If you have only one SolarWinds Orion module, see the system requirements for that module in the Success Center.

Before you read on, answer the following questions:

- What is the size of the environment you want to monitor with the Orion Platform?
- How many and which Orion Platform products do you want to use to monitor your environment?
- Where do you want to deploy the Orion Platform, in the cloud or on-premise?

Size of monitored environment and Orion Platform products installed

**Small**

For the purposes of this article, "small environments" mean up to three modules from the following list:

- IPAM IP1000 - IP4000
- NCM DL50 - DL200
- NPM SL100 - SL500 (including up to 10 remote agents for DPI)
- SAM SAM10 - SAM 25
- UDT UT2500 - 5000
- VMAN VMS8 - VMS64
  - If you use VMAN Recommendations, increase the total memory on the server by 4 GB.
- VNQM IPSLA 5 - IPSLA 25 (up to 5,000 operations)
- WPM 5 - WPM 20

You can install Log Analyzer, NTA, or SCM as part of a small deployment, but it is not included in this configuration. Use the Medium Deployment guidelines for these Orion Platform products.

**Medium**

For the purposes of this article, "medium environments" include the following modules:

- NPM SL500 - SL2000,
- NTA for NPM SL2000
  - 50,000 FPS received sustained on the main polling engine

and 2 - 4 additional modules:

- IPAM IP16,000
- Log Analyzer LA10 - LA250
• NCM DL500 - DL1000
• SAM SAM50 - SAM75
• SCM SCM50 - SCM1000
• UDT UT10,000 - 25,000
• VMAN VMS112 - VMS320
  If you use VMAN Recommendations, increase the total memory on the server by 8 GB.
• VNQM IPSLA 25 - IPSLA 50 (up to 10,000 operations)
• WPM 50 - WPM 200

Large

For the purposes of this article, "large environments" include the following modules:

• NPM SLX (with multiple polling engines)
• NTA for NPM SLX
  ○ 50,000 FPS received sustained on the main polling engine
  ○ Up to 6 polling engines (5 in addition to the main polling engine) for 300,000 FPS received sustained
• Any combination of these modules:
  ○ IPAM IPX
    ○ 750,000 IP
  ○ Log Analyzer LA250 - LA1000
  ○ NCM DLX
    ○ 1 Additional Polling Engine (APE) for every 10,000 devices, for NCM 7.1 and later
    ○ Maximum of 30,000 devices per NCM instance (that is, NCM server + 2 NCM APEs)
  ○ SAM SAM300
    ○ 1 APE for every 10,000 component monitors
  ○ SCM SCM5000
  ○ UDT UTX
    ○ 150,000 ports per polling engine
  ○ VMAN VMS480 and higher
    ○ Per VMAN Recommendations, increase the total memory on the server by 16 GB.
    ○ 1 APE for every 3000 VMs. VMAN APEs do not require extra licenses.
  ○ VNQM IPX
    ○ ~5,000 IP SLA operations per polling engine

Xlarge

For the purposes of this article, “xlarge environments” monitor up to 400,000 elements. Monitoring these environments requires deploying Additional Polling Engines to scale your deployment.

Disk Performance is measured using IOPS.

CPU recommendations use the PassMark score (© 2018 PassMark® Software, obtained at https://www.cpubenchmark.net/high_end_cpus.html on April 9, 2018).
### How do I find out the PassMark score of my server?


2. Run it on your server to find out a PassMark score of your server.

### Orion Platform deployed in the cloud

Orion Platform products support the following cloud solutions:

- [Amazon Web Service](https://aws.amazon.com)
- [Microsoft Azure](https://azure.microsoft.com)

#### Amazon Web Service

In Amazon Web Services (AWS), the [Elastic Block Storage](https://aws.amazon.com/elasticblockstore/) (EBS) volumes are not your dedicated hardware devices. For [databases used by Orion Platform products](https://docs.solarwinds.com/solarwinds/collectors/orion/platform/cloud-compute-support), SolarWinds recommends using [dedicated instance](https://aws.amazon.com/ec2/instance-types/) EBS volumes for medium and large deployments. For large deployments, SolarWinds recommends EBS with [provisioned IOPS](https://aws.amazon.com/ebs/provisioned-iops/) for high performance for intensive database workloads.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>small</th>
<th>medium</th>
<th>large</th>
<th>xl</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orion server</td>
<td>m4.large</td>
<td>m4.xlarge</td>
<td>m5d.2xlarge</td>
<td>m5.2xlarge</td>
</tr>
<tr>
<td></td>
<td>Recommended:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>m4.xlarge</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary database server</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon RDS service</td>
<td>db.r4.large</td>
<td>db.r4.xlarge</td>
<td>db.r4.2xlarge</td>
<td>db.r4.8xlarge</td>
</tr>
<tr>
<td>Deploying SQL in an Amazon VM</td>
<td>m4.large</td>
<td>r4.xlarge</td>
<td>r5d.2xlarge</td>
<td>r5d.4xlarge</td>
</tr>
<tr>
<td>NTA Flow Storage Database</td>
<td>see medium</td>
<td>r3.xlarge</td>
<td>r5d.4xlarge</td>
<td>r5d.4xlarge</td>
</tr>
<tr>
<td>Log Analyzer Database</td>
<td>see medium</td>
<td>r3.xlarge</td>
<td>r5d.4xlarge</td>
<td>r5d.4xlarge</td>
</tr>
<tr>
<td>Additional Polling engine server</td>
<td></td>
<td></td>
<td></td>
<td>m5.xlarge</td>
</tr>
</tbody>
</table>
## Microsoft Azure

<table>
<thead>
<tr>
<th>Requirements</th>
<th>small</th>
<th>medium</th>
<th>large</th>
<th>xl</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orion server</td>
<td>A4_v2</td>
<td>DS12_v2</td>
<td>DS4_v2</td>
<td>DS4_v2</td>
</tr>
<tr>
<td>Primary database server</td>
<td><strong>Azure SQL</strong> recommended: Only products on Orion Platform 2019.2 and later. The Orion Server must be set to use the same time zone as Azure SQL (UTC by default). Starting with Orion Platform 2019.4, Orion Platform products do not support memory-optimized tables.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Azure SQL</td>
<td>DTU Standard Tier S3 or better vCore General Purpose Tier 2 or better</td>
<td>DTU Standard Tier S3 or better vCore General Purpose Tier 2 or better</td>
<td>DTU Standard Tier S4 or better vCore General Purpose Tier 2 or better</td>
<td>DTU Standard Tier S9 (up to 100k elements), S12 (up to 400k elements) or better vCore General Purpose Tier 2 or better</td>
</tr>
<tr>
<td>Azure Managed Instance</td>
<td><strong>Azure Managed Instance:</strong> 4 vCores</td>
<td><strong>Azure Managed Instance:</strong> 8 vCores</td>
<td><strong>Azure Managed Instance:</strong> 16 vCores</td>
<td><strong>Azure Managed Instance:</strong> 64 vCores</td>
</tr>
<tr>
<td>Orion database deployed in an Azure VM</td>
<td><strong>Database server:</strong> A4_v2</td>
<td><strong>Database server:</strong> DS4_v2 Standard</td>
<td><strong>Database server:</strong> E8s_v3</td>
<td><strong>Database server:</strong> E32-8s_v3</td>
</tr>
<tr>
<td>NTA Flow Storage Database</td>
<td>-</td>
<td>DS12_v2</td>
<td>D15_v2</td>
<td>D15_v2</td>
</tr>
<tr>
<td>Log Analyzer Database</td>
<td>-</td>
<td>DS12_v2</td>
<td>D15_v2</td>
<td>D15_v2</td>
</tr>
<tr>
<td>Additional polling engine server</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
## Orion Platform deployed on-premise

<table>
<thead>
<tr>
<th>Requirements</th>
<th>small</th>
<th>medium</th>
<th>large</th>
<th>xl</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Orion server</strong></td>
<td>Physical server or virtual machine (VM)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CPU: 4 cores + 1 core for each additional module</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RAM: 8 GB + 2 GB for each additional module</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>How do I calculate hardware requirements?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Storage: 150 GB, 15,000 RPM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 x 1 Gb dedicated NIC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2019 or 2016, Standard or Datacenter Edition</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The SolarWinds Orion installer installs IIS and .NET 4.8 or later if they are not already on your server.

- CPUs with a total combined PassMark score of 7,000 or higher
- **Calculate RAM according to the number of modules**: 8 GB + additional 2 GB for each module
- Disk: Read/Write I/O performance of 800 IOPS
<table>
<thead>
<tr>
<th>Requirements</th>
<th>small</th>
<th>medium</th>
<th>large</th>
<th>xl</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary database server</td>
<td>Standard or Enterprise Edition of the following SQL versions:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2017, including Linux installs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2016, 2016 SP1, 2016 SP2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SQL Server 2014, 2014 SP1 or 2014 SP2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SolarWinds recommends SQL Server 2016 SP1 or later.</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>See details on RAID</strong> (physical servers)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Quad core processor or better</td>
<td>Eight processor cores or more</td>
<td>Eight processor cores or more</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 16 GB RAM</td>
<td>64 GB RAM</td>
<td>128 GB RAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 100 GB (or more)</td>
<td>250 GB (or more)</td>
<td>1 Gb LAN port</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minimum:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPUs with a total combined PassMark score of 32,000 or higher</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 256 GB RAM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Disk: Read/Write I/O Performance of 30,000 IOPs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- MS SQL:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Enterprise edition only</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Recommended:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 4 CPU/ 60 cores</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 512 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 190,000 IOPS or better</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 1 Gbit dedicated NIC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirements</td>
<td>small</td>
<td>medium</td>
<td>large</td>
<td>xl</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------</td>
<td>--------</td>
<td>-------</td>
<td>-----</td>
</tr>
<tr>
<td><strong>NTA Flow Storage Database</strong></td>
<td>-</td>
<td>Physical server or virtual machine</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Quad core processor or better</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 16 GB RAM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Increase the NTA Flow Storage database RAM as the database size increases.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 100 GB - 1 TB of storage capacity on local NTFS disk</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: More or less space may be required, depending on your data retention policies and the number of stored flows. You need approximately 8 GB of additional storage for every 1,000 flows per second retained for 30 days. For example, if you want 50,000 flows per second stored for 30 days, you need a base of 100 GB plus an additional 400 GB of storage.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 x 1 Gb dedicated NIC</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Storing flow data in NTA</strong></td>
<td></td>
<td><strong>NTA 4.1 and later</strong> requires a 64-bit operating system. SolarWinds recommends a separate NTA Flow Storage database.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NTA 4.4 and later</strong> uses a second database catalog for storing flow data and requires an instance of MS SQL Server 2016 SP1 or later. SolarWinds Orion database and NTA Flow Storage can reside on the same SQL Server. See <a href="#">NTA current version requirements</a> for more details.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Log Analyzer Database</strong></td>
<td>-</td>
<td>Physical server or virtual machine</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Quad core processor or better</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 16 GB RAM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 100 GB - 1 TB of storage capacity on local NTFS disk</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: More or less space may be required, depending on the number of stored events. Log Analyzer supports 1,000 Events per Second across all polling engines.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 x 1 Gb dedicated NIC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MS SQL Server 2016 with SP1 and later, Standard or Datacenter Edition</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Supported collations:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ English with collation setting SQL_Latin1_General_CP1_CI_AS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ English with collation setting SQL_Latin1_General_CP1_CS_AS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### RAID recommendations

RAID recommendations are only relevant if your primary database is deployed on a physical server. They are NOT relevant if your database is deployed on a virtual machine.

More or less space may be needed depending on your data retention policies, number of elements measured, and polling frequency.

<table>
<thead>
<tr>
<th>Requirements</th>
<th>small</th>
<th>medium</th>
<th>large</th>
<th>xl</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional polling engine server</td>
<td></td>
<td></td>
<td>Virtual machine recommended</td>
<td>Quad core processor or better</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>32 GB RAM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Storage: 150 GB, 15,000 RPM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1 x 1 Gb dedicated NIC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Windows Server 2019 or 2016</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The SolarWinds Orion installer installs IIS and .NET 4.8 if they are not already on your server.</td>
</tr>
<tr>
<td>small</td>
<td>medium</td>
<td>large</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
<td>-------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAID 1+0 configuration (RAID 5 not supported)</td>
<td>RAID 1+0 configuration (RAID 5 not supported)</td>
<td>Hardware RAID Controller (software RAID not supported)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware RAID Controller (software RAID not supported)</td>
<td></td>
<td><strong>Disk Subsystem 1 Array 1:</strong> 2 x 146 GB 15,000 disks RAID 1 (mirroring) operating system</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Disk Subsystem 2 Array 2:</strong> 2 x 146 GB 15,000 disks RAID 1 (Pagefile + extra storage)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Disk Subsystem 3 Array 3:</strong> with 6x 15,000 146 GB or 300 GB disks configured in a RAID 1+0 arrays to allow for maximum write performance. This is for your SQL MDF AND FILEGROUPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Disk Subsystem 4 Array 4:</strong> with 4x 15,000 146 GB or 300 GB disks configured in a RAID 1+0 arrays to allow for maximum write performance. This is for your SQL LDF Transaction LOG file</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Disk Subsystem 5 Array 5:</strong> with 4x 15k 146 GB or 300 GB disks configured in a RAID 1+0 array for your tempdb data file</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Disk Subsystem 6 Array 6:</strong> with 4x 15k 146 GB or 300 GB disks configured in a RAID 0 array for your tempdb log file</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How do I calculate hardware requirements for my Orion server?

Your first Orion Platform product must meet the minimum system requirements for that product. Typically, you need a single quad-core processor and 8 GB of RAM. For each additional module on the same system, add one CPU core and 2 GB of RAM.

<table>
<thead>
<tr>
<th>Modules</th>
<th>CPU</th>
<th>RAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Required: 4 cores</td>
<td>Required: 8 GB</td>
</tr>
<tr>
<td></td>
<td>Recommended: 8 cores</td>
<td>Recommended: 16 GB</td>
</tr>
<tr>
<td>2</td>
<td>Required: 5 cores</td>
<td>Required: 10 GB</td>
</tr>
<tr>
<td></td>
<td>Recommended: 10 cores</td>
<td>Recommended: 18 GB</td>
</tr>
<tr>
<td>3</td>
<td>Required: 6 cores</td>
<td>Required: 12 GB</td>
</tr>
<tr>
<td></td>
<td>Recommended: 12 cores</td>
<td>Recommended: 20 GB</td>
</tr>
<tr>
<td>4</td>
<td>Required: 7 cores</td>
<td>Required: 14 GB</td>
</tr>
<tr>
<td></td>
<td>Recommended: 14 cores</td>
<td>Recommended: 22 GB</td>
</tr>
<tr>
<td>5</td>
<td>Required: 8 cores</td>
<td>Required: 16 GB</td>
</tr>
<tr>
<td></td>
<td>Recommended: 16 cores</td>
<td>Recommended: 24 GB</td>
</tr>
<tr>
<td>6</td>
<td>Required: 9 cores</td>
<td>Required: 18 GB</td>
</tr>
<tr>
<td></td>
<td>Recommended: 18 cores</td>
<td>Recommended: 26 GB</td>
</tr>
<tr>
<td>7</td>
<td>Required: 10 cores</td>
<td>Required: 20 GB</td>
</tr>
<tr>
<td></td>
<td>Recommended: 20 cores</td>
<td>Recommended: 28 GB</td>
</tr>
<tr>
<td>8</td>
<td>Required: 11 cores</td>
<td>Required: 22 GB</td>
</tr>
<tr>
<td></td>
<td>Recommended: 22 cores</td>
<td>Recommended: 30 GB</td>
</tr>
<tr>
<td>9</td>
<td>Required: 12 cores</td>
<td>Required: 24 GB</td>
</tr>
<tr>
<td></td>
<td>Recommended: 24 cores</td>
<td>Recommended: 32 GB</td>
</tr>
<tr>
<td>10</td>
<td>Required: 13 cores</td>
<td>Required: 26 GB</td>
</tr>
<tr>
<td></td>
<td>Recommended: 26 cores</td>
<td>Recommended: 34 GB</td>
</tr>
</tbody>
</table>
License Orion Platform products in the Orion Web Console

SolarWinds Orion Platform products use the web-based License Manager to license products, Additional Polling Engines (APE), Additional Web Servers (AWS), and High Availability (HA) pools.

⚠️ Your main Orion server acts as a licensing server. It cannot be down for more than 14 days or your licenses may be invalidated.

Click Settings > All Settings, scroll down, and click License Manager in the Details grouping to view and manage your licenses.

![License Manager](image)

ℹ️ The web-based License Manager replaces the stand-alone License Manager in Orion Platform products. If you have upgraded from a previous version of your Orion Platform product, you can still use the stand-alone Windows version for Orion Platform 2016.2 and lower. New installs use the web-based License Manager only. If you have upgraded to the new web-based License Manager, SolarWinds recommends that you uninstall the standalone version.

Evaluate Orion Platform products

When you install an Orion Platform product, you can try a fully functional product for the trial period using an evaluation license. The evaluation period for most Orion Platform products takes 30 days. It begins when you install the product and do not have a commercial license activated. You can verify the amount of time remaining for the evaluation in the License Manager.
When you activate a commercial license for most products, the evaluation license expires, and you lose any remaining evaluation days.

The Orion Scalability Engine Evaluation License covers an unlimited number of Additional Polling Engines (APE) and Additional Web Servers (AWS) until the end of the evaluation period even if you activate a commercial license.

What happens after an evaluation license expires?

- Additional Web Servers stop working.
- Polling engines stop polling.
- High Availability pools are disabled.
- Orion Web Console keeps working, but displays only historical data.
- The Evaluation license in the web-based License Manager is marked as expired until it is replaced by a commercial license.

Evaluate performance improvements achieved with Additional Polling Engines and Additional Web Servers

When you install an Additional Polling Engine or Additional Web Server, the Orion Scalability Engine Evaluation license is added to your licenses in the License Manager on the main polling engine. With this license, each polling engine can poll an unlimited number of elements for 30 days.

If you purchase and activate an APE or AWS license during the evaluation period, you can still install and use further APEs or AWS's with the Orion Scalability Engine Evaluation license until the end of the evaluation period.

When the Orion Scalability Engine Evaluation expires, the license is marked as expired in the License Manager. Purchase and activate the appropriate number of APE or AWS licenses.

Can I still evaluate an APE or AWS if I have a commercial license for only one of them?

Yes. If you purchased a license for one type of scalability engine, and want to keep the option to evaluate the other in the future, activate the license before you install the scalability engine to prevent the evaluation license from activating.

You can also request a temporary key from your sales representative.

1. Click Settings > All Settings > License Manager.
2. Click Activate, provide your activation key, and complete the activation. The license will remain unassigned.
3. Install the scalability engine. During the installation, the activated license will be used, and the evaluation period will not start.

When you install the other scalability engine, the evaluation license will still be available.
Evaluate High Availability

High Availability (HA) is licensed per pool. To use the HA feature, you need to license HA pools.

With the High Availability Evaluation license, you can create an unlimited number of HA pools and use HA for 30 days. High Availability Evaluation licenses start the 30-day countdown when you add the first HA pool.

What happens when a High Availability evaluation license expires?

High Availability evaluation licenses expire after the 30-day evaluation period or when you add a commercial license key. When the evaluation license expires, all pools without a valid license are disabled. To enable a pool when the evaluation expires, activate a full license and assign it to the pool.

Activate licenses for Orion Platform products

Activated licenses are automatically assigned to a server that needs a license. If there are more licenses than installed servers, the extra licenses remain unassigned. You can change the license assignment.

The License Manager automatically detects whether your Orion server has access to the Internet, or whether it is offline.

Activate licenses with Internet access

1. Click Settings > All Settings.
2. Click License Manager in the Details section.

If you license your product before you install it, click Add/Upgrade License, enter the details, and complete the activation to see the license in the License Manager.
3. Select the product, and click Activate.

4. Enter the activation key.

   If you are evaluating Orion Platform products and have received a license activation key from a SolarWinds representative, continue with step 5.
   a. Click Customer Portal, and log in using your Customer ID and password or your individual user account information.

   ![Tip] If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support and submit a ticket.

   b. On the top menu bar, click Licenses > Manage Licenses.
   c. Click the plus sign next to the SolarWinds product to display your activation key.
   d. Copy the unregistered activation key, and paste it into the Activation Key field in the License Manager Activate window.

5. Enter registration details, and click Activate.

The license type, the expiration date, the assigned server, and the license key are displayed in the License Manager.

**Activate licenses offline**

If you have installed an Orion Platform product on a computer without Internet access, the web-based License Manager guides you through offline activation.

![Tip] In the offline activation mode, you cannot activate a license for a product that is not installed.

1. Click Settings > All Settings > License Manager to open the web-based License Manager.

2. Select a product, and click Activate.

3. Click Copy to Clipboard to copy the unique machine key.

4. Provide the machine key to SolarWinds to obtain a .lic file.

   If you are evaluating Orion Platform products, provide the machine key to a SolarWinds representative and continue with step 5.
   a. Log in to the Customer Portal, and click Licenses > Manage Licenses.
   b. In the Customer Portal License Management, expand the product license to activate, and click Activate License Manually.
   c. Paste the unique machine id from clipboard, and click Generate License File. Save the .lic file locally and transfer it to the offline computer.

5. In the License Manager on the offline computer, choose the .lic file, and click Activate.

Your license is now activated, and the license details are displayed in the License Manager.
Upgrade licenses in the Orion Platform

When you change how your product is licensed, for example when you increase the number of licensed objects, you receive a new activation key. Activate the key to upgrade your license.

If your Orion Web Console is connected to the Internet, you can also add and activate a license for an Orion Platform product before installing it.

1. Click Settings > All Settings, and then click License Manager.
2. In the License Manager, click Add/Upgrade License.
3. Enter the Activation Key and Registration Information, and click Activate.

Not sure how to get your Activation key? See Activate licenses for more details.

The license is now added to the License Manager and assigned to a server that needs it. If no server needs the license, the license remains unassigned.

Update a license

When you receive a new activation key for a license, activate it.

1. Go to the web-based License Manager, select the license, and click Update.
2. Enter the Activation Key and registration details, and click Activate.

The license key will be used for the license, and you can monitor the number of elements covered by the license.

Assign licenses for Orion Platform products to a server

The License Manager automatically assigns an activated license to a server that needs a license.

When do I need to assign a license?

- To use the license by a different polling engine
- To improve polling capacity (stacking licenses)
- To change the default polling engine or web server assignment

Stack licenses (Additional Polling Engines)

Stacking licenses can improve the polling capacity of your polling engines. You can assign up to four polling engine licenses to one server.

Each polling engine can poll a specified number of elements at the default polling interval. After reaching the maximum number, the polling interval is prolonged. To maintain the default polling interval, assign an additional license to the same polling engine. See Scalability Engine Guidelines for more information about extending the monitoring capacity.
Assign licenses to a polling engine

1. Click Settings > All Settings.
2. Click License Manager in the Details section.
3. Select the license to reassign, and click Assign.
4. Select a polling engine and click Assign.

The polling engine is now using the license.

Migrate Orion Platform licenses from one server to another

You must migrate your licenses if you need to move your main polling engine or Orion server from one computer to another. For example, if you buy new hardware for your Orion server, you must migrate your licenses from the decommissioned server to the new server. See the SolarWinds Migration Guide for more information about moving Orion Platform products.

During the migration period, you can use the evaluation license on the new server. If your migration period extends beyond your evaluation, contact your sales representative for a temporary key. Deactivate the temporary license before activating your license on the new server.

These steps apply to all Orion Platform products, including Additional Polling Engines and Additional Web Servers and assumes you have already installed your SolarWinds products on the new computer.

Do not use the stand-alone License Manager tool for any Orion Platform that you have licensed through the Orion Web Console, including Additional Polling Engines and Additional Web Servers.

Migrate licenses with Internet access

1. On the Orion server, open the Orion Web Console, and click Settings > All Settings > License Manager.
2. Select the licenses, and click Deactivate.

3. On the new server, open the Orion Web Console, and click Settings > All Settings > License Manager.
4. Select the product, and click Activate.

5. Enter the activation key from the Customer Portal, complete the registration form, and click Activate.

Your license is now activated on the new server, and your deprecated server is now unlicensed and no longer gathers data. You can still access historical data on the deprecated server.
Migrate licenses offline

1. On the Orion server, open the Orion Web Console, and click Settings > All Settings > License Manager.

2. Select the licenses, and click Deactivate.

   ![DEACTIVATE]

3. Save the deactivation file, and transfer it to a computer with Internet access.

4. On the computer with Internet access, log in to the Customer Portal, and click License Management > License Management.

5. Select one of the products you are deactivating, and click Manually deactivate this license.

   ![Manually deactivate this license]

6. Upload the Deactivation file when prompted, and confirm that you want to deactivate the products.

7. On the new server, open the Orion Web Console, and click Settings > All Settings > License Manager.

8. Select a product, and click Activate.

   ![ACTIVATE]

9. Click Copy to Clipboard to copy the unique machine key.

10. Log in to the Customer Portal, and click License Management > License Management.

11. In the Customer Portal License Management, expand the product license to activate, and click Activate License Manually.

   ![Activate license manually]

12. Paste the unique machine id from clipboard, and click Generate License File. Save the .lic file locally and transfer it to the offline computer.

13. In the License Manager on the offline computer, choose the .lic file, and click Activate.

Your license is now activated on the new server, and your deprecated server is now unlicensed and no longer gathers data. You can still access historical data on the deprecated server.
Synchronize licenses in the Orion Platform

When your Orion server has access to the Internet, the maintenance status of your licenses is synchronized with the Customer portal daily.

When you want to upgrade your Orion Platform product and your maintenance is expired, extend the maintenance, and then synchronize your license with the Customer Portal. When the license is synchronized, you can upgrade immediately, without having to wait for the next daily synchronization or without having to update the license key manually.

1. Click Settings > All Settings > License Manager to start the License Manager.
2. Click Synchronize.

The License Manager synchronizes with the Customer Portal and any updates in the Customer Portal are reflected in the web-based License Manager.
Discover and add network devices to the Orion Platform

When you install your Orion Platform product, you must 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.

Discover your network for the Orion Platform with the Discovery wizard

Before you begin:

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

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

Add nodes with high latency one at a time.

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

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

<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 rather than including all ranges in a single job.</td>
</tr>
</tbody>
</table>
Subnets  
Use this option to scan every IP address in a subnet. SolarWinds recommends scanning at most a /23 subnet (512 addresses max).

Scanning a subnet returns everything that responds to ping, so we recommend only scanning subnets where the majority of devices are objects you want to monitor.

IP Addresses  
Use this option for a limited number of IP addresses that do not fall in a range.

Since a network discovery job can take a long time to complete, SolarWinds recommends using this option when you are first starting out.

Active Directory  
Use this option to scan an Active Directory Domain Controller.

Using Active Directory for discovery is particularly useful for adding large subnets because Orion can use the devices specified in Active Directory instead of scanning every IP address.

---

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

This setting ensures that any agents you deploy, including the one on your Orion server, are up-to-date. If there are no nodes using agents, you can leave this option unchecked.
5. On the Virtualization panel, to discover VMware vCenter or ESX hosts on your network:
   a. Check Poll for VMware, and click Add vCenter or ESX Credential.
   b. Select <New credential> and provide required information.

![Add VMware Credential]

If you do not add the host credentials, Orion still discovers the virtual machines (VMs) on the host. However, you will not be able to see the relationships mapped between the VMs and hosts.
6. On the SNMP panel:
   a. If all devices on your network require only the default SNMPv1 and SNMPv2 public and private community strings, click Next.
   b. If any device on your network uses a community string other than public or private, or if you want to use an SNMPv3 credential, click Add Credential and provide the required information.

   ![Add New Credential]

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

   ![Network Sonar Wizard]

   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 a few minutes to a few hours, depending on the number of network elements the system discovers.

Add nodes to the Orion Platform using Active Directory

Query your Active Directory Domain Controller to add nodes quickly and efficiently. Your Orion server can use the devices specified in AD instead of scanning every IP address in the subnet.
Create scheduled discoveries to discover and import any new servers and workstations that have been added to AD automatically.

1. Click Settings > Network Discovery, and click Add New Discovery.
2. On Network Selection, click Add Active Directory Controller to query.
3. On the Add Active Directory DC pop-up, enter your domain controller’s IP address/hostname and credentials, and click Next.
4. Select the organizational units (OUs) you want to scan for nodes, and click Finish.

By default, all OUs are selected, but only servers will be added. Add workstations by clearing the Import servers only check box below the OUs.

On the Network Selection page, you will see the OUs you have added. You can add additional AD controllers, or any other IP addresses that you need before continuing with discovery.

5. Complete the Network Discovery.

Credentials for Active Directory discovery in the Orion Platform

When you use Active Directory discovery to add nodes, you must provide the credentials of a Domain Administrator user.

The credentials you provide are added to the discovery wizard as Windows credentials automatically.

If the Active Directory credentials are not same as the Windows credentials for monitoring the node, add credentials for WMI monitoring in the Windows Credentials step.
Automatically add discovered nodes to the Orion Platform

Automatic monitoring means you do not have to go through the Discovery Import wizard every time you run a discovery. It is useful when you have configured your discovery to find similar nodes or network devices.

1. Click Settings > Network Discovery, and add a discovery, or select an existing one and click Edit.
2. Click through the Discovery Wizard to the Monitoring Settings page.
3. Choose to include devices that only respond to ICMP (ping). If you decide to exclude devices that only respond to ICMP, your discovery list may be smaller than you expect and you must add those devices manually.
4. On Monitor Settings, select Automatically monitor based on my, and click Define Monitoring Settings.

5. Select the interfaces properties you want to apply to any discovered nodes and click Next. You can also create advanced filters for interfaces under Advanced selection options. This option is available for NPM.

Tips for choosing interfaces

- Only monitor access ports that should always be up. Do NOT monitor desktop access ports because these ports will show an error state when everyone goes home for the day (for example).
- For switches, routers & firewalls, select Up trunk ports and wireless access ports.
- For servers, select Up interfaces.
- Use Advanced Filtering Options for existing interface descriptions to choose your most interesting ports, such as 'uplink', 'WAN', etc.
6. Choose the types of volumes you want to monitor.

Tips for choosing volumes

- For switches, routers, and firewalls, select Flash memory, and RAM.
- For servers, select RAM, Virtual Memory, Fixed Disk, Mount Points (*nix systems), or Network Disk (Windows).
- We do not recommend monitoring CDs, removable disks, or floppy disks (CDs always show '100% full,' and removable disks disappear and display as unknown).
- Other and Unknown volumes cannot be identified on import, so you may need to take additional actions to identify them.

7. Choose the applications you want to monitor. Only the most commonly monitored applications are available in this screen. You can monitor other applications by using applications templates. This option is available for SAM.

8. Click Finish.

9. Continue configuring your discovery. When the discovery is run, your monitoring settings will be applied to any discovered devices, and anything that matches will be imported and monitored automatically.

Advanced discovery in the Orion Platform

Check out this video on managing discovery jobs and performance.

At this point you have completed an initial discovery. Now you can add discoveries to include other segments of your IT environment.
Discovery jobs do not impact polling. Polling is prioritized first.

- **Multiple jobs.** SolarWinds recommends building as many discovery jobs as needed to scan your network. Initially, run the jobs immediately so you can see everything on your network, and then schedule the jobs to run periodically. Dividing the discovery into multiple jobs makes it easier to be selective about what to monitor, and decreases the amount of time each job runs. When you have a large environment, consider dividing discovery jobs by:
  - Credentials - the more credentials you have, the longer it takes for the discovery job to complete. Place the most common credentials at the top of the list.
  - IP address range - use a range that consists of fewer than 2,000 IP addresses. In a range, unresponsive IP addresses slow down discovery.
  - Latency - run discoveries for remote offices separately so that you can adjust the timeout threshold.
  - Polling engine - if you have multiple polling engines, configure a discovery for a specific polling engine.

- **Discovery ranges.** Although you can discover specific nodes, SolarWinds recommends using a range of IP addresses or subnets for a more complete picture of your network. None of the discovered elements count toward your license total or affect system performance until you begin monitoring. You can add multiple IP ranges or subnets to the same scan, but you cannot include IP ranges and subnets in the same scan.

- **Discovery thresholds.** If you run a discovery and nodes you expect to see are not found, you may need to adjust the timeout and retry thresholds. In an environment with high latency, the default values may not be high enough. Only adjust these values after an initial scan. The higher the threshold value, the longer the discovery job takes to complete.

- **Polling engine.** If you have multiple polling engines, you will see an option to select a polling engine. The polling engine you select runs the discovery job and monitors your network. SolarWinds recommends that you limit a poller to 12,000 elements, so be careful not to overload one polling
engine. If you have a large environment with significant differences in latency, position the polling engine close to the monitored objects.

- **Schedule intervals.** Schedule your discovery jobs to run periodically to identify new devices that were added to your network. Unless you work in a dynamic environment where new devices are frequently added to your network, SolarWinds recommends scheduling discovery daily. You can also select Advanced from the Frequency drop-down menu to create a custom frequency. The schedule interval you choose depends on how often you want to scan for changes to the network and the size and performance of your deployment.

- **Scheduled results.** A manual, scheduled discovery only finds network elements, but does not automatically start monitoring. You must select what you want the system to monitor. If the scheduled job locates nodes that you do not want to monitor, select those nodes and click Add to Ignore List. Ignoring hides elements from the results list the next time the discovery job runs.

1. Scheduled discovery profiles should not use IP address ranges that include nodes using DHCP.
Add discovered devices to the Orion Platform

After the Network Sonar Wizard discovers your network, the Network Sonar Results Wizard opens, allowing you to import network elements into your Orion Platform product. Nodes that are discovered do not count against your license count. Only nodes that you have added to the SolarWinds Orion database count against your license.

When you manually run discovery, by default, the system automatically selects all network elements to be monitored. You must clear the check boxes for elements you do not want monitored.

If you are discovering your network for the first time, SolarWinds recommends that you monitor a small number of devices.

1. If the Network Sonar Results Wizard does not open automatically, click the Scheduled Discovery Results tab, select nodes you want to monitor, and then click Import Nodes.
2. Ensure the device types you want to monitor are selected, and click Next.

![Network Sonar Results Wizard](image)

If a device appears as unknown vendor, it means that the credentials could not be validated. As a result, the product can only detect if the device is up or down, and cannot collect any other data. To resolve this issue, verify the SNMP configuration on the device. If the credentials still cannot be validated, and you have an active SolarWinds contract, contact technical support.

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

SolarWinds recommends that you do not monitor VoIP interfaces or NULL interfaces.

![List of Interfaces](image)
By default, SolarWinds NPM imports interfaces that are discovered in an Operationally Up state. However, because interfaces may cycle off and on, you can also select Operationally Down or Administratively Shutdown states for import.

4. Ensure the volume types you want to monitor are selected, and click Next.

SolarWinds recommends that you do not monitor compact disks or removable disks.

5. Review the list of elements to be imported, and click Import.

6. When the import completes, click Finish.
7. Click the My Dashboards > Summary to begin exploring your network.

![Orion Summary Home]

**Add a single node for monitoring to the Orion Platform**

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

💡 Adding a single node offers more detail in monitoring and is recommended for nodes with high latency. Do not include nodes with high latency in a discovery job.

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

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

To add a single node for monitoring:

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

![Polling Method Selection](image)

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

![Statistics Selection](image)

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

   ![Polling Settings Table]

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

   c. Enter values for custom properties for the node.

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

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

7. Click OK, Add Node.
   The node will be monitored according to the options you set.

**Choose the polling method to use in the Orion Platform**

Select a polling method to monitor nodes in the way that best suits your environment.

**External Node (No Status)**

Orion Platform products do not poll the node, no data is collected from the node. This method is suitable for nodes hosting applications or other elements that you want to monitor with specific Orion Platform products, such as SAM.

Use this method to build a complete map of the environment monitored by your Orion Platform products.

**Status Only: ICMP**

This method monitors only the status and measures the average response time and packet loss percentage for managed devices using the Internet Control Message Protocol (ICMP).
Use this method when you need limited information or to monitor devices that do not support SNMP or WMI.

This polling method requires that you enable ICMP on your nodes. Consider adjusting any network intrusion detection systems or your firewalls to allow for the ICMP traffic.

**Most Devices: SNMP & ICMP**

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

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

Consider adjusting any network intrusion detection systems or your firewalls to allow for the ICMP traffic.

**SNMPv3**

SNMPv3 is a secure version of the protocol that adds authentication and/or encryption. It may require additional configuration on your devices.

To poll the device with SNMPv3, specify the credentials, the authentication, and encryption.

If you have both read-only and read/write credentials configured on the device, you may also need to provide the read/write credentials. To enable Orion Platform products to execute commands that require read/write privileges, type your read/write credentials in the Read / Write SNMPv3 Credentials section. Read/write privileges may be required by Engineer's Toolset or NPM/NCM, for example for changing an administrator status on the device.

You can save the credentials (username, context, authentication, and encryption) to the credential library for reuse directly from the Add Node wizard. Provide the details, type a name for the credentials set and click Save in the Credential Set Library section. Click Saved Credential Sets to select a set from the library.

**Windows Servers: WMI and ICMP**

This polling method can only be used for Windows computers. Windows Management Instrumentation (WMI) is a proprietary technology used to poll performance and management information from Windows-based network devices, applications, and components.

When used as an alternative to SNMP, WMI can provide much of the same monitoring and management data currently available with SNMP-based polling with the addition of Windows-specific communications and security features.
Your devices must have WMI and ICMP enabled to use this polling method. You can use `WBEMTest.exe`, which is included on every computer that has WMI installed, to test the connectivity between your Orion server and your Windows computer.

Due to specific characteristics of WMI polling requests, polling a single WMI enabled object uses approximately five times the resources required to poll the same or similar object with SNMP on the same polling frequency. Consider adjusting any network intrusion detection systems or your firewalls to allow for the ICMP traffic.

**Windows and Linux/Unix Servers: Agent**

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

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

This polling method is most useful in the following situations:

- When host and applications are behind firewall NAT or proxies
- Polling node and applications across multiple discrete networks that have overlapping IP address space
- Secure encrypted polling over a single port is required
- Support for low bandwidth, high latency connections
- Polling nodes across domains where no domain trusts have been established
- Full end-to-end encryption between the monitored host and the poller

**Meraki Wireless: API**

If you have NPM 12.1 and later installed, select this option to monitor Meraki wireless infrastructure.

**SNMP credentials for the Orion Platform**

The SNMP Credentials page displays a list of all the SNMP credentials that are defined for your network. Community strings are displayed for SNMPv1 and SNMPv2c credentials, and the User and Context are displayed for SNMPv3 credentials.

The default SolarWinds Orion community strings for SNMPv1 and SNMPv2c devices are public and private.

Make sure the most frequently used credentials are on the top of the list to make the discovery faster.
Add SNMP credentials

1. From the Network Sonar Wizard, click Add New Credential.
2. Select the SNMP Version of your new credential, provide the details, and then click Add.

SNMPv3

SNMPv3 is a secure version of the protocol that adds authentication and/or encryption. It may require additional configuration on your devices.

To poll the device with SNMPv3, specify the credentials, the authentication, and encryption.

If you have both read-only and read/write credentials configured on the device, you may also need to provide the read/write credentials. To enable Orion Platform products to execute commands that require read/write privileges, type your read/write credentials in the Read / Write SNMPv3 Credentials section. Read/write privileges may be required by Engineer’s Toolset or NPM/NCM, for example for changing an administrator status on the device.

You can save the credentials (username, context, authentication, and encryption) to the credential library for reuse directly from the Add Node wizard. Provide the details, type a name for the credentials set and click Save in the Credential Set Library section. Click Saved Credential Sets to select a set from the library.

The new credentials are used in the Discovery Wizard, and are stored for further use.

Import nodes to the Orion Platform from a list of IP addresses

1. Open the file with IP addresses to import.
2. Log in to the Orion Web Console, and click Settings > Network Discovery.
3. Click Add New Discovery to create a new discovery, or select a discovery, and click Edit.
4. Click IP Addresses, and copy and paste the IP addresses or host names of the devices from your file into the field.

   🔄 Enter one IP address or host name per line.

5. Click Validate to confirm that the provided IP addresses and host names are assigned to SNMP-enabled devices.
6. Complete the discovery and import the devices.

The Network Sonar Results Wizard opens with the results of your discovery.
Manage scheduled discovery results in the Orion Platform

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

1. Log in to the Orion Web Console and navigate to Settings > Network Discovery.
2. Click Scheduled Discovery Results.
3. Filter the results the left pane.
4. Update your SolarWinds Orion database to include changed or discovered nodes by selecting all nodes to update or to add, and clicking Import Nodes.
5. Ignore devices in future discoveries by selecting the nodes to ignore, and clicking Add to Ignore List.

Minimize SNMP processing load during discoveries in the Orion Platform using the Discovery Ignore List

Network discoveries often find devices you do not intend to monitor. Add the devices you do not want to monitor to the Discovery Ignore List to minimize the SNMP load associated with discovering devices not meant for monitoring.

1. Log in to the Orion Web Console, and navigate to Settings > Network Discovery.
2. Click Scheduled Discovery Results.
3. Select devices you want to ignore, and click Add to Ignore List.

Use items in the Status and Group by lists to help you find devices.

The selected devices will not be discovered by the discovery.

Add ignored devices back to discovery

1. Log in to the Orion Web Console, and navigate to Settings > Network Discovery.
2. Click the Discovery Ignore List, and select the objects you want to monitor.
3. Click Remove from Ignore List.
4. Confirm that you want to stop ignoring selected items by clicking OK.

The devices removed from the list will be included in the discovery again.

Manage devices in the Orion Web Console

In the Orion Web Console, you can add and remove devices, and quickly view and edit device properties from the Manage Nodes view.

You need node management rights.
Orion Platform 2017.3 introduces an updated version of Node Management view, the Manage Entities view. The new, intuitive page provides flexible filters and commands for managed entities. To go to the new page, click The New Manage Entities Page in the upper right.

To access the Manage Nodes view:

- Click Settings > Manage Nodes.
- Click Manage Nodes in the All Nodes resource.

The Orion Summary Home view includes the All Nodes widget, or resource, by default, but you can include it on any other view.

Delete devices from monitoring

Deleting a node removes all its applications, interfaces, and volumes. An individual event may be recorded for each deleted network object.

Delete Nodes in Node Management

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Select the entity, and click Delete.

Delete multiple interfaces on different nodes

On the Manage Nodes page, use the search tool to find the nodes, select the interfaces, and click Delete.

On the Manage Entities page, expand related entities for the nodes, select interfaces in Related Entities, and click Delete.

4. Click OK to confirm deletion.

You have removed the node and its applications, interfaces, and volumes from monitoring.

Delete nodes from the Management widget

1. Go to the Node Details view of the node.
2. In the Management widget, click Delete Node.
3. Confirm the message.

The node, together with all applications, interfaces, and volumes monitored on the node are removed from monitoring.

View node data in tooltips

Hover over a monitored node in the Orion Web Console to view an immediate status overview of the device.
**Node Data in tooltips**

<table>
<thead>
<tr>
<th>Node Status</th>
<th>Current status of the node (Up, Down, Warning, Unmanaged, or Unreachable).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling IP Address</td>
<td>The IP address currently assigned to the selected node.</td>
</tr>
<tr>
<td>Machine Type</td>
<td>The vendor icon and vendor description of the selected node.</td>
</tr>
<tr>
<td>Average Response Time</td>
<td>The measured average response time of the selected node as of the last node poll.</td>
</tr>
<tr>
<td>Packet Loss</td>
<td>The percent of all transmitted packets that are lost by the selected node as of the last node poll.</td>
</tr>
<tr>
<td>CPU Load</td>
<td>The percent of available processing capacity on the selected node that is currently used as of the last node poll.</td>
</tr>
<tr>
<td>Memory Used</td>
<td>The percent of available memory on the selected node that is currently used as of the last node poll.</td>
</tr>
</tbody>
</table>

**Edit node properties**

⚠️ Only edit node properties in a single browser tab to prevent database errors and data losses.

ℹ️ You must have **Node Management Rights** to edit properties.

Available properties depend on the Orion Platform products you have installed.

1. Click Settings > Manage Nodes.
2. Locate and select the node, and click Edit Properties.
3. Make changes on the Edit node view, and submit your changes.

**Edit the node name, web address, and the default node view**

- To rename the node, enter a name in the Name field on the Edit node view.
  Changing the node name only affects the way the node is identified on charts and graphs in the Orion Web Console. It does not impact the node as it is referenced on the network.
- To change the default view for the node, select the View Type from the list.
- To change the navigation to the node from the resource, replace the default Web Browse Template with `http://{{HrefIPAddress}}`.
- Click Submit.

You have updated the node properties.

**Edit polling settings**

1. To change the polling IP address, enter the IP address, or click Select IP Address and select the IP address.
Changing the IP address affects data collection. Change the IP address only if it changed on your network to continue collecting the statistics without reconfiguring the node.

2. To dynamically assign the IP address of the selected node, select Dynamic IP Address (DHCP or BOOTP), provide the DNS Hostname, and select the IP Address Resolution format.

If the device is dual-stack, IPv4 resolution is used by default.

3. Change the polling method for a node.

4. If you are using SNMP to poll the selected node, you can:
   a. Edit the SNMP Version and SNMP Port.
   b. Allow 64-bit counters. When experiencing frequent counter rollovers for high-speed interfaces, confirm that the monitored device supports 64-bit counters, and select Allow 64-bit Counters.

   Some vendor implementations of 64-bit counters produce faulty data. If you notice inconsistent or incorrect data, clear the box to disable 64-bit counters.

   c. Edit the Community Strings (for SNMPv1 and SNMPv2c) or Credentials, Privacy and Authentication settings (for SNMPv3).

   Changing the community string or SNMP port affects data collection. Do not change the IP address, community string, or SNMP port unless they have changed on your network.

   Changing the SNMP port applies to statistics polls, Universal Device Pollers (UnDPs), and SNMP trap collection.

d. Click Test to test your provided SNMP settings.

5. To change the existing polling intervals, provide new intervals in the Node Status Polling, Collect Statistics, and Poll for Topology Data fields.

6. If there are multiple polling engines in your environment and you want to change the polling engine that polls the node, click Change Polling Engine.

7. Click Submit.

You have updated the polling settings for the node.

Edit dependencies or custom properties

To add, edit, or delete an existing dependency that includes the node:

1. Click Manage Dependencies and adjust the dependencies.

2. Provide values for custom properties on the node. If you cannot see the required custom property, click Manage Custom Properties to create or manage custom properties.

3. Click Submit.

You have edited dependencies or custom properties.
Add data to poll on the node

Some Orion Platform products provide additional monitoring for specific devices. To poll additional data for a node, select relevant options, enter required information, and click Submit.

- If the node is a UCS device that you'll poll for UCS data, select the UCS Manager Credentials check box and fill out the fields that appear, including the Port on which the UCS Manager listens and credentials for the UCS Manager web portal. See Set up monitoring for UCS devices for details.
  
  Click Test to verify that the UCS Manager credentials are valid.

- If you have SolarWinds User Device Tracker (UDT) installed and the node has UDT ports attached, you can poll Layer 3 data. Select Poll Layer 3 Data from Device, and enter the Layer 3 Polling Interval.

  Select Disable VRF Context Polling, if required.

- If SolarWinds SAM is installed, you can monitor Active Directory users that log in to your network. Select Active Directory Domain Controller, and provide the following information.
  a. Select the credential to be used, or select New Credential, and define the credential.

  You only need administrator credentials for installing agents.

  b. Click Test to validate the credentials.

  c. Enter the Domain Controller Polling Interval. The default is 30 minutes.

- To poll for VMware, select Poll for VMware, provide the vCenter or ESX Server credentials, and click Test. See Monitor virtual infrastructure for more details.

You have set up your Orion Platform product to poll additional data on the device.

Customize alert thresholds

Specify custom thresholds for the node to receive alerts when polled values exceed a threshold for the metric.

1. Scroll down, select Override Orion General Thresholds for the metric, and adjust the default values.
2. Click Submit.

You have updated alerting thresholds for the device.

Change the polling method for a node

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Select the node for which you want to change the polling method, and click Edit Properties.
4. Select the Polling Method.
5. If you are using SNMP to poll the selected node, select the SNMP version supported on the device, and provide the port and community strings. Click Test to verify that the SNMP settings are correct.

- By default, Orion Platform products use SNMPv2c to poll for performance information. To poll the device using SNMPv1, you must disable SNMPv2c on the device.
- For most SNMPv2c devices, the community string public gives sufficient access. To see the available community strings, click into the Community String field, and press the down arrow key.
- To save the community strings as a credential set, provide a Name, and click Save.

6. Click Submit.

Your Orion Platform product polls the device using the selected method.

Promote a node from ICMP to SNMP monitoring

Orion Platform products only use ICMP to poll devices for status, average response time, and packet loss.

If a node which you added to the SolarWinds Orion database as an ICMP only node also supports SNMP, and you want to start collecting additional statistics, change the polling method to SNMP.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Select Nodes from the Show drop-down list, and locate the node which you want to edit.
4. Select the node, and click Edit Properties.
5. In the Polling Method section, select Most Devices: SNMP and ICMP.
6. Select the version of SNMP to use. The default is SNMPv2c.
7. If you have installed multiple polling engines, select the Polling Engine you want to use to collect statistics from the added node. This option is not displayed if you are only using one polling engine.
8. If the SNMP port on the added node is not the Orion default of 161, enter the actual port number.
9. If the added node supports 64-bit counters and you want to use them, select Allow 64-bit Counters.

- If you notice erratic or incorrect data when using 64-bit counters, clear the Allow 64 Bit Counters box for the device, and contact the hardware manufacturer.

10. For SNMPv1 or SNMPv2c, enter the Community String and, optionally, the Read/Write Community String. Click Test to validate the strings.

- The Community String is a password to authenticate data sent between the management station and the device. The default is usually "public". Use the strings configured on the device.

11. For SNMPv3, provide the credentials and click Test to validate the credentials. See the vendor documentation for your network device for further information.

12. Click Submit.
Change polling engine node assignments in the Orion Platform

Reassigning nodes to new polling engines may be required in the following situations:

- Moving or renaming your Orion server
- Deleting an existing polling engine
- Merging two or more Orion servers
- Deploying Additional Polling Engines to distribute the load

To change the polling engine that polls a node:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Select the node for which you want to change the polling engine.
4. Click More Actions, and click Change Polling Engine.

   The current number of Assigned Objects is listed for each available polling engine. This number is updated with each automatic polling engine synchronization. Updates to the Assigned Objects count can only be completed for polling engines that are operationally up.

5. Select the polling engine, and click Change Polling Engine.

Your Orion Platform product polls the node using the selected polling engine.

View the resources and statistics monitored on a node

Resources monitored on a node include interfaces and volumes. The status of objects is signified by an icon. The List Resources view also lists statistics monitored on the node.

1. Click Settings > Manage Nodes.
2. Select the node, and click List Resources on the Node Management toolbar.

The view now lists discovered interfaces and volumes for the node, and indicates the currently monitored items.

In Orion Platform 2017.3, SolarWinds introduced an updated Manage Nodes view that is called Manage Entities.

   To display interfaces on Manage Entities, click the arrow at the end of the node line. Monitored interfaces on the node display in the Related Entities pane.

Suspend data collection or alerts for nodes in Maintenance Mode

During maintenance, nodes might be Down for short periods of time. To prevent alert messages, and to ensure that your Orion Platform product collects the data you need, place the nodes to Maintenance Mode.

You need the Allow Account to Unmanage Objects & Mute Alerts right.
Choose one of the following maintenance options:

- **Mute alerts**: data for the node, interfaces, and volumes on the node are collected, but alerts do not trigger.
  
  **Muting alerts is not supported for SRM and VMAN objects.**
  
  This option only mutes new alerts. If alert actions keep triggering although you have muted the alert, the alert is configured to trigger repeatedly. Acknowledge the alert to stop triggering new alert actions.

- **Stop collecting data for the node**: data for the node, interfaces, and volumes on the node are **not** collected, and alerts do not trigger.
  
  **If you stop polling data for a node, polling is also stopped for all interfaces and volumes on the node.**

- **Schedule a maintenance period**: specify a period of time to stop collecting data or to mute alerts for a node.

  Orion Platform 2017.3 and later provide access to the maintenance options from the Manage Entities view: select nodes, click More, and select a maintenance option.

  Click the mute icon to unmute alerts or to cancel suspended alerts.

### Mute alerts

Mute alerts for a node to perform maintenance on the node without interruptions by false positive alerts.

1. Click Settings > Manage Nodes.
2. Select the nodes and click Maintenance Mode > Mute Alerts.
   
   You do not receive alerts until you resume alerts for the nodes.

### Resume alerts

After maintenance, resume alerts for the node, interfaces, and volumes on the node.

1. Go to the node details view.
2. In the Management resource, select Maintenance Mode > Resume Alerts (Unmute).

Alerts for the node are active.

### Stop collecting statistics

To stop collecting statistics for nodes during maintenance, unmanage the nodes.

1. Click Settings > Manage Nodes.
2. Select the nodes, and click Maintenance Mode > Unmanage Now.

NPM stops collecting statistics for the node until you manage the node again.
Start collecting statistics
After maintenance, resume polling the node.

1. Go to the Node Details view.
2. In the Management resource, select Maintenance Mode > Manage Again.

NPM collects performance and availability data, and displays the data in the Orion Web Console.

Schedule a maintenance period
Suspend alerts or stop collecting performance and availability data for nodes during a specified time period.

1. Click Settings > Manage Nodes.

You can also schedule maintenance from the node details view for the node. Click Maintenance Mode in the Management resource, and select a maintenance option.

2. Select the nodes and click Maintenance Mode > Schedule.
3. Select the maintenance option:
   - **Mute alerts**: collect data for the node, interfaces, and volumes, but do not trigger alerts.
   - **Stop polling the node**: data for the node, interfaces, and volumes on the node are *not* collected, and alerts do not trigger.
4. Specify the maintenance period, and click Schedule.

The maintenance is scheduled.

Change scheduled maintenance
You can reschedule the maintenance or change the maintenance mode.

1. Go to the Node Details view and locate the Management resource.

To change or cancel maintenance for multiple nodes, go to Settings > Manage Nodes, and select the nodes.

2. Click Maintenance Mode > Schedule. Change the time period for the maintenance or the maintenance mode, and click Submit.

The maintenance schedule is adjusted according to your settings.
Cancel scheduled maintenance from the Node Details resource

1. On the Node Details view, locate the Node Details resource.
2. Review the maintenance information in Node Status, and click Cancel.

The scheduled maintenance is canceled.

Cancel scheduled maintenance from Manage Entities page

In Orion Platform 2017.3, you can cancel scheduled maintenance from the Manage Entities page.

1. Click Settings > Manage Nodes.
2. Click the link to Manage Entities in the info bar.
3. To cancel a planned maintenance with:
   - muted alerts, click the muted alerts icon next to the node.
   - Unmanage, select the nodes and click More > Cancel Planned Unmanage.

The scheduled maintenance is canceled.

To cancel scheduled maintenance for multiple nodes, select the nodes and click More > Manage Again or Resume Alerts, according to the maintenance settings.

Poll and rediscover devices immediately

Orion Platform products regularly poll devices for statistics and status, as specified in the Polling Settings. Discoveries run according to a schedule.

Use the Rediscover option to update node data that do not change often, such as machine type, system name, or location.

You can poll a device or rediscover a node manually at any time.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Select the entity you want to poll or rediscover.
4. To poll the selected entity, click Poll Now.
5. To rediscover the selected entity, click More > Rediscover.
Your Orion Platform polls the entity, or redisCOVERS static data.

Calculate node status in the Orion Platform

By default, node status is detected using ICMP: The Orion Platform sends a ping request. If the Orion Platform does not receive the response, it places the node into the Warning state and fast-polls the device for 120 seconds. If the node still does not respond, the Orion Platform notifies you that the node is Down.

ICMP only tells you the Orion Platform did not receive a response for the ping request. The device could be down, but there might also be a routing problem, an intermediary device could be down, or something could have blocked the packet on its way to or from the device. See Get more details about the node in the NPM Getting Started Guide for more details.

Status of sub-elements, such as interfaces and volumes, is detected using SNMP. This is more accurate, because the device tells you that the sub-element is Down.

Orion Platform status options

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status name</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>critical</td>
</tr>
<tr>
<td>🔄</td>
<td>down</td>
</tr>
<tr>
<td>🔄</td>
<td>external</td>
</tr>
<tr>
<td>🔄</td>
<td>unknown</td>
</tr>
<tr>
<td>🔄</td>
<td>unmanaged</td>
</tr>
<tr>
<td>🔄</td>
<td>unreachable</td>
</tr>
<tr>
<td>🔄</td>
<td>up</td>
</tr>
<tr>
<td>🔄</td>
<td>warning</td>
</tr>
</tbody>
</table>

Enhanced node status - what does it mean?

In Orion Platform 2018.4 and earlier, the node status icon consisted of two circles - the large one reflected whether the node was up or down, the small one provided information about additional metrics.
Starting with Orion Platform 2019.2, you can keep using this "classic" method for calculating node status, or switch to the "enhanced" node status calculation where you can select what "contributors" are reflected in the status. A contributor is a status of a metric or feature that can influence the node status, such as the status of an interface, a hardware health sensor, or even a threshold.

Based on your settings, the following items might be reflected in node status:

- **Node thresholds**: Both global thresholds and thresholds specified for individual nodes are now reflected in the node status.
- **Child objects**: The status of interfaces, hardware health, or applications monitored on a node is reflected in the node status.

Where can you see a change when you switch to the enhanced node status calculation?

- **Orion Maps**: The status of mapped objects reflects the status of components used to calculate the node status.
- **Groups**: With enhanced status calculation, you can only use nodes to form a group. Status of all child objects associated with them will be reflected in the node status.
- **Alerts**: Thresholds and child objects now influence node status so you no longer need alert definitions for individual metrics or child entities.

To keep you informed about what went wrong, new macros for root cause were added:

- `{N=SwisEntity;M=NodeStatusRootCause}`
- `{N=SwisEntity;M=NodeStatusRootCauseWithLinks}`

If you add these variables to the trigger action message, the notification will include any node thresholds which have been crossed, as well as a list of all child objects in a degraded state associated with the node.
- **Node tooltips**: If you position your cursor over a node in the critical status in any widget, the child entities causing the problem are listed at the bottom of the tooltip.

```
<Diagram of a widget with a tooltip>
```

**Configure enhanced mode**

The enhanced node status calculation is enabled by default on new installations.

If you upgraded from a previous Orion Platform version, you might need to configure the feature.

> Before you enable enhanced status calculation, SolarWinds recommends that you disable alert actions in the Alert Manager. Click Alerts & Activity > Alerts, and click More > Pause actions of all alerts. After you enable the feature, check active alert, tweak the alerts that should not trigger, and re-enable alert actions.

1. **Enable the feature.**
2. **Specify what should influence your node status**. This step is optional, as SolarWinds provides with a default combination of enabled contributors.
3. **Adjust the status rollup mode for individual nodes.** This step is optional. The default option is Mixed status.

Enable the enhanced node status calculation

Starting with Orion Platform 2019.2, this is the default option.

1. Click Settings > All Settings > Polling Settings.
2. Scroll down to Node Status calculation, and select Enhanced.
3. Submit your changes.

Specify what should be included in the node status calculation

Including a group contributors, such as interfaces, into the node status calculation means that the node status turns to warning when any of the entities on the node is down.

1. Click Settings > All Settings and scroll down to Thresholds & Polling.
2. Click Node Child Status Participation.
3. Review the list of components that can influence the node status. Available items depend on the Orion Platform products you have installed.
4. Enable items to be included in node status calculation.

SolarWinds recommends that you keep the default settings.

<table>
<thead>
<tr>
<th>Node status contributors</th>
<th>Polling settings</th>
<th>What are status contributors?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Node Poller</td>
<td>NOT Contributing</td>
<td></td>
</tr>
<tr>
<td>Custom Interface Poller</td>
<td>NOT Contributing</td>
<td></td>
</tr>
<tr>
<td>CPU Load Threshold</td>
<td>Contributing</td>
<td></td>
</tr>
<tr>
<td>Percent Packet Loss Threshold</td>
<td>Contributing</td>
<td></td>
</tr>
<tr>
<td>Memory Usage Threshold</td>
<td>Contributing</td>
<td></td>
</tr>
<tr>
<td>Response Time Threshold</td>
<td>Contributing</td>
<td></td>
</tr>
<tr>
<td>Hardware Sensor (Node)</td>
<td>NOT Contributing</td>
<td></td>
</tr>
<tr>
<td>Overall Hardware Status (Node)</td>
<td>Contributing</td>
<td></td>
</tr>
<tr>
<td>Hardware Category (Node)</td>
<td>NOT Contributing</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Contributing</td>
<td></td>
</tr>
<tr>
<td>Windows Scheduled Tasks</td>
<td>Contributing</td>
<td></td>
</tr>
<tr>
<td>AppInsight for SQL Application</td>
<td>Contributing</td>
<td></td>
</tr>
</tbody>
</table>
Exclude specific entities from node status calculation

Excluding the status of specific entities, such as interfaces or applications, from node status calculation is not supported. If you do not want a child issue to participate in its parent's status, consider the following options:

- Remove the entity from monitoring.
- Unmanage the entity. For details on unmanaging interfaces, see Suspend collecting data for interfaces.
- Change the parent node's rollup mode not to be affected by this child status.
- Remove all entities of this type from participating in the node status.

Specify how to calculate node status for enhanced calculation

You have now defined the components that influence the node status calculation. Decide how to use them in the status calculation. Orion Platform uses status roll-up mode to set how the partial components of node status should be evaluated.

**Worst**

The total node status is the worst status among the configured options.

**Best**

The total node status is the best status among the configured options.

**Mixed (default option)**

The global node status combines all specified contributors.
Review the following table:

<table>
<thead>
<tr>
<th>Final Node Status</th>
<th>Polled Status</th>
<th>Child 1 Status</th>
<th>Child 2 Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRITICAL</td>
<td>UP or WARNING</td>
<td>UP</td>
<td>CRITICAL</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>UP or WARNING</td>
<td>DOWN</td>
<td>CRITICAL</td>
</tr>
<tr>
<td>DOWN</td>
<td>DOWN</td>
<td>ANY</td>
<td>ANY</td>
</tr>
<tr>
<td>WARNING</td>
<td>UP or WARNING</td>
<td>UP</td>
<td>WARNING</td>
</tr>
<tr>
<td>WARNING</td>
<td>UP or WARNING</td>
<td>UP</td>
<td>DOWN</td>
</tr>
<tr>
<td>WARNING</td>
<td>UP or WARNING</td>
<td>UP</td>
<td>UNREACHABLE</td>
</tr>
<tr>
<td>WARNING</td>
<td>WARNING</td>
<td>UP</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>WARNING</td>
<td>UP or WARNING</td>
<td>DOWN</td>
<td>WARNING</td>
</tr>
<tr>
<td>WARNING</td>
<td>UP or WARNING</td>
<td>DOWN</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>WARNING</td>
<td>UP or WARNING</td>
<td>DOWN</td>
<td>DOWN</td>
</tr>
<tr>
<td>WARNING</td>
<td>WARNING</td>
<td>UNKNOWN</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>UP</td>
<td>UP</td>
<td>UP</td>
<td>UP</td>
</tr>
<tr>
<td>UP</td>
<td>UP</td>
<td>UP</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>UP</td>
<td>UP</td>
<td>UP</td>
<td>SHUTDOWN</td>
</tr>
<tr>
<td>UP</td>
<td>UP</td>
<td>UNKNOWN</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>UNMANAGED</td>
<td>UNMANAGED</td>
<td>ANY</td>
<td>ANY</td>
</tr>
<tr>
<td>UNREACHABLE</td>
<td>UNREACHABLE</td>
<td>ANY</td>
<td>ANY</td>
</tr>
</tbody>
</table>

Child status: EXTERNAL

Change status rollup mode

By default, the status rollup mode is set to mixed. To change it, edit it in the settings for individual nodes:

1. Go to the node details page, or select the node on Manage Nodes.
2. Click Edit Node.
3. Select the status rollup mode for the node, and submit your changes.

Status Rollup Mode in the Orion Platform

In the Orion Web Console, the status rollup mode designates how the availability status of a collection of nodes on the node tree or on a map is displayed in the web console.

- Status rollup mode for network maps, groups, and tree widgets
- Child status rollup mode

Status rollup mode for maps, groups, and tree widgets

For object collections of nodes or applications with different status levels in a selected group, on a map, or in a tree widget, you can specify status rollup mode:

1. Click Settings > All Settings in the Orion Web Console, and then click Web Console Settings in the Product Specific Settings grouping.
2. Select one of the following options:

- **Show Best Status** is most useful for displaying groups that are defined as collections of redundant or backup devices. The following table indicates how the Show Best Status option operates:

<table>
<thead>
<tr>
<th>Object States</th>
<th>Group Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ] (Up, Warning, Down)</td>
<td>[ ] (Up)</td>
</tr>
<tr>
<td>[ ] (Warning, Up)</td>
<td>[ ] (Up)</td>
</tr>
<tr>
<td>[ ] (Warning, Down, Unknown)</td>
<td>[ ] (Warning)</td>
</tr>
</tbody>
</table>

- **Show Worst Status** ensures that the worst status in a group of objects is displayed for the whole group. The following table indicates how the Show Worst Status option operates:

<table>
<thead>
<tr>
<th>Object States</th>
<th>Group Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ] (Up, Warning, Down)</td>
<td>[ ] (Down)</td>
</tr>
<tr>
<td>[ ] (Warning, Up)</td>
<td>[ ] (Warning)</td>
</tr>
<tr>
<td>[ ] (Warning, Down, Unknown)</td>
<td>[ ] (Down)</td>
</tr>
</tbody>
</table>
Mixed Status shows Warning ensures that the status of a group displays the worst warning-type state in the group. If there are no warning-type states, but the group contains a mix of up and down states, then a Mixed Availability warning status is displayed for the whole group. The following table indicates how the Mixed Status shows Warning option operates:

<table>
<thead>
<tr>
<th>Object States</th>
<th>Group Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /> (Critical)</td>
</tr>
<tr>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /> (Critical)</td>
</tr>
<tr>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /> (Mixed Availability)</td>
</tr>
</tbody>
</table>

Child status rollup mode

In the Orion Platform, you can monitor child objects on single nodes, such as interfaces, applications, or other related entities. If the child entities have different status, the Orion Platform rolls the status up according to your settings.

Starting with Orion Platform 2019.2, the rollup mode depends on the method used to calculate node status:

- Enhanced node status calculation (new in Orion Platform 2019.2)
- Classic calculation
Child status rollup mode for enhanced node status calculation

If you are calculating node status using the enhanced calculation method, the status of child entities can be reflected in the overall node status.

By default, the status rollup mode is set to mixed and is calculated as shown in this table:

<table>
<thead>
<tr>
<th>Final Node Status</th>
<th>Polled Status</th>
<th>Child 1 Status</th>
<th>Child 2 Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRITICAL</td>
<td>UP or WARNING</td>
<td>UP</td>
<td>CRITICAL</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>UP or WARNING</td>
<td>DOWN</td>
<td>CRITICAL</td>
</tr>
<tr>
<td>DOWN</td>
<td>DOWN</td>
<td>ANY</td>
<td>ANY</td>
</tr>
<tr>
<td>WARNING</td>
<td>UP or WARNING</td>
<td>UP</td>
<td>WARNING</td>
</tr>
<tr>
<td>WARNING</td>
<td>UP or WARNING</td>
<td>UP</td>
<td>DOWN</td>
</tr>
<tr>
<td>WARNING</td>
<td>UP or WARNING</td>
<td>UP</td>
<td>UNREACHABLE</td>
</tr>
<tr>
<td>WARNING</td>
<td>WARNING</td>
<td>UP</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>WARNING</td>
<td>UP or WARNING</td>
<td>DOWN</td>
<td>WARNING</td>
</tr>
<tr>
<td>WARNING</td>
<td>UP or WARNING</td>
<td>DOWN</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>WARNING</td>
<td>UP or WARNING</td>
<td>DOWN</td>
<td>DOWN</td>
</tr>
<tr>
<td>WARNING</td>
<td>WARNING</td>
<td>UNKNOWN</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>UP</td>
<td>UP</td>
<td>UP</td>
<td>UP</td>
</tr>
<tr>
<td>UP</td>
<td>UP</td>
<td>UP</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>UP</td>
<td>UP</td>
<td>UP</td>
<td>SHUTDOWN</td>
</tr>
<tr>
<td>UP</td>
<td>UP</td>
<td>UNKNOWN</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>UNMANAGED</td>
<td>UNMANAGED</td>
<td>ANY</td>
<td>ANY</td>
</tr>
<tr>
<td>UNREACHABLE</td>
<td>UNREACHABLE</td>
<td>ANY</td>
<td>ANY</td>
</tr>
<tr>
<td>Child status</td>
<td>EXTERNAL</td>
<td>ANY</td>
<td>ANY</td>
</tr>
</tbody>
</table>

You can change the rollup mode for individual nodes.
Child status rollup mode for classic node status calculation

If you are calculating node status using the **classic method**, the status of child objects is displayed using a sub-icon. Specify what to display:

1. Click Settings > All Settings, and click Web Console settings.
2. Scroll down to Child Status Rollup Mode, and select one of the following options:
   - **Show Worst Status** - the child icon shows the worst status of all children.
   - **Show Worst Status (Interfaces only)** - the child icon shows the worst status of interfaces on the node
   - **Show Only ICMP status** - no child icon is displayed, because ICMP is used for node status only. The status of child entities is reported using SNMP.

**Group objects and mirror network dependencies in the Orion Web Console**

Groups and dependencies help you organize how data about your network is presented in the Orion Web Console and can improve or simplify alerts.

You can manage Orion objects such as nodes, volumes, applications, interfaces, and even other groups as groups. By using groups, you can logically organize monitored objects, and use the groups as the basis of alerts. For example, you can group nodes from the same location and create alerts and reports about the status of the group.

Dependencies between objects allow you to better represent the status of objects on your network.

Without dependencies, all monitored objects on an unresponsive monitored node report as down. By establishing dependencies, the child objects are displayed as Unreachable instead of down. This prevents false object down alerts.

**Group monitored objects**

A group is a collection of monitored objects, such as a group of nodes from the same location, or group of all nodes owned by a department.

You can include groups in other groups. For example, you can group all nodes managed by DevOps that are mission critical and then add that group to a more inclusive list of mission critical objects.

* Nesting a group within another does not create a strict parent/child relationship. You can include any group as a member in any number of other groups.*
Create groups

Select objects you want the group to contain, or specify group members using a dynamic query based on shared properties. Objects added through dynamic queries are automatically added or removed from the group.

1. Click Settings > All Settings in the menu bar.
2. In the Node & Group Management grouping, click Manage Groups.
3. Click Add New Group.
4. Click Advanced to set the Status Rollup Mode, how often objects refresh in the group, or any custom properties.
   - To create custom properties, click Manage Custom Properties in a new tab. See Custom properties in the Orion Platform.

5. Manually or automatically select objects for this group.
   - Select the check box next to the object to select object manually.
   - Automatically select group members based on shared properties by clicking Add Dynamic Query and creating conditions.
   
   - Click Preview to verify that the dynamic query is selecting the intended objects.

6. Click Create Group.

The new group is listed on the Manage Groups page and can be used in other parts of the product, including alerts and dependencies.

Edit group properties or change the group members

You can edit the properties of an existing group, or add and remove objects. If you remove an object from the group and that object has triggered an alert while it was a member of the group, the alert continues to be active until it's acknowledged.

1. Click Settings > All Settings in the menu bar.
2. In the Node & Group Management grouping, click Manage Groups.
3. Select a group you want to edit, and click Edit Properties.
4. Click Advanced to set the Status Rollup Mode, how often objects refresh in the group, or any custom properties.
   - To create custom properties, open Manage Custom Properties in a new tab.

5. To add or remove the group members, click Add & Remove Objects.
   - You can also change group members directly on the Manage Groups page.
6. Manually or automatically select objects for this group.
   - Select the check box next to the object to select object manually.
   - Automatically select group members based on shared properties by clicking Add Dynamic Query and creating conditions.

   **Click Preview to verify that the dynamic query is selecting the intended objects.**

7. Edit an existing query by selecting a dynamic query, and clicking Edit Dynamic Query.
8. To remove an object or query from a group, select the query or object, and click Remove.
9. Click Submit to save the edited objects and queries.
10. Click Submit again to save the group.

Delete groups

1. Click Settings > All Settings in the menu bar.
2. In the Node & Group Management grouping, click Manage Groups.
3. Select a group, and click Delete.

Set the group status based on the status of the group members

The status of a group is determined on the status of the group members.

The Show Best Status selection is useful for displaying groups that are defined as collections of redundant or backup devices.

<table>
<thead>
<tr>
<th>Object States</th>
<th>Group Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Up, Warning, Down)</td>
<td>(Up)</td>
</tr>
<tr>
<td>(Up, Down)</td>
<td>(Up)</td>
</tr>
<tr>
<td>(Warning, Down, Unknown)</td>
<td>(Warning)</td>
</tr>
</tbody>
</table>

The Show Worst Status selection ensures that the worst status in a group of objects is displayed for the whole group.

<table>
<thead>
<tr>
<th>Object States</th>
<th>Group Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Up, Warning, Down)</td>
<td>(Down)</td>
</tr>
<tr>
<td>(Warning, Up)</td>
<td>(Warning)</td>
</tr>
<tr>
<td>(Warning, Down, Unknown)</td>
<td>(Down)</td>
</tr>
</tbody>
</table>
The Mixed Status Shows Warning selection ensures that the status of a group displays the worst warning-type state in the group. If there are no warning-type states, but the group contains a mix of up and down states, then a Mixed Availability (◌) warning status is displayed for the whole group.

<table>
<thead>
<tr>
<th>Object States</th>
<th>Group Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="red" alt="Critical" /> <img src="red" alt="Critical" /></td>
<td><img src="red" alt="Critical" /> (Critical)</td>
</tr>
<tr>
<td><img src="red" alt="Critical" /> <img src="green" alt="OK" /> <img src="green" alt="OK" /></td>
<td><img src="red" alt="Critical" /> (Critical)</td>
</tr>
<tr>
<td><img src="green" alt="OK" /> <img src="red" alt="Critical" /></td>
<td><img src="yellow" alt="Mixed Availability" /> (Mixed Availability)</td>
</tr>
</tbody>
</table>

Mirror network object dependencies in the Orion Web Console

Dependencies are parent-child relationships between network objects that allow you to account for constraints on the network. The constraints can be the result of the design of a specific device, such as interfaces on a switch or router, or the result of the physical architecture of the network itself.

For example, all monitored objects behind an edge router are dependent on that router for connectivity. If the router has problems or goes down, any dependent devices will also appear to have problems, and you will receive status alerts about those devices as well.

However, if you define those nodes as being dependent on the edge router, you will not get false alerts about the status of dependent nodes when the parent object has issues.

When you use dependencies, consider the following:

- Dependencies themselves do not prevent alerts from being triggered. Instead, dependencies prevent the child objects from going down, and as a result, down node alerts are not triggered. By using dependencies, status alerts are prevented from triggering, but all other alerts are triggered.
- A child object can have several parents, and the child's status only turns to Unreachable if all parents in all defined dependencies go down.

Enable Auto Dependencies in the Polling Settings page to create 1:1 parent-child node dependencies automatically. You can choose to ignore dependencies created this way in the Manage Dependencies view.

Create a dependency between network objects

1. Click Settings > All Settings in the menu bar.
2. In the Node & Group Management grouping, click Manage Dependencies.
3. Click Add New Dependency.

4. Select the parent object or group, and click Next.

5. Type a Dependency Name, select the child entities, and click Next.

6. Review the settings for the dependency. If there are active alerts on child objects, they are listed on this view.

7. Click Submit.

The dependency appears on the Manage Dependencies page. This dependency can be used to limit an alert, which is then triggered only for the router that goes down, and not when a monitored device is unreachable because the router is down.

You can also display the dependency on custom views in the Orion Web Console.
Edit a dependency between network objects

Automatic Dependencies cannot be edited.

1. Click Settings > All Settings in the menu bar.
2. Click Manage Dependencies in the Node & Group Management grouping.
3. Select a dependency, and click Edit.
4. Select the parent object or group, and click Next.

   To define a dependency so that the reported states of child objects depend on the status of multiple parent objects, create a group including all parent objects, and select it on this view.

5. Select the child object or group, and click Next.

   To define a dependency so that the reported states of multiple child objects depend on the status of one or more parent objects, create a group including all child objects, and select it on this view.

6. Review the settings for the dependency. If there are active alerts on child objects, they are listed on this view. If the parent object is down, the listed alerts might be suppressed.
7. Click Submit.

Changes are saved to the dependency. Active alerts that affect members of the dependency stay active until acknowledged, even if you remove the object from the dependency.

Delete a dependency between network objects

Automatic Dependencies cannot be deleted. You can ignore them in the Manage Dependencies page.

1. Click Settings > All Settings in the menu bar.
2. Click Manage Dependencies in the Node & Group Management grouping.
3. Select the dependency, and click Delete.
4. Click Yes to confirm.

Deleted dependencies are removed from the Manage Dependencies page. The dependencies are not removed from historical logs. Active alerts that rely on the deleted dependency stay active until acknowledged.

Create dependencies between network objects automatically

You can choose to calculate dependencies automatically using the Auto Dependency feature. Auto Dependency calculates node-to-node dependencies based on topology connections. First it determines the root node of each polling engine or cluster of connected nodes. Then it determines dependencies using the root node as the base.
Since the path followed by each polling engine may be different, a unique path is created for each polling engine. When a cluster is polled by multiple polling engines, dependencies are not created between nodes that are polled by different engines even if they are topologically dependent.

Manually created dependencies are always used if there is a conflict between an automatically generated dependency.

Automatic dependencies are recalculated when topology is recalculated. Ignored dependencies continue to be ignored when your topology is recalculated.

Enable automatic dependencies

1. Click Settings > All Settings in the menu bar.
2. Click Polling Settings in the Thresholds & Polling grouping.
3. Select the Enable Auto Dependencies check box in the Calculations & Thresholds section.
4. Click Submit.

Once Auto Dependency has been enabled, dependencies are calculated immediately and are displayed within a few minutes.

View automatic dependencies

Automatic dependencies are shown along with user-defined dependencies in the All Dependencies resource and in the Manage Dependencies page. Auto dependencies are automatically named with an AutoDep- prefix.

Manage automatic dependencies

Changes made to an automatic dependency add audit events to your event log.

> Automatically calculated dependencies cannot be edited or deleted.

1. Click Settings > All Settings in the menu bar.
2. Click Manage Dependencies in the Node & Group Management grouping.
3. If Auto Dependency has been enabled, the Calculate dependencies automatically icon is toggled on.
4. Automatically calculated dependencies display Calculated Automatically in the Origin column.
5. To show only automatically calculated dependencies, select Dependency Origins from the Group by drop-down menu, and click on Calculated Automatically.

Ignore an automatically calculated dependency

1. Select the automatically calculated dependency and click Ignore Auto Dependency.
2. Click Yes, to confirm that you want to ignore the dependency.

The automatically calculated dependency is removed from the Manage Dependencies tab and displayed on the Manage Ignored Dependencies tab. The ignored dependency does not affect the child's node status.
Restore an ignored automatically calculated dependency

1. Click on Manage Ignored Dependencies.
2. Select the dependency, and click Restore Auto Dependency.

The automatically calculated dependencies is removed from the Manage Ignored Dependencies tab and displayed on the Manage Dependencies tab. The dependency is then used when calculating node status.

View active alerts on child objects when the parent object is down

When a parent object is down and the dependent child objects are Unreachable, alerts based on polled statistics are not triggered, but you can display active alerts on child objects manually.

Alerts based on default or custom property values are not affected.

If a child object can be polled using a different route, it is polled as usual. Its status does not switch to Unreachable, and alerts are not suppressed.

1. Click Settings > All Settings in the menu bar.
2. Click Manage Dependencies in the Node & Group Management grouping.
3. Select the dependency that includes the child object on which the alerts are active, and click Alerts on Child.
View events, alerts, traps, and syslogs in the Orion Web Console Message Center

The Message Center provides a view where you can see all events, alerts, traps, and Syslog messages on your network.

1. Click Alerts & Activity > Message Center.
2. To display messages for specific devices, select device properties in the Filter Devices area.
3. In the Filter Messages area, select the Time period for the messages you want to review, and provide the number of messages you want to show.
4. To show all messages, including messages that have been acknowledged, select Show Acknowledged in the Filter Messages area.
5. To display only certain types of messages, select the messages to be displayed.
6. Click Apply to update the list of displayed messages.

Filter the displayed logged events in the Web Console

Network events are logged and shown in the order they occur in the Events view of the Orion Web Console.

You can choose how long network events are kept in the Events Retention field in Orion Polling Settings under Database Settings.

1. Click Alerts & Activity > Events in the menu bar.
2. Filter events by object, event type, or time period.
3. In the Show X Events field, provide the maximum number of events to view. Showing a large number of events, such as a 1000, can negatively impact performance.
4. To show events that have already been cleared, select Show Cleared Events.
5. Click Refresh.

Remove events from the Web Console

Clearing an event removes the event from the Events view.

* Cleared events are not removed from the event log and can still be used for reporting.

1. Click Alerts & Activity > Events in the menu bar.
2. Select individual events to clear or click Select All.
3. Click Clear Selected Events.
Selected events are removed from the view. To view the events again, select Show Acknowledged, and click Apply.
Monitor hardware health

Get immediate insight into hardware issues on your network. Monitoring hardware health on Cisco, Dell, FS, HP, and Juniper devices informs you which of these devices are in Up, Warning, Critical, or Unknown states.

1. When adding a device into the SolarWinds Orion database for monitoring, enable polling hardware health statistics.
2. Hardware health statistics are polled through SNMP, from a MIB tree on your devices. For Cisco devices, make sure that the correct MIB is selected.
3. Make sure the correct sensors are enabled for the nodes.

Click here to learn about hardware health monitoring requirements in SolarWinds SAM, which involves downloading third-party agent software for supported devices.

Monitored Hardware Sensors

<table>
<thead>
<tr>
<th>Sensor</th>
<th>Up</th>
<th>Warning</th>
<th>Critical</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan status</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
<td>🍃</td>
</tr>
<tr>
<td>Power Supply status</td>
<td>🍃</td>
<td>🔴</td>
<td>🟠</td>
<td>🟠</td>
</tr>
<tr>
<td>Temperature</td>
<td>🍃</td>
<td>🟠</td>
<td>🟠</td>
<td>🟠</td>
</tr>
</tbody>
</table>

Enable hardware health monitoring

When you add nodes using Network Sonar Discovery, the hardware health sensors are enabled for devices that support hardware health monitoring automatically.

When adding individual nodes with the Add Node wizard, you can enable or disable hardware health monitoring in the wizard.

To verify that hardware health statistics are being collected, list monitored resources for the node and ensure that hardware health monitoring is enabled.
Enable monitoring from the Add Node wizard

When selecting resources for monitoring a node in the Add Node wizard, select the Hardware Health Sensors box to enable hardware health monitoring.

Enable hardware health monitoring on a node

1. Click My Dashboards > Home in the Orion Web Console.
2. In the All Nodes resource, click the node you want to monitor.
3. In the Management resource on the Summary tab of the Node Details view, click List Resources.
4. Make sure the Hardware Health Sensors box is selected, and click Submit.

Hardware health statistics for enabled hardware sensors are collected for the node.

Enable, disable, or adjust hardware health sensors

To view all currently monitored sensors, click Settings > All Settings, and in the Node & Group Management grouping, select Manage Hardware Sensors. By default, all sensors available in the selected MIB are monitored on devices with enabled hardware health monitoring.

On the Manage Hardware Health Sensors page, you can enable or disable polling on individual sensors, or change hardware health thresholds.
Use the Group By options to filter available hardware sensors. These options include the Vendor, Parent (or node), Product Line, Sensor Category, Last Status, Enabled, and Custom Threshold Defined. You have the following options:

- Update hardware health statistics
- Enable and disable hardware sensors

### Update hardware health statistics

All changes are applied in the Orion Web Console with the next poll. Look up the current polling interval, and if necessary, poll for the statistics manually.

1. Click Settings > All Settings, and click Polling Settings in the Thresholds & Polling grouping.
2. Scroll down to Hardware Health Polling section, and note the Default Statistics Poll Interval.

   - We recommend that you do **NOT** enter a shorter polling interval here because it might affect the polling performance. To immediately update hardware health statistics for a node, see step 3.
   - Consider how often you need to update the health statistics and how long you need to keep historical records. To improve the performance, enter a longer polling interval, or shorten the retention periods.

3. Go to the node details view, and click Poll Now in the Management resource.

Hardware health statistics will be immediately updated. This will not affect the performance as if you shortened the polling interval.

### Enable hardware sensors

Hardware health information is collected only for nodes where the hardware sensors are enabled.

1. Go to Manage Hardware Sensors view (Settings > All Settings > Node & Group Management > Manage Hardware Sensors).
2. Find the sensor(s) you want to enable. You can either use the Group by pane, or use the Search box.

To find all sensors available on a node, select Node in the Group by list, and then select the node.

3. Select the sensor that you want to enable on the node, and click Enable.

Hardware health information for the selected nodes will be collected now.

**Disable hardware sensors**

If you do not want to collect specific hardware health information or any hardware health information, disable sensors.

1. Go to Manage Hardware Sensors view (Settings > All Settings > Node & Group Management > Manage Hardware Sensors).
2. Find the sensor(s) you want to enable. You can either use the Group by pane, or use the Search box.

To find all sensors available on a node, select Node in the Group by list, and then select the node.

3. Select the sensor(s) which you want to disable on the node, and click Disable.

Hardware health statistics for the selected sensors on the selected nodes will not be collected now.

**Edit hardware health thresholds**

Hardware states displayed in the Orion Web Console change based on thresholds set for the sensors. You can either use thresholds available on the device, set a sensor to always appear to be up, or customize thresholds.

When values polled on a node reach the threshold value, an event triggers together with the alert "Hardware is in warning or critical state."

1. Go to Manage Hardware Sensors view (Settings > All Settings > Node & Group Management > Manage Hardware Sensors).
2. Select the sensor that you want to edit, and click Edit Thresholds.

To find all sensors available on a node, select Node in the Group By list, and select the node.

3. Select how you want to change the selected hardware sensor's status:

   **Use Orion Defaults**
   
   Use thresholds configured on the device. This is the default setting.

   **Force to Up**
   
   If you are not concerned about a sensor, select this option. The sensor will always be displayed as UP, ignoring the real data from the sensor.
Set Custom Thresholds

Use the dynamic query builder to define the status for the selected sensor.

4. Click Submit.

The status of the hardware health sensor will now be governed by the specified threshold.

Change the MIB used for polling hardware health statistics

Hardware sensors information on Cisco devices can be polled using one of the following MIBs.

- CISCO-ENTITY-SENSOR-MIB (default MIB)
- CISCO-ENVMON-MIB

Each MIB contains different OIDs, and information for individual nodes might be included only in one of them. If you see inconsistencies between the actual hardware health and the status shown in the Orion Web Console, change the MIB used for polling hardware health statistics.

Change the MIB tree used for polling hardware health globally

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Thresholds & Polling grouping, click Polling Settings.
4. Scroll down to the Hardware Health Polling section, and select the MIB in the Preferred Cisco MIB list.
5. Click Submit.

The default MIB used for polling all hardware sensors on all monitored nodes is changed now.

Change the MIB for polling hardware health statistics on a specific node

1. Open the Node Details view, and click Edit Node in the Management resource.
2. Scroll down to the Hardware Health Polling section, and select the MIB.
3. Click Submit.

Changing MIB for a node overrides the general settings. Once you customize the MIB for polling hardware health sensors, it will not change if you change the general settings.

Change hardware health temperature units

By default, hardware health resources display temperature in degrees Fahrenheit.

1. Log in to the Orion Web Console.
2. Navigate to a node details view.
3. Go to the Current Hardware Health resource, and click Edit.
4. Select the unit for temperature display (Fahrenheit or Celsius).
5. Click Submit.

The selected unit will be applied in all hardware health resources in the Orion Web Console. This setting is user-specific, and it is connected with your user account.

You can also access the temperature unit setting when editing a user in the Hardware Health Package Settings.
Monitor Hardware Health for Nutanix appliances

RC Documentation: The following content is draft content for a SAM Release Candidate. All content is subject to change. Please note that some links to external docs may not function yet.

The Nutanix™ enterprise cloud platform is a scale-out, hyperconverged system of high-performance nodes, or servers, each running a standard hypervisor with processors, memory, and local storage. Each Nutanix node runs VMs like a standard VM host and includes a Controller VM (CVM) capable of polling local storage from all nodes in the cluster. The environment is hypervisor-agnostic; nodes can run their own hypervisors while also running hypervisors from vendors such as VMware®.

With the Hardware Health monitoring functionality in the Orion Platform, you can:

- Get Hardware Health data for hosts associated with monitored Nutanix clusters.
- Display Nutanix Hardware Health data in the AppStack Environment.
- Use alerts and reports for Nutanix objects.

Note the following details about Nutanix Hardware Health monitoring:

- The default polling frequency is 10 minutes.
- The Nutanix Prism™ Central management not tool is not supported.
- If you delete a Nutanix cluster, the Orion Platform stops updating Hardware Health data but child nodes, such as VMware hypervisors, remain visible in the Orion Web Console.
- If Hardware Health data for ESXi devices is also gathered via VCenter, Common Information Model (CIM) and VCenter API polling take precedence over Nutanix polling.
- Hardware Health monitoring for Nutanix differs from the workflow that uses a Universal Device Poller (UnDP) described here.

To get started with Hardware Health monitoring for Nutanix appliances:

1. Review requirements.
2. Add Hyper-V or VMware nodes for monitoring. Click here for details.
3. Add your first Nutanix cluster, as described in Set up Hardware Health monitoring for Nutanix appliances.

After you add a Nutanix cluster, navigate to the Virtualization - Summary page to display details about it. You can also configure alerts and reports for Nutanix appliances. If you run into issues, see Troubleshoot Nutanix Hardware Health monitoring.
Nutanix Hardware Health monitoring requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td><strong>SAM 2019.4 or VMAN 2019.4</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Acropolis™ (AOS) 5.10 and 5.11</strong></td>
</tr>
<tr>
<td>Hypervisors</td>
<td><strong>Microsoft® Hyper-V</strong></td>
</tr>
<tr>
<td></td>
<td><strong>VMware vSphere®</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Nutanix Acropolis HyperVisor (AHV)</strong></td>
</tr>
<tr>
<td>Credentials</td>
<td>Collect Nutanix credentials for AHV nodes, as well as Hyper-V and VMware child nodes.</td>
</tr>
<tr>
<td></td>
<td>Controller VM (CVM) credentials require privileges to connect via SSH to hosts and execute Nutanix Cluster Check (NCC) commands.</td>
</tr>
<tr>
<td>API access</td>
<td>The Orion Platform main polling engine or Additional Polling Engine (APE) — whichever polls the node — must have access to the Nutanix AOS API (© 2019, Nutanix, available at <a href="https://portal.nutanix.com">https://portal.nutanix.com</a>, obtained on September 10, 2019).</td>
</tr>
<tr>
<td></td>
<td>The Orion Platform uses a combination of AOS API v1 and v2.</td>
</tr>
<tr>
<td></td>
<td><strong>Did you know that SAM now includes an API Poller feature?</strong> Click here for details.</td>
</tr>
<tr>
<td>Subnet</td>
<td>All CVMs and hypervisor hosts must be on the same subnet. A hypervisor can be multi-homed as long as one interface is on the same subnet as the CVM. If the Intelligent Platform Management (IPMI) interfaces are connected, they should be on the same subnet as CVMs and hypervisor hosts.</td>
</tr>
<tr>
<td></td>
<td>Guest VMs can be on a different subnet.</td>
</tr>
</tbody>
</table>

For a comprehensive list of port requirements for Orion Platform products, see SolarWinds Port Requirements.

Set up Hardware Health monitoring for Nutanix appliances

**Before you begin**, add Hyper-V or VMware nodes for monitoring. Click here for details.

Configuring Hardware Health monitoring for Nutanix appliances involves adding the Nutanix cluster with the Add Node wizard, and then providing CVM credentials for the cluster.
To add a Nutanix cluster:

1. Click Settings > All Settings, and then click Add Node.
2. On the Add Node page, enter the IP Address:
3. For the Polling Method, select VMware, Hyper-V or Nutanix entities, and then click Next.
   The Add a Virtual Object for Monitoring page appears.

4. Select Nutanix Cluster and then click Next.
5. Provide credentials on the Polling & Credentials tab.
6. Click Next to test credentials and advance to the Metrics tab.

7. Review your information, click Finish to close the window, and then click OK, Add Node.
To provide CVM credentials for a Nutanix cluster:

- CVM credentials require privileges to connect via SSH to the device and execute Nutanix Cluster Check (NCC) commands.

1. Navigate to All Settings > Virtualization Settings.
2. Click Nutanix Settings to open the Virtualization Polling Settings page.

3. Select the cluster and then click Assign CVM Credentials.
4. In the Assign Credentials dialog box, you can either:
   - Select an existing credential, or
   - Click New credential, and then provide:
     - Credential Name
     - User Name
     - Password (enter twice to confirm)
5. Click Assign to test credentials.

When finished, wait ten minutes for polling to complete.
Display Hardware Health data for Nutanix appliances

To display Hardware Health data for Nutanix appliances, navigate to the Virtualization - Summary page. Then you can drill down into individual child nodes to display additional information.

![Virtualization Summary](image)

Manage alerts and reports for Nutanix appliances

You can use Hardware Health sensor events to configure alerts related to Hardware Health monitoring for Nutanix appliances. Define thresholds on the Manage Sensors page like you do for other device types.

Nutanix events only appear in the Add New Alert wizard if the filter is set to All Events; they do not appear if you select a specific event type, such as Hardware Sensor Warning. To learn more about alerts, see Use alerts to monitor your environment with the Orion Platform.

The following reports support Nutanix devices:

- HardwareHealth: Current Hardware and Hardware Sensors Status
- HardwareHealth: Hardware Health Power Consumption Cost Calculations
- HardwareHealth: Historical Hardware Sensor Daily Availability
- HardwareHealth: Historical Hardware Sensor Statistic

To learn about creating reports, see Manage and view reports in the Orion Platform.
Understand Hardware Health sensor status mapping

The following table describes about how Nutanix hardware health sensor status translates to the Orion Platform.

<table>
<thead>
<tr>
<th>Nutanix status</th>
<th>Description</th>
<th>Orion Platform status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cr</td>
<td>critical</td>
<td>Critical</td>
</tr>
<tr>
<td>nc</td>
<td>non-critical</td>
<td>Warning</td>
</tr>
<tr>
<td>nr</td>
<td>non-recoverable</td>
<td>Critical</td>
</tr>
<tr>
<td>ok</td>
<td>OK</td>
<td>Up</td>
</tr>
<tr>
<td>ns</td>
<td>non-specified</td>
<td>Unknown</td>
</tr>
<tr>
<td>PSU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Present, OK</td>
<td>PSU is present.</td>
<td>Up</td>
</tr>
<tr>
<td>CPU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Populated</td>
<td>CPU is present.</td>
<td>Up</td>
</tr>
<tr>
<td>Empty</td>
<td>CPU is not present.</td>
<td>Unknown</td>
</tr>
<tr>
<td>Populated, Disabled</td>
<td>CPU is present but disabled.</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

If the Nutanix API does not provide a sensor status, the Orion Platform sets the status to Unknown and that value can be modified by custom thresholds.

Troubleshoot Nutanix Hardware Health monitoring

This topic describes issues you may encounter when monitoring Hardware Health for Nutanix appliances. You can also search for troubleshooting tips in the SolarWinds Success Center and our online IT community, THWACK.

Be sure to review Nutanix Hardware Health monitoring requirements.

Issue: Hardware Health data is not updated and the last polling time has not changed.

Querying a Nutanix cluster from multiple sources can cause Nutanix Cluster Check (NCC) locks that prevent the Nutanix API from returning data to the Orion server. This can occur if:

- A Nutanix ncc hardware_info command (for example, ncc hardware_info show_hardware_info) was run against a manually connected CVM device.
- Two Orion instances are monitoring the same Nutanix cluster.

Polling can also fail if a Nutanix device automatically fires an Update command to refresh sensors.
Issue: Many Nutanix values appear as UNKNOWN in Hardware Health widgets.

The Orion Platform gathers available data from the Nutanix API. If a specific data set is not available, it appears as UNKNOWN in Hardware Health widgets.

Issue: I can't find Nutanix hardware sensor events.

Nutanix hardware events only appear in the Alert Manager if the filter is set to All Events when configuring alerts. They don't appear if you select a specific Event Type such as Hardware Sensor Warning.

Issue: Some nodes appear twice in Summary widgets.

Nutanix is hypervisor-agnostic. It has proprietary hypervisors, but also supports hypervisors from other vendors such as VMware. As a result, you may see "child" records repeated as parent records in some widgets, similar to those shown in the following example:
Monitor Cisco UCS devices in the Orion Platform

The Cisco® Unified Computing System (UCS) is designed to provision, migrate, and manage internetworking systems in data centers.

When you add a UCS controller as a parent node in the Orion Platform and then add devices such as fiber interconnects, chassis, blades, and rack servers to create a UCS cluster, you gain a view to all information that UCS provides.

You can then:

- Set up polling to check the health of UCS devices.
- Manage Hardware Health sensors for UCS controllers and related servers.
- Display chassis status in the AppStack Environment and Orion Maps.
- Access the Cisco UCS Manager web portal page for a device from its Orion node.

To begin monitoring UCS devices, review requirements and then:

- Add a node for a UCS controller via the Discovery wizard,
- Add a node for a UCS controller on the Manage Nodes page, or
- Enable UCS monitoring on an existing node on the Edit Node page.

To learn more about monitoring UCS devices, see:

- UCS device monitoring requirements
- Set up monitoring for UCS devices
- Add nodes for devices connected to UCS controllers to the Orion Platform
- Manage alerts and reports for UCS devices in the Orion Platform
- Troubleshoot UCS device monitoring in the Orion Platform

To ensure that MachineType and other device values are not overwritten when polled data is saved to the database, the Orion Platform uses EntityType to identify UCS nodes. The EntityType column in the Orion database is also used for polling by the ESX VMWare API.

UCS device monitoring requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAM 6.8 or VMAN 8.4</td>
<td>If running earlier product versions, upgrade to extend monitoring capabilities for UCS devices.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Details</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Polling method</td>
<td>Use ICMP or SNMP for UCS devices. SolarWinds recommends using the &quot;Most Devices: SNMP and ICMP&quot; polling option to gather data from UCS controllers, chassis, blades, and rack servers.</td>
</tr>
<tr>
<td></td>
<td>For fabric interconnects, the polling method must be SNMP. All SNMP versions are supported.</td>
</tr>
<tr>
<td>Cisco UCS Manager credentials</td>
<td>The credentials used to access the UCS Manager web portal and monitor B-series blade servers.</td>
</tr>
<tr>
<td>UCS listening port</td>
<td>The port on which the UCS Manager listens to UCS devices, as configured in the UCS Manager web portal. Default values are 80 for HTTP and 443 for HTTPS.</td>
</tr>
<tr>
<td>API access</td>
<td>The Orion Platform main polling engine or Additional Polling Engine (APE) — whichever type polls the node — must have access to the UCS API.</td>
</tr>
<tr>
<td>Fabric interconnects</td>
<td>Verify that fiber interconnects have external IP addresses. If the external gateway, external IP address, or external mask are set to 0.0.0.0, update the IP address.</td>
</tr>
<tr>
<td></td>
<td>1. Log into the Cisco UCS Manager web portal</td>
</tr>
<tr>
<td></td>
<td>2. Provide external IP addresses for the external gateway, external IP address, or external mask.</td>
</tr>
</tbody>
</table>

**Set up monitoring for UCS devices**

To gain an overview of all information provided by UCS, add the parent UCS controller to the SolarWinds Orion database. Afterward, you can add connected UCS devices, such as fiber interconnects, chassis, rack servers, and blade servers, to create a UCS cluster.

Review **UCS monitoring requirements** before adding nodes.

To add a node to monitor a parent UCS controller in the Orion Platform:

1. Log into the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes, and then click Add Node.
3. On the Add Node page, provide the IP Address, or provide the host name and select Dynamic IP Address.
4. Select an ICMP polling method and provide credentials. To gather maximum UCS data, select Most Devices: SNMP and ICMP as the Polling Method.
5. Select the UCS Manager Credentials check box.
6. Provide UCS credentials information, including the port on which the UCS Manager listens:
   - Port
   - Use HTTPS
   - User Name

   ![Tip](Image)
   If you have trouble with the User Name, try prepending it with "ucs-".

   - UCS Password

7. Click Test to verify credentials, and then click Next.
8. On the Choose Resources page, select the resources and statistics you want to monitor, and then click Next.
9. Advance to the Add Pollers and Change Properties pages to add relevant pollers and adjust node properties.
10. Review your information, and click OK, Add Node.

After adding a node for the parent UCS controller, navigate to its Node Details page and click the Hardware icon in the left menu to access the Hardware subview. Double-click child UCS devices in the Overview widget and begin managing them as nodes to monitor a UCS cluster in the Orion Platform. See Add nodes for devices connected to UCS controllers to the Orion Platform for details.

### Add nodes for devices connected to UCS controllers to the Orion Platform

![Tip](Image)
You need Node Management rights to add UCS devices. See Define what users can access and do.

1. Navigate to the Node Details page for the parent UCS controller.
2. Click the Hardware icon in the left menu to access the Hardware subview.
3. Click a fabric interconnect, blade, or rack server in the Overview widget.

If the device is already managed by the Orion Platform, its Node Details page appears. Otherwise, the following dialog box appears:

4. Click OK to open the Add Node wizard, where the device IP address is automatically populated.
5. Follow the onscreen prompts to complete the Add Node wizard.

To gather maximum UCS data, select Most Devices: SNMP and ICMP as the Polling Method for chassis, rack servers, and blade servers.

For UCS fabric interconnects, the polling method must be SNMP.

6. Repeat steps for additional devices in the UCS cluster, as necessary.

Manage alerts and reports for UCS devices in the Orion Platform

SolarWinds provides predefined alerts and reports for UCS devices that you can configure and customize in the Orion Web Console.
UCS device alerts

The following preconfigured alert is automatically enabled for all monitored UCS devices with hardware sensors:

- Chassis sensor is in warning or critical state

To view all currently monitored sensors, click Settings > All Settings, and then click Manage Hardware Sensors in the Node & Group Management grouping. In SAM and NPM, you can also enable, disable, or adjust hardware health sensors.

You can configure alerts for UCS devices using any Hardware Health BMC or Hardware Sensor trigger condition, as well as the following UCS-specific trigger conditions:

- UCS Blades
- UCS Chassis
- UCS Fabrics
- UCS Fans On Chassis
- UCS Fans On Fabrics
- UCS PSUs On Chassis
- UCS PSUs On Fabrics

UCS device reports

The Orion Platform includes the following out-of-the-box reports for UCS devices that you can use to view trends, establish baselines, or identify potential issues.

- Current – Hardware Health BMC Sensors
- Current – Hardware Health BMC Sensors with Problems

The Original Status column in both reports displays values that come directly from UCS sensors, as they appear in the UCS Manager web portal. Orion statuses are represented by colored icons on reports.

Troubleshoot UCS device monitoring in the Orion Platform

This topic describes about issues you may encounter when monitoring UCS devices in the Orion Platform. For additional troubleshooting information, visit the SolarWinds Success Center and our online IT community, THWACK.

Be sure to review UCS device monitoring requirements.

Issue: Polling does not return data for UCS fabric interconnects.

Verify the following items:
Make sure a child node for the fabric interconnect exists beneath the parent node for the UCS controller. See Add nodes for devices connected to UCS controllers to the Orion Platform.

For fabric interconnects, the polling method must be SNMP.

Verify that fiber interconnects have external IP addresses. If the external gateway, external IP address, or external mask are set to 0.0.0.0, update the IP address.

The Orion Platform main polling engine or Additional Polling Engine (APE) — whichever polls the UCS cluster — must have access to the UCS API.

Issue: When setting up a UCS blade as a node in the Orion Platform, you select the Operating System Interface but no change occurs.

As you add a node for a UCS blade, you must specify which network interface to use to monitor the blade:

- **Management Interface:** Use the Management Interface to monitor the blade. When you add the node, the IP address automatically populates with information captured from the parent BMC controller during SNMP polling.

- **Operating System Interface:** Use this method to monitor the blade via its build-in operating system that returns a broader range of data, such as hardware health. To add the node, you'll need to provide its IP address because polling occurs in a layer of the OSI model that does not capture IP addresses.

If you select the Operating System Interface option but no change occurs, the blade probably has existing connections to other Orion Platform entities based on its IP address, as configured in the following product versions:

- NPM 12.4 and earlier
- SAM 6.7.1 and earlier
- VMAN 8.3 and earlier

If the blade was already associated with other nodes in earlier product versions, you cannot switch the network interface used for the blade from the Management interface to the Operating System interface. This logic preserves existing node connections that are based on the blade IP address provided by the Management interface.

To work around this functionality, remove the blade node from the Orion Platform and then add it back again.

Issue: Users want to be warned when certificate errors occur.

By default, the Orion Platform is configured to ignore certificate errors when monitoring UCS devices. You can update that setting on the Global tab of the Advanced Configuration page in the Orion Web Console, if necessary.

Before proceeding, note the following details about this functionality:

- Generally, you should not modify any Advanced Configuration settings unless instructed to do so from a KB article or the direction from the SolarWinds Support team.
- The IgnoreCertificateErrors settings applies only to nodes for which the Cisco UCS Manager is added via HTTPS.
To configure UCS device monitoring so users are prompted to validate untrusted connections, follow these steps:

1. Log into the Orion Web Console as an administrator.

2. In the address field of the web browser, enter:
   
   http:// (your host name)/Orion/Admin/AdvancedConfiguration/Global.aspx : Global tab

3. When the Advanced Configuration page opens, clear the IgnoreCertificateErrors check box for UCS.Settings.

4. Use the Orion Service Manager to restart the following services:
   
   - SolarWinds Collector Service
   - SolarWinds Orion Module Engine
Monitor cloud instances and VMs

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.

Using the Cloud Infrastructure Monitoring feature with Orion Platform products such as SolarWinds SAM and VMAN provides several benefits, including the ability to:

- Manage hybrid environment metrics and status through a single console. Displaying on-premises, virtual, and cloud systems together helps you compare performance, locate bottlenecks, and better plan capacity and resource allocation.
- Track end user and business context for performance by using SAM to gather 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.

To enhance cloud monitoring, configure cloud instances/VMs as managed nodes in the Orion Platform so that you can:

- Poll specific metrics beyond the basic metrics gathered by cloud service APIs, including OS, memory, and other detailed metrics retrieved by SAM application monitors.
- Use SAM application monitors and templates to poll applications deployed in the cloud.
- Display cloud instance/VM details in AppStack for quick troubleshooting across your environment.
- Develop and deploy custom script monitors for PowerShell, Nagios, Linux/UNIX, and Windows.
- Assign Custom Properties to nodes.

To learn more, see Manage a cloud instance/VM as an Orion Platform node.
Cloud monitoring recommendations

For optimal performance, SolarWinds recommends the following limits for cloud monitoring:

- Up to 10 cloud service accounts
- Up to 1,000 instances/VMs to monitor
- Up to 1,000 volumes to monitor
- Up to 1,000 instances/VMs managed as nodes
- Up to 1,000 Orion agents deployed on managed nodes

Before exceeding recommended limits, consider the impact on polling load, costs incurred due to API request overages, and the possible need to expand hardware, CPU resources, memory, etc.

Cloud monitoring requirements

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor AWS cloud metrics</td>
<td>An <a href="https://aws.amazon.com">AWS account configured for cloud monitoring</a> You will need the following <a href="https://aws.amazon.com/credentials">credentials</a> to add an account to the Orion Platform or <a href="https://www.solarwinds.com">deploy Orion agents</a> to instances:</td>
</tr>
<tr>
<td></td>
<td>- Access Key ID</td>
</tr>
<tr>
<td></td>
<td>- Secret Access Key</td>
</tr>
<tr>
<td>Monitor Azure cloud metrics</td>
<td>An <a href="https://azure.microsoft.com">Azure account configured for cloud monitoring</a> You will need the following <a href="https://azure.microsoft.com/credentials">credentials</a> to add an account to the Orion Platform or <a href="https://www.solarwinds.com">deploy Orion agents</a> to VMs:</td>
</tr>
<tr>
<td></td>
<td>- Subscription ID</td>
</tr>
<tr>
<td></td>
<td>- Tenant/Directory ID</td>
</tr>
<tr>
<td></td>
<td>- Client/Application ID</td>
</tr>
<tr>
<td></td>
<td>- Application Secret Key</td>
</tr>
</tbody>
</table>

- The Orion server must be [configured to communicate with public services](https://www.solarwinds.com) to collect data from cloud service APIs. Use the default setting — public — in community strings for polled devices to allow read access.

After you [configure a cloud account](https://www.solarwinds.com) and [add an initial cloud account](https://www.solarwinds.com) to the Orion Platform, cloud services start polling for metrics, as displayed on the Cloud Summary page in the Orion Web Console. See Explore cloud instances and VMs on the Cloud Summary page.
Cloud metrics vs. OS metrics

Cloud services APIs, such as the Amazon CloudWatch API and Azure Rest API, capture basic metric data for instances/VMs and volumes so you can allocate resources as needed, such as partial CPU processing and disk space across multiple instances/VMs. These resources can change through direct interactions and automation. For example, when the Amazon EC2 web service reports data to the Orion Platform, it calculates the percentage of assigned resources shared between instances.

Cloud metrics differ with OS metrics due to the fluid nature of cloud computing. OS metrics directly capture values from the core system, not the assigned amounts. This data does not calculate shared resources or other users attached to the instances and volumes. This data directly displays the actual usage at a polled point in time.

Both cloud metrics and OS metrics provide insight into potential and actual issues with performance and resources. Metrics report vastly different information to the cloud and OS based on allocated resources and metric calculations.

CPU steal is an example of cloud vs. OS metrics. When CPU usage and metrics spike in a cloud environment, multiple processes and instances/VMs in the cloud may access the CPU as multiple owners. Typically, OS metric spikes tend to look like noisy neighbors. The cloud metric data better represents the data as shared resources usage across multiple owners with metrics broken down by owner.

To better define resource usage and alerts, SAM and integrated VMAN display cloud instance/VM metrics throughout all cloud resources in Orion Web Console views, resources, hover-over data, and reports. Cloud metrics, including calculated health status, CPU load, and IOPS data, are used to apply global cloud thresholds that trigger alerts and status changes. For a list of cloud metrics gathered by cloud service APIs, see the table included in the Edit global thresholds for cloud monitoring topic.

For instances and VMs managed as nodes, the Orion Platform pulls specific OS data for memory and provides additional data through Orion agent, WMI, and SNMP polling methods.

Learn more

In addition to the Orion Platform Administrator Guide, check out these resources to learn more about cloud monitoring with SolarWinds products:

- Deploy SolarWinds Orion Platform products to Amazon Web Services
- Deploy SolarWinds Orion Platform products to Microsoft Azure
- Monitoring Azure PAAS with SolarWinds SAM (THWACK)
- SolarWinds Lab Episode #60: SolarWinds Cloud, GO! Learn Modern Monitoring for Apps, Cloud & DevOps
- SolarWinds Lab #72: Two Geeks and a Goddess II: Azure the Easy Way

Add the first cloud account to the Orion Platform

To get started with cloud monitoring, add a cloud account to the Orion Platform.
Before proceeding, make sure the **cloud account is configured for the Orion Platform**. Be sure to have your **cloud account credentials** handy.

1. Log into the Orion Web Console.
2. Click My Dashboards > Cloud to access the Cloud Summary page.
3. In the Getting Started resource, click Monitor my Cloud Instances.

![Monitor My Cloud Instances](image)

4. Select a Cloud Service Provider.

![Add Cloud Account](image)

5. Click Monitor AWS or Monitor Azure, depending on which provider you selected.
6. On the Cloud Settings tab, enter a Display Name for the account and provide **account credentials**.
7. If the SolarWinds Orion server requires a proxy server to connect to certain websites, click "Are you behind a proxy?" to **configure proxy settings**.
8. (Optional) Click Test Connection.

   ![Tip](image)

   If an error occurs, verify account credentials and confirm that accounts are **configured for the Orion Platform**.

9. (Optional) Toggle Auto Monitoring off for instances/VMs added later, either manually or via automated discovery.
10. Click Continue to complete the wizard.

   ![Tip](image)

   To learn more about wizard options, see **Add a Cloud Account**.
Working in the Cloud Summary page

After an account is added, the Orion Platform begins polling for data. Click Dashboards > Cloud to display the Cloud Summary page and review instances/VMs for the new account.

💡 If necessary, you can restrict other Orion Web Console users from displaying instances/VMs for an account.

Hover over the name of a cloud instance/VM to display more details about it.
If an instance/VM is a managed node, additional data, such as CPU usage and packet loss, displays.

The Cloud Summary page displays a variety of data. Use the Search Instances field to find instances/VMs and volumes quickly. Click hyperlinks to access more details quickly. Hover over points to compare collected data and linked alerts.

- The **Cloud Instances Status Summary** shows various metrics. Values that exceed thresholds are colored to indicate warning (orange) and critical (red) values.
- The **Cloud Asset Summary** displays totals for instances/VMs, attached volumes, and storage capacity, grouped by cloud service provider.
- The **Cloud Server Infrastructure** section groups instances/VMs by cloud account and region.
- The **Active Cloud Alerts** section lists unacknowledged alerts currently affecting cloud instances/VMs.
- The **Cloud Applications with Problems** section lists applications with issues on cloud instances managed as nodes in SAM.
- The **Cloud Volumes Performance** section includes various volume-related metrics.

To track performance and usage trends, you may want to focus on the following resources:

- **Active Alerts** lists 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.
Explore cloud instances and VMs on the Cloud Summary page

To quickly review status and metrics for your cloud infrastructure, cloud instances and VMs in the Orion Web Console, click Dashboards > Cloud to display the Cloud Summary page. You can also use this page to drill down and display specific details about a cloud instance or VM.

Use the Search Instances field to find instances and VMs quickly. Click hyperlinks to access more details and hover over points to compare collected data and linked alerts.

- The Cloud Instances Status Summary shows various metrics. Values that exceed thresholds are colored to indicate warning (orange) and critical (red) values.
- The Cloud Asset Summary displays totals for instances/VMs, attached volumes, and storage capacity, grouped by cloud service provider.
- The Cloud Server Infrastructure section groups instances/VMs by cloud account and region.
- The Active Cloud Alerts section lists unacknowledged alerts currently affecting cloud instances/VMs.
- The Cloud Applications with Problems section lists applications with issues on cloud instances managed as nodes in SAM.
- The Cloud Volumes Performance section includes various volume-related metrics.
To review the status and metrics for a specific cloud instance/VM, hover over the name of cloud instance/VM to display details about it.

To track performance and usage trends, you may want to focus on the following resources:

- **Active Alerts** lists active alerts affecting the cloud instance/VM.
- **Min/Max/Average of Average CPU load** displays average CPU load collected and calculated for the cloud instance/VM.
- **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/VM for a custom period of time.

**Configure cloud accounts for the Orion Platform**

Before adding a cloud account to the Orion Web Console, AWS and Azure must be configured to interact with the Orion Platform, as described in:

- [Configure AWS for cloud monitoring](#)
- [Configure Microsoft Azure for cloud monitoring](#)

**Configure AWS accounts for cloud monitoring**

Before adding AWS accounts to the Orion Platform, IAM permissions must be configured in the AWS Management Console to provide access to the Orion Platform so it can collect status and metrics for AWS instances.

To integrate the AWS cloud service with the Orion Platform, Identity and Access Management (IAM) permissions must be configured and IAM policies must be [assigned to AWS accounts](#), as described next. Consult your system administrator and refer to [AWS documentation](https://docs.aws.amazon.com) for details (© 2019 Amazon Web Services, Inc., available at [https://docs.aws.amazon.com](https://docs.aws.amazon.com), obtained on January 21, 2019).

**Establish AWS IAM permissions**

To interact with the Orion Platform, an AWS account must be able to retrieve CloudWatch metrics from various resources. Use this section as a reference for specific permissions.

![New York](image)

---

Although you can embed inline policies to set permissions, SolarWinds recommends attaching an IAM policy to an account so JSON code can be used to permit or restrict user actions.
Each AWS account requires the following resource-level permissions:

- ec2:DescribeInstances
- ec2:DescribeAddresses
- ec2:DescribeVolumes
- ec2:DescribeVolumeStatus
- cloudwatch:GetMetricStatistics
- autoscaling:DescribeAutoScalingInstances

To define actions that can be performed against an instance, add the following permissions:

- ec2:StartInstances
- ec2:StopInstances
- ec2:RebootInstances
- ec2:TerminateInstances

The following JSON code provides standard access to an Orion Platform user:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeAddresses",
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumeStatus",
                "cloudwatch:GetMetricStatistics",
                "autoscaling:DescribeAutoScalingInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

Add an IAM policy to AWS accounts

These steps describe how to create an AWS IAM policy to attach to AWS accounts.

1. Log into the AWS Management Console and open the IAM console.
2. Click Policies.
3. If this is your first time adding Policies, the Welcome page appears. Click Get Started.
4. Click Create Policy.
5. On the Create Policy page, click Select > Create Your Own Policy.
6. Enter policy details, such as name and description.
7. To enter policies in a policy editor, add the following permission statements to the Policy Document:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeAddresses",
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumeStatus",
                "cloudwatch:GetMetricStatistics",
                "autoscaling:DescribeAutoScalingInstances",
                "ec2:StopInstances",
                "ec2:StartInstances",
                "ec2:RebootInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*
        }
    ]
}
```

8. Click Validate Policy.
9. Click Create Policy.

To attach the policy to an account:

1. In the AWS Management Console, click Policies.
2. Navigate to the policy and selects its check box.
3. Click Policy Actions > Attach.
4. Select the All Types option and Users.
5. Navigate to the account and selects its check box.
6. Click Attach Policy.

Configure Microsoft Azure for cloud monitoring

Before adding an Azure cloud account to the Orion Web Console, Azure must be configured to interact with the Orion Platform. An account must have 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. Identity and Access Management (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 tips about setting up an Azure AD app and IAM permissions.
While using the Azure Portal, record credentials needed to add Azure accounts in the Orion Web Console. See Find cloud account credentials for details.

Cloud service polling overview

Cloud service APIs poll instances/VMs and volumes regularly to monitor details about resources, such as status, volume IDs, subnet IDs, memory usage, CPU usage, and IP addresses.

The Orion Platform sends API requests (also known as "calls") to cloud services to retrieve status and metric data used to monitor resources, trigger notifications, track system health, and more. Third-party products and custom code may also send API requests for various purposes.

Note these details about cloud service polling:

- AWS and Azure both provide 1 million free API requests per calendar month. If free polling limits are exceeded, cloud accounts are charged for extra requests within the remaining time frame. See AWS polling and Azure polling.
- Cloud metrics gathered by cloud service APIs and retrieved by the Orion Platform vary from OS metrics, as described next.

To avoid exceeding polling limits, consider toggling Auto Monitoring off when adding a cloud account to block polling for new instances/VMs launched and then discovered for an account. You can enable monitoring for individual instances/VMs later.

Cloud metrics vs. OS metrics

Cloud services APIs capture basic metric data for instances/VMs and volumes so you can allocate resources as needed, such as partial CPU processing and disk space across multiple instances/VMs. These resources can change through direct interactions and automation. For example, when the Amazon EC2 web service reports data to the Orion Platform, it calculates the percentage of assigned resources shared between instances.

Cloud metrics differ with OS metrics due to the fluid nature of cloud computing. OS metrics directly capture values from the core system, not the assigned amounts. This data does not calculate shared resources or other users attached to the instances and volumes. This data directly displays the actual usage at a polled point in time.

Both values provide insight into potential and actual issues with performance and resources. Metrics report vastly different information to the cloud and OS based on how allocated resources and metric calculations.

CPU steal is an example of cloud vs. OS metrics. When CPU usage and metrics spike in a cloud environment, multiple processes and instances/VMs in the cloud may access the CPU as multiple owners. Typically, OS metric spikes tend to look like noisy neighbors. The cloud metric data better represents the data as shared resources usage across multiple owners with metrics broken down by owner.
To better define resource usage and alerts, SAM and integrated VMAN display cloud instance metrics throughout all cloud resources in Orion Web Console views, resources, hover-over data, and reports. Cloud metrics, including calculated health status, CPU load, and IOPS data, are used to apply global cloud thresholds that trigger alerts and status changes.

For instances and VMs managed as nodes, the Orion Platform pulls specific OS data for memory and provides additional data through Orion agent, WMI, and SNMP polling methods.

AWS polling

To poll resources and gather metrics, multiple AWS APIs — including CloudWatch, EC2, and EBS — make requests (also known as "calls") to cloud instances and volumes.

⚠️ AWS provides 1 million free requests per calendar month for each account. If you exceed that limit, your AWS account will be charged for extra requests within the remaining time frame.

The amount of polling requests that occur depends on many factors, including:

- Polling frequency.
- The quantity of resources being polled.
- The types of resources being polled.

For example, monitoring a single AWS EC2 instance with a 5-minute polling interval consumes approximately 60,000 requests per calendar month; an EBS volume with the same polling interval may use 100,000 requests per month. Instances managed as nodes, third-party products, and custom code also consume requests.

Here is an overview about how the Orion Platform works with AWS to poll for metrics:

1. Multiple AWS APIs (including CloudWatch, EC2, and EBS) poll AWS cloud instances and volumes.
2. The EC2 web service sends metric data to the Amazon CloudWatch monitoring service.
3. The Orion Platform polls the Amazon CloudWatch service for standard AWS metrics, plus metrics such as memory, usage, and alerts.
4. The Orion Platform saves metric data to the Orion SQL database.

To track the quantity of API requests, you can either:

- Display the latest amount of consumed requests in the AWS Management Console, or
- Display approximate usage in the Orion Web Console:
  a. On the Cloud Summary page, click Cloud Infrastructure Monitoring.
  b. On the Cloud Infrastructure Monitoring page, click Manage Cloud Accounts.
  c. On the Manage Cloud Accounts and select the check box for an AWS account.
  d. Click Edit Properties.
  e. On the Edit Properties page, switch to the API Polling Options tab and examine the Approximate Requests Used this Month value.
To manage polling, you can:

- Edit cloud account properties to select instances to monitor, toggle monitoring on and off, and adjust polling intervals.
- Use the AWS Simple Monthly Calculator to estimate costs.
- Disable CloudWatch polling at the account level.
- Configure polling alerts for throttling, exceeded limits, health status, and more.
- Consider toggling Auto Monitoring off when adding accounts to the Orion Platform to prevent overages.
- To avoid exceeding polling limits, consider toggling Auto Monitoring off when adding a cloud account to block polling for new instances discovered launched and then discovered for an account. You can enable monitoring for individual instances later.
- Request a limit increase from AWS.

To learn more about AWS polling, see:

- Exceed AWS polling limits
- AWS cloud metric reference

**Exceed AWS polling limits**

The Orion Platform tracks requests through the CloudWatch API and can notify users when the system gets close to or surpasses the 1 million free polling requests that AWS provides per account per calendar month, depending on how alerts are configured. See Alerts and events for cloud monitoring.

You can also request a limit increase for specific resources; see the Cloud metric reference.

**Disable CloudWatch API polling for metrics**

You can disable polling by the AWS CloudWatch API at the account level to avoid exceeding AWS polling limits and incurring fees. The API will continue polling resources for status, as displayed on the Cloud Summary and Instance Details pages, but will stop gathering metrics.

To disable CloudWatch API polling:

1. On the Cloud Summary page, click Cloud Infrastructure Monitoring.
2. On the Cloud Infrastructure Monitoring page, click Manage Cloud Accounts.
3. On the Manage Cloud Accounts page, select the check box for an AWS account.
4. Click Edit Properties.
5. On the Edit Properties page, switch to the API Polling Options tab and click the green Monitoring On/Off option to turn off polling.

To avoid exceeding polling limits, consider toggling Auto Monitoring off when adding a cloud account to block polling for new instances launched and then discovered for an account. You can enable monitoring for individual instances later.
# AWS cloud metric reference

The following table details the AWS metrics available for instances using cloud monitoring.

These terms are included in the table:

- Amazon Machine Image (AMI) provides information required to launch an instance.
- Amazon Resource Name (ARN) is a format to identify resources in AWS.
- Key Management Service (KMS) is a managed service to create and control data encryption keys.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>AWS EC2 instance</td>
</tr>
<tr>
<td>Instance Name</td>
<td>User-friendly name for the AWS EC2 instance.</td>
</tr>
<tr>
<td>Region</td>
<td>The region where an instance is located. Regions are divided into Availability Zones to protect instances from failures in other Availability Zones.</td>
</tr>
<tr>
<td>Auto-Scaling Group</td>
<td>The group an instance belongs to that is used to calculate the number of Amazon EC2 instances available to handle the load for an application.</td>
</tr>
<tr>
<td>Status</td>
<td>Calculated value of Up/Down.</td>
</tr>
<tr>
<td>State</td>
<td>Instance state reported by AWS: Up/Down.</td>
</tr>
<tr>
<td>Platform</td>
<td>The OS platform, such as Windows. This is not returned for all platform types.</td>
</tr>
<tr>
<td>Architecture</td>
<td>CPU architecture type. Currently AWS supports two CPU architecture types, &quot;i386&quot; and &quot;x86_64&quot;.</td>
</tr>
<tr>
<td>Public DNS Name</td>
<td>The public hostname of the instance that resolves to the instance's public or Elastic IP address. Example: ec2-54-213-116-42.us-west-2.compute.amazonaws.com</td>
</tr>
<tr>
<td>Private DNS Name</td>
<td>The internal hostname of the instance that resolves to the instance's private IP address. Example: fogbugz.dev.local</td>
</tr>
<tr>
<td>Subnet ID</td>
<td>The range of IP addresses in a virtual private cloud (VPC) that the instance was launched into, if applicable. Click here to learn more about VPCs and subnets.</td>
</tr>
<tr>
<td>Source/Destination Check</td>
<td>Indicates if source/destination checks are being performed on an instance to determine if it sends/receives traffic.</td>
</tr>
<tr>
<td>Instance ID</td>
<td>The ID for the cloud instance.</td>
</tr>
<tr>
<td>Instance Type</td>
<td>The type of instance determines your instance's CPU capacity, memory, and storage (for example, m1.small or c1.xlarge). See the AWS Instance Types page for full details.</td>
</tr>
<tr>
<td>Instance Creation Date</td>
<td>The time the instance launched.</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Image ID</td>
<td>An encrypted machine image stored in Amazon Elastic Block Store or Amazon Simple Storage Service. An Amazon Machine Image (AMI) acts as a template of a computer's root drive. It contains the OS and can also include software and layers of your application such as database servers, middleware, and web servers. Example: ami-3231adad</td>
</tr>
<tr>
<td>AMI Launch Index</td>
<td>A number indicating the order in which the instance was launched. The first or only instance has an index of 0.</td>
</tr>
<tr>
<td>Last Poll</td>
<td>The time when the instance was last polled by Orion Platform.</td>
</tr>
<tr>
<td>Next Poll</td>
<td>The time when the instance will be polled again by Orion Platform.</td>
</tr>
<tr>
<td>Monitored</td>
<td>The level of CloudWatch monitoring that is enabled for this instance: Basic/Detailed</td>
</tr>
<tr>
<td>RAM disk ID</td>
<td>The RAM disk associated with the image, if one was specified.</td>
</tr>
<tr>
<td>Kernel ID</td>
<td>The OS kernel associated with the AMI.</td>
</tr>
<tr>
<td>Root Device type</td>
<td>The root device type used by the AMI. The AMI can use an Amazon EBS or instance store root device.</td>
</tr>
<tr>
<td>Root Device Name</td>
<td>The ID of the system device contains the boot volume.</td>
</tr>
<tr>
<td>EBS optimized</td>
<td>Indicates if additional, dedicated throughput between Amazon EC2 and Amazon EBS was enabled for the instance.</td>
</tr>
<tr>
<td>Tenancy</td>
<td>Type of tenancy: Dedicated/Default. If dedicated, the instance is running on single-tenant, dedicated hardware.</td>
</tr>
<tr>
<td>IAM role</td>
<td>The IAM roles (for example: s3acces) associated with the instance, if applicable.</td>
</tr>
<tr>
<td>Owner</td>
<td>The AWS account number of the AMI owner, without dashes.</td>
</tr>
<tr>
<td>Security Groups</td>
<td>The security groups to which the instance belongs. A security group is a collection of firewall rules that restrict the network traffic for the instance.</td>
</tr>
<tr>
<td>VPC ID</td>
<td>The ID of the virtual private cloud (VPC) the instance was launched into, if applicable. A VPC is an isolated portion of the AWS cloud.</td>
</tr>
<tr>
<td>KeyPair name</td>
<td>The name of the key pair, if this instance was launched with an associated KeyPair.</td>
</tr>
<tr>
<td>Placement Group</td>
<td>If the cloud instance is a cluster instance, this is the cluster group to which the instance belongs.</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Virtualization</td>
<td>The type of virtual machine running: paravirtual/hvm.</td>
</tr>
<tr>
<td>Reservation</td>
<td>The reservation ID used to launch the instance.</td>
</tr>
<tr>
<td>State Transition Reason</td>
<td>The reason for the change of instance state. For example, if the instance was terminated, the reason might be ‘User initiated shutdown’.</td>
</tr>
<tr>
<td>Public IP address</td>
<td>Public Internet routable IP address of the instance</td>
</tr>
<tr>
<td>Private IP address</td>
<td>The private IP address of the instance. Multiple IP addresses are listed if there is more than one network interface to the instance.</td>
</tr>
<tr>
<td>Secondary Private IP address</td>
<td>Any secondary private IP addresses assigned to a network interface attached to the instance.</td>
</tr>
<tr>
<td>Elastic IP address</td>
<td>The Elastic IP address assigned to the instance, if applicable. Elastic IP addresses are static IP addresses assigned to your account that you can quickly remap to other instances.</td>
</tr>
<tr>
<td>CPU utilization</td>
<td>The percentage of allocated EC2 compute units that are currently in use on the instance. This metric identifies the processing power required to run an application upon a selected instance.</td>
</tr>
<tr>
<td>Disk Read Ops</td>
<td>Completed write operations to all ephemeral disks available to the instance in a specified period of time. This metrics requires EBA volumes.</td>
</tr>
<tr>
<td>Disk WriterOps</td>
<td>Completed write operations from all ephemeral disks available to the instance. This metrics requires EBA volumes.</td>
</tr>
<tr>
<td>DiskReadBytes</td>
<td>Bytes read from all ephemeral disks available to the instance. This metrics requires EBA volumes.</td>
</tr>
<tr>
<td>DiskWriteBytes</td>
<td>Bytes written to all ephemeral disks available to the instance. This metrics requires EBA volumes.</td>
</tr>
<tr>
<td>NetworkIn</td>
<td>The number of bytes received on all network interfaces by the instance. This metric identifies the volume of incoming network traffic to an application on a single instance.</td>
</tr>
<tr>
<td>NetworkOut</td>
<td>The number of bytes sent out on all network interfaces by the instance. This metric identifies the volume of outgoing network traffic to an application on a single instance.</td>
</tr>
</tbody>
</table>

The following table details the AWS metrics available for monitored volumes.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume ID</td>
<td>User-friendly name of the cloud volume</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Volume Type</td>
<td>Indicates whether the volume is a standard (Magnetic), gp2 (General Purpose (SSD)) or io1 (Provisioned IOPS (SSD))</td>
</tr>
<tr>
<td>Size</td>
<td>The capacity of the Amazon EBS volume in GiB. Note that 1 GiB = 1024^3 bytes, whereas 1 GB = 1000^3 bytes.</td>
</tr>
<tr>
<td>Alarm Status</td>
<td>CloudWatch alarm summary for alarms monitoring metrics for this volume.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the volume. For example: Creating/Available/In-Use/Deleting/Error</td>
</tr>
<tr>
<td>Encrypted</td>
<td>Indicates whether the volume is encrypted. For example: Encrypted/Not Encrypted</td>
</tr>
<tr>
<td>Region</td>
<td>The Availability Zone where the volume is located</td>
</tr>
<tr>
<td>CreatedTime</td>
<td>Date/time the Amazon EBS volume was created</td>
</tr>
<tr>
<td>AttachedTime</td>
<td>Date/Time the Amazon EBS volume was attached to the Instance</td>
</tr>
<tr>
<td>Delete on Termination</td>
<td>Denotes if the volume will be deleted when the associated instance it is attached to is terminated: True/False</td>
</tr>
<tr>
<td>KMS Key ID</td>
<td>A unique identifier for the customer master key. This value can be a globally unique ID.</td>
</tr>
<tr>
<td>KMS Key Aliases</td>
<td>Key Management Service friendly name</td>
</tr>
<tr>
<td>KMS Key ARN</td>
<td>The Amazon Resource Name for the Key Management Service key</td>
</tr>
<tr>
<td>Product Codes</td>
<td>DevPay or AWS Marketplace codes associated with the volume, if applicable</td>
</tr>
<tr>
<td>Snapshot</td>
<td>The ID of the snapshot used to create the volume, if applicable. A snapshot is a copy of an Amazon EBS volume at a point in time.</td>
</tr>
<tr>
<td>Volume Idle Time</td>
<td>The total number of seconds in a specified period of time when no read or write operations were submitted.</td>
</tr>
<tr>
<td>Throughput Percentage</td>
<td>Only used with Provisioned IOPS volumes. The percentage of I/O operations per second (IOPS) delivered of the total IOPS provisioned for an Amazon EBS volume. Provisioned IOPS (SSD) volumes deliver within 10 percent of the provisioned IOPS performance 99.9 percent of the time over a given year.</td>
</tr>
<tr>
<td>Read Bandwidth (KB/S)</td>
<td>( \frac{\text{Sum}(\text{VolumeReadBytes})}{\text{Period}} / 1024 )</td>
</tr>
<tr>
<td>Write Bandwidth (KB/S)</td>
<td>( \frac{\text{Sum}(\text{VolumeWriteBytes})}{\text{Period}} / 1024 )</td>
</tr>
<tr>
<td>Read Throughput IOPS</td>
<td>( \frac{\text{Sum}(\text{VolumeReadOps})}{\text{Period}} )</td>
</tr>
<tr>
<td>Write Throughput IOPS</td>
<td>( \frac{\text{Sum}(\text{VolumeWriteOps})}{\text{Period}} )</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Average Queue Length</td>
<td>The number of read and write operation requests waiting to be completed in a specified period of time.</td>
</tr>
<tr>
<td>Average Read Size</td>
<td>The total number of bytes read in a specified period of time.</td>
</tr>
<tr>
<td>Average Write Size</td>
<td>The total number of bytes written in a specified period of time.</td>
</tr>
<tr>
<td>Average Read Latency</td>
<td>The total number of seconds spent by all operations that completed in a specified period of time. If multiple requests are submitted at the same time, this total could be greater than the length of the period. For example, for a period of 5 minutes (300 seconds): if 700 operations completed during that period, and each operation took 1 second, the value would be 700 seconds.</td>
</tr>
<tr>
<td>Average Write Latency</td>
<td>The total number of seconds spent by all operations that completed in a specified period of time. If multiple requests are submitted at the same time, this total could be greater than the length of the period. For example, for a period of 5 minutes (300 seconds): if 700 operations completed during that period, and each operation took 1 second, the value would be 700 seconds.</td>
</tr>
<tr>
<td>Consumed R/W IOPS</td>
<td>Used with Provisioned IOPS (SSD) volumes only. The total amount of read and write operations (normalized to 256K capacity units) consumed in a specified period of time. I/O operations that are smaller than 256K each count as 1 consumed IOPS. I/O operations that are larger than 256K are counted in 256K capacity units. For example, a 1024K I/O would count as 4 consumed IOPS.</td>
</tr>
</tbody>
</table>

**Azure polling**

You can monitor and manage resource status and metrics through the Azure Portal, Orion Web Console, SAM, or integrated VMAN. SAM provides additional metrics for memory and features for cloud infrastructure management, usage, alerts, and more.

Here is an overview about how the Orion Platform works with Azure to poll for status and metric data:

1. The Azure Resource Manager and Azure APIs poll cloud VMs and volumes to gather status metrics for the Azure Monitor service.
2. The Orion Platform API polls the Azure Monitor service.
3. The Orion Platform saves data to the Orion SQL Database.

⚠️ Azure provides 1 million standard API calls per calendar month at no cost. Extra charges are incurred for overages based on Azure Monitor pricing. Azure may link limits and charges to either subscriptions or tenant accounts, depending on how Azure is configured for your organization. Check with your subscription administrator.

See these topics for details:

- [Understanding Azure polling limits](#)
- [Track Azure resource usage](#)
• Disabling the Azure Monitor API to reduce polling
• Azure Monitor cloud metric reference

Understand Azure polling limits

Azure has a polling limit of 1 million free API requests per subscription per calendar month and considers a single API request (also known as a "call") to be one that returns 1,440 data points.

- If an API request returns more than 1,440 data points, Azure counts it as multiple API requests.
- If an API request returns less than 1,440 data points, Azure counts as less than one API request.

Azure calculates the number of API requests per day by aggregating the number of data points consumed each day, and then dividing that total by 1,440. 1,440 is also the total number of data points that can be stored per metric per day. To learn about increasing polling limits, review Azure subscription and service limits from Microsoft.

Requests may be consumed by third-party products, custom code, Azure VMs managed as nodes in the Orion Platform.

Azure constantly checks incoming requests against account limit settings. To manage polling to avoid exceeding limits and incurring charges, you can:

- Edit cloud account properties to toggle monitoring on and off for an entire cloud account or individual VMs.
- Configure polling alerts for throttling, exceeded limits, health status, and more.
- Request a limit increase from Microsoft.
- Disable the Azure Monitor API.
- Proactively track Azure resource usage, as described next.

Track Azure resource usage

There are many ways to track Azure usage and proactively adjust capacity before exceeding limits and incurring charges, including:

- Log into the Azure Portal and display usage statistics.
- Download a usage file from the Azure Portal.

To display approximate usage in the Orion Web Console

1. On the Cloud Summary page, click Cloud Infrastructure Monitoring.
2. On the Cloud Infrastructure Monitoring, click Manage Cloud Accounts.
3. On the Manage Cloud Accounts and select the check box for an Azure account.
4. Click Edit Properties.
5. On the Edit Properties page, switch to the API Polling Options tab and examine the Approximate Requests Used this Month value.

Azure tracks API requests and applies throttling after reaching 15,000 read-requests per hour, by default.
To consolidate all Azure payments into a single bill and identify your total spending for cloud services, download the free Cost Calculator for Azure. Click here for details.

Disable the Azure Monitor API

You can disable the Azure Monitor API at the account level to avoid exceeding polling limits and incurring fees, especially if levels get close to or exceed the limit of free requests. Azure APIs continue polling for VM status, as displayed on the Cloud Summary and Instance Details pages, but metric polling stops.

Azure Monitor cloud metric reference

This table details metrics available for Azure VMs and volumes.

You may notice that more metrics appear for AWS instances than for Azure volumes. This is due to the fact that AWS generally provides more metrics for volumes than Azure does, as reflected by the metrics displayed in the Orion Web Console.

<table>
<thead>
<tr>
<th>Category</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response</td>
<td>Response Time</td>
</tr>
<tr>
<td>Wait Time</td>
<td>Instance Wait Time</td>
</tr>
<tr>
<td>Session</td>
<td>Active Sessions</td>
</tr>
<tr>
<td></td>
<td>Total User Sessions</td>
</tr>
<tr>
<td></td>
<td>Blocked Sessions</td>
</tr>
<tr>
<td></td>
<td>Distinct Machines</td>
</tr>
<tr>
<td></td>
<td>Distinct Users</td>
</tr>
<tr>
<td>Resources</td>
<td>CPU Utilization</td>
</tr>
<tr>
<td></td>
<td>Memory Utilization</td>
</tr>
<tr>
<td>I/O Stats</td>
<td>Total Read I/O Wait</td>
</tr>
<tr>
<td></td>
<td>Total Write I/O Wait</td>
</tr>
<tr>
<td></td>
<td>Total I/O Wait</td>
</tr>
<tr>
<td></td>
<td>SQL Disk Read Latency</td>
</tr>
<tr>
<td></td>
<td>SQL Disk Write Latency</td>
</tr>
</tbody>
</table>
## Throttling overview

Most cloud service providers monitor incoming API requests to control the consumption of resources used by an instance/VM, an individual cloud account, or an entire service. To continue meeting service level agreements with customers, a cloud service will apply throttling to block requests from a customer if increased polling places an extreme load on cloud resources. Throttling helps maintain performance and availability for Orion Platform services.
Limits are set by time, region, and cloud account; Orion Platform alerts can be configured to alert users when API request get close to or exceed limits. To prevent throttling issues, you can extend polling intervals and/or disable API polling for specific resources. See AWS throttling and Azure throttling.

AWS throttling

The AWS API Gateway constantly checks incoming requests from the Orion Platform against AWS account limits. AWS limits steady-state request rates to 1000 requests per second (RPS) and allows bursts of up to 2000 RPS across all APIs, stages, and methods within an AWS account.

AWS applies throttling to relevant instances and volumes when requests exceed default or custom polling thresholds, or if a single event such as a failed polling request occurs. When throttling is applied, the following results occur:

- AWS blocks incoming API requests.
- AWS returns a 429 HTTP response to the Orion Platform.
- Polling is suspended. Relevant instances and volumes enter an Unknown state — AWS Throttling Applied — until the workload decreases.
- Throttling alerts in the Orion Platform are triggered.
- Users receive email notifications that indicate the number of affected instances and volumes.

When throttling stops, resource statuses are updated and alerts are cleared.

Manage AWS throttling alerts

To help reduce multiple alerts overwhelming the alert list, use the Alert me when AWS throttling is applied for cloud account alert, which aggregates throttling events for instances or volumes into a single alert. The Orion Platform checks CloudWatch each minute for throttled instances and volumes; email notifications are sent when throttling stops.

To always receive alerts per throttled instance and volume, disable the account-level alert and enable the following alerts.

- **Alert me when AWS throttling is applied for cloud instance**: Disabled by default, this alert checks every minute if throttling is applied to instances. Conditions check for the instance status of Unknown and AWS Throttling applied through EC2 API calls.
- **Alert me when AWS throttling is applied for cloud volume**: Disabled by default, this alert checks every minute if throttling is applied to volumes. Conditions check for the attached volume status of Unknown and AWS Throttling applied through EC2 API calls.

Azure throttling

Azure constantly monitors incoming requests from the Orion Platform and throttles VMs, as necessary, to control the consumption of resources so it can continue to function even when increased demand places an extreme load on resources.

For each subscription and tenant across all regions, the Azure Resource Manager limits read requests to 15,000 per hour and write requests to 1,200 per hour for each VM. For each region, Azure limits read requests to 25,000 per hour but it may be hard to predict how often that limit will be reached in a region.
The number of requests is scoped to either your subscription or tenant. If you have multiple, concurrent applications making requests in your subscription, those requests are added together to determine the number of remaining requests.

When read requests from the Orion Platform reach the limits, Azure sends HTTP status code 429 and triggered alerts appear in the Orion Web Console. The status of a throttled VM switches to N/A — not available — until polling resumes.

For tips on reducing Azure throttling, click here.

The Orion Platform checks every minute for throttled VMs and volumes. To prevent multiple alerts from flooding the alert list, the **Azure throttling is applied for cloud account** alert aggregates throttling events for VMs or volumes linked to an account into a single alert. An email notification indicates the number of affected VMs and volumes.

To always receive alerts per throttled VM and volume, disable the account level alert and enable the following alerts.

If multiple VMs and volumes incur throttling, the list of alerts can be extensive.

- **Azure throttling is applied for VM**: Disabled by default, this alert checks every minute to determine if throttling is applied to VM. Conditions check for the VM status of Unknown and throttling applied through Azure API calls.
- **Azure throttling is applied for cloud volume**: Disabled by default, this alert checks every minute to determine if throttling is applied to volumes. Conditions check for the attached volume status of Unknown and throttling applied through Azure API calls.

To create additional throttling alerts, copy an existing alert and customize it. See Manage cloud monitoring alerts.

Manage your cloud infrastructure

This section describes how to monitor cloud instances and VMs in the Orion Platform. It includes the following topics:

- Find cloud account credentials
- Configure cloud monitoring settings
  - Access the Cloud Infrastructure Monitoring Settings page
  - Add another cloud account
  - Manage existing cloud accounts
  - Edit retention settings for cloud-related statistics
  - Create cloud application monitors and templates
  - Edit global thresholds for cloud monitoring
- Manage cloud monitoring alerts
- Troubleshoot cloud monitoring
Find cloud account credentials

As you work with cloud accounts in the Orion Platform, you may be prompted to provide account credentials (for example, when deploying an Orion agent to a cloud instance).

**For an AWS account,** provide the Access Key ID and Secret Access Key.

To find AWS credentials:

1. Log into the AWS Management Console,
2. Click Account > Security Credentials.
3. Scroll down to locate the credentials.
4. Copy credentials into the Orion Web Console.

**For an Azure account,** provide the following credentials, available in the Azure Portal:

- Subscription ID
- Tenant/Directory ID
- Client/Application ID
- Application Secret Key

For tips on finding Azure credentials in the Azure Portal, click [here](#). Also, note that Azure uses different terms for the same credential, as outlined next.

<table>
<thead>
<tr>
<th>Orion Web Console reference</th>
<th>Microsoft Azure reference</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Subscription ID             | Subscription ID           | • Used by Microsoft to manage billing.  
                                |                           | • Grants access to the Azure Portal.  
                                |                           | • Governs access to and use of Azure services.  
                                |                           | • Each deployed resource is linked to only one subscription. |
| Tenant/Directory ID          | Directory ID              | • Linked to an Active Directory (AD) app that enables the Orion Platform to access Azure.  
<table>
<thead>
<tr>
<th>Orion Web Console reference</th>
<th>Microsoft Azure reference</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client/Application ID</td>
<td>Client ID</td>
<td>• Used to grant permissions.</td>
</tr>
<tr>
<td></td>
<td>Application ID</td>
<td>• Often called the Client ID in external applications.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• See <a href="https://docs.microsoft.com">Getting an Application ID and authentication key</a>, (© 2019, Microsoft Corp., available at <a href="https://docs.microsoft.com">https://docs.microsoft.com</a>, obtained on January 23, 2019)</td>
</tr>
<tr>
<td>Application Secret Key</td>
<td>Application Secret Key</td>
<td>• See <a href="https://docs.microsoft.com">Getting an Application ID and authentication key</a>, (© 2019, Microsoft Corp., available at <a href="https://docs.microsoft.com">https://docs.microsoft.com</a>, obtained on January 23, 2019)</td>
</tr>
<tr>
<td></td>
<td>Authentication Key</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Client Secret</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Client Secret Key</td>
<td></td>
</tr>
</tbody>
</table>

When you generate a secret Key in the Azure Portal, record it immediately. Otherwise, you will need to generate a new key later.

Configure cloud monitoring settings

After cloud accounts are configured in the AWS Management Console and Azure Portal, and an initial cloud account is added to the Orion Platform, customize cloud monitoring settings by:

- Access the Cloud Infrastructure Monitoring Settings page.
- Adding another cloud account.
- Managing existing cloud accounts to:
  - Edit cloud account properties.
  - Choose instances/VMs to monitor.
  - Perform actions against instances/VMs.
  - Manage instances/VMs as Orion Platform nodes.
  - Remove accounts.
- Editing global retention setting for cloud statistics in the Orion SQL database.
- Editing global thresholds for cloud monitoring that trigger alerts and determine warning/critical status.
Access the Cloud Infrastructure Monitoring Settings page

There are two ways to access the Cloud Infrastructure Monitoring Settings page to add cloud accounts, edit account properties, configure retention settings, and edit global thresholds.

- In the Orion Web Console, click Settings > All Settings to navigate to the Main Settings & Administration page. Under Product Specific Settings, click Cloud Infrastructure Monitoring Settings.
- Click My Dashboards > Cloud and then click the Cloud Infrastructure Monitoring Settings link in the top corner of the Cloud Summary page.
Add another cloud account

After the first cloud account is added to the Orion Platform, you can add more accounts via the Cloud Infrastructure Monitoring Settings page.

Before proceeding, make sure the cloud account is configured for the Orion Platform and have your cloud account credentials handy.

To add a cloud account:

1. Access the Cloud Infrastructure Monitoring Settings page.
2. Click Add Cloud Account.
3. Select a cloud service provider.
4. When the Cloud Settings page appears, enter cloud account credentials.
5. Click Test Connection.
   
   If an error occurs, verify account credentials and confirm that accounts are configured for the Orion Platform.
6. (Optional) Toggle Auto Monitoring on and off.
7. Click Continue to advance to the API Polling page.
8. (Optional) Disable automatic polling for instances/VMs currently linked to the account, as well as for future instances/VMs launched for the account.

To avoid exceeding polling limits, consider toggling Auto Monitoring off when adding a cloud account to block polling for new instances/VMs launched and then discovered for an account. You can enable monitoring for individual instances/VMs later.

9. (Optional) Change the default polling frequency — 5 minutes.

10. (Optional) Click Manage Alerts to configure alerts for the account. See Manage cloud monitoring alerts.

Depending on your account permissions, you may not have access to this option.

11. Click Continue.

12. (Optional) On the Instances page, filter instances/VMs that appear by state, region, availability zone, platform, or OS. If an instance/VM is shutdown or not accessible, this icon appears: 

By default, all new instances/VMs related to a cloud user account are monitored and the default polling frequency is 5 minutes.

After an account is added, the Orion Platform begins polling all instances or VMs linked to the new account for status and metrics every five minutes. Click Dashboards > Cloud to display the Cloud Summary page and review instances/VMs for the new account.

13. (Optional) Restrict other users from displaying instances/VMs for the new account in the Orion Web Console, as described next.

Update Orion user account settings to block access to cloud accounts instances/VMs

After adding a cloud account, you can modify user account settings in the Orion Web Console to control which users can access cloud accounts via the Cloud Summary page.

To restrict Orion users from adding, editing, or removing managed cloud instance nodes, modify account permissions in the AWS Management Console or the Azure Portal.

To hide or configure a specific view for summary and instance information, modify Orion account settings.

1. In the Orion Web Console, click Settings > All Settings, locate the User Accounts section, and click Manage Accounts.

2. Select an account and click Edit.

3. Locate and expand Cloud Monitoring Settings to configure the page to display for the Cloud Summary View.

4. On the Cloud Summary page, expand Virtual Infrastructure Monitor Settings and locate the Cloud Instance Details View option.

5. If an instance/VM is Manage a cloud instance or VM as an Orion Platform node, set the Cloud Instance Details View option to Node Details - Cloud. Otherwise, leave it set to Default.

6. Click Submit.
Manage existing cloud accounts

After a cloud account is added to the Orion Platform, you can update existing cloud accounts by:

- Editing cloud account properties, such as name, credentials, and API polling.
- Choosing instances/VMs to monitor.
- Perform actions against cloud instances/VMs such as stop, start, and terminate.
- Configure a cloud instance/VM to be a managed node in the Orion Platform.
- Remove a cloud account.

Edit cloud account properties

To edit cloud account properties, including credentials and polling options:

1. Access the Cloud Infrastructure Monitoring Settings page.
2. Click Manage Cloud Accounts.
3. On the Manage Cloud Accounts page, select the account you are updating.
4. Click Edit Properties.
5. On the Edit Properties page, modify account credentials and settings as needed.
6. Click Test Connection to verify the changes.
7. Click Save.
8. (Optional) Switch to the API Polling Options tab, update settings, and click Save.

Instead of clicking Save at the bottom of the Edit Properties page, you can click Save and Choose Instances/VMs.

Choose cloud instances/VMs to monitor

This topic describes how to enable monitoring for instances/VMs related to a cloud account from the Cloud Infrastructure Monitoring Settings page. You can also manage instances/VMs displayed on the Cloud Summary page; see Manage Cloud Instances/VMs.

Monitored instances/VMs do not count against SAM and integrated VMAN licenses unless they are managed as Orion nodes. See Manage a cloud instance or VM as an Orion Platform node.

1. Access the Cloud Infrastructure Monitoring Settings page.
2. Click Manage Cloud Accounts.
3. On the Manage Cloud Accounts page, select the check box next to the account for which you are choosing instances/VMs to monitor.
4. Click Choose Instances/VMs.
5. Select the check box next to an instance/VM to toggle Auto Monitoring on or off.
6. Scroll down and click Save.

Perform actions against cloud instances and VMs

With the necessary account permissions, you can perform the following actions via the AWS Cloud Instance Management resource or Azure Cloud VM Management resource displayed on the Cloud Summary page.

- **Stop an AWS cloud instance/VM** to block access to it. The cloud service erases all data and polling stops. If the Manage a cloud instance or VM as an Orion Platform node, SAM and integrated VMAN retain licenses for it.
- **Stop an Azure VM** to remove it from the Hypervisor standpoint but maintain it in the control plane.
- **Reboot a cloud instance/VM** to restart it and preserve data.
- **Delete a cloud instance/VM** to remove it permanently from the cloud service. If the Manage a cloud instance or VM as an Orion Platform node, select the option to remove the node from Orion. The cloud service deletes all stored instance/VM data. The instance/VM no longer appears as an available instance/VM for an account in the Orion Web Console.
- **Unmanage and manage a cloud instance/VM** to release the license and halt polling, which is useful when performing maintenance. Cloud service APIs continue to poll.

If you disable Orion Platform polling for an instance, VM, or managed node, the cloud service API continues to monitor for status but will not gather other metrics.

- **Poll an instance/VM immediately.**
- **Turn polling on and off for an instance/VM.**

Note the following details about performing actions against cloud instances and VMs:

- The page name on which you perform actions and the resource name vary based on whether an AWS instance or Azure VM is selected on the Cloud Summary page.
  - If you click an AWS instance on the Cloud Summary page, or in the Cloud Server Infrastructure resource, the AWS Cloud Instance Details page displays the AWS Cloud Instance Management resource, as shown in the following example:

    ![Cloud Instance Management](image)

    - If you click an Azure VM on the Cloud Summary page, or in the Cloud Server Infrastructure resource, the Cloud VM Details page displays the Azure Cloud VM resource.
- Depending how Azure is configured for your organization, you may require different Azure credentials and/or permissions to perform actions. Consult a subscription administrator.
• You can also manage cloud instances/VMs in the AWS Management Console (© 2018, Amazon Web Services, Inc. or its affiliates, obtained from https://aws.amazon.com/console/ on October 22, 2018) or Azure Portal (© 2018 Microsoft, obtained from https://portal.azure.com, on October 22, 2018). Before doing so, review this section to learn about Orion Platform settings that may need to be configured for instances/VMs changed outside of the Orion Web Console.

Stop an AWS cloud instance/VM

You can stop and restart an AWS cloud instance with an EBS attached volume to block polling for the instance (© 2018, Amazon Web Services, Inc. or its affiliates, obtained from https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Stop_Start.html on October 22, 2018). Data on the local volume for the cloud instance is cleared and is retained on the attached EBS volume.

⚠️ SolarWinds does not recommend forcing an AWS cloud instance to stop because it does not allow the system to flush file caches or metadata. If you use this option, you will need to perform file system checks and repairs.

1. In the Orion Web Console, select My Dashboards > Cloud.
2. On the Cloud Summary page, locate the instance in the Cloud Instances Status Summary or Cloud Server Infrastructure resource.
3. Click the instance to open the AWS Cloud Instance Details page. If an instance is a managed node, this page is called "Node Details."
4. Click Stop in the AWS Cloud Instance Management resource.

![Cloud Instance Management](image)

5. When a confirmation message appears, click Yes to force the instance to stop.
6. Perform file system checks and repairs to flush file caches or metadata, as necessary. See Troubleshooting Stopping Your Instance (© 2018, Amazon Web Services, Inc. or its affiliates, obtained from https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesStopping.html on October 22, 2018).

Stop an Azure cloud VM

You can stop an Azure cloud VM to remove it from the Hypervisor standpoint but keep it available in the control plane. Virtual machines in the Deallocated state do not incur compute charges. See Virtual machine state information (© Microsoft 2018, obtained from https://docs.microsoft.com/en-us/azure/virtual-machines/windows/states-lifecycle on October 22, 2018).

1. In the Orion Web Console, select My Dashboards > Cloud.
2. On the Cloud Summary page, locate the Azure VM in the Cloud VMs Status Summary or Cloud Server Infrastructure resource.
3. Click the VM to open the Azure Cloud VM Details page.
If a VM is managed as a node, this page is called "Node Details."

4. Click Stop in the Azure Cloud VM resource.

Reboot a cloud instance/VM

A reboot restarts a cloud instance/VM while preserving data. For AWS instances, both the public DNS name and data on the attached EBS volume are retained. Azure VMs retain all data.

1. In the Orion Web Console, select My Dashboards > Cloud.
2. On the Cloud Summary page, locate the instance/VM in the Cloud Instances/VMs Status Summary or Cloud Server Infrastructure resource.
3. Click the instance/VM to open its Details page. If an instance/VM is a managed node, this page is called "Node Details."
4. Click Reboot in the Cloud Instance/VM Management resource.
5. When a confirmation message appears, click Yes.

Delete a cloud instance/VM

The Delete option on the Cloud Instance Details page permanently removes an instance/VM from your environment. The cloud service stops monitoring the instance/VM and deletes all stored data in its system. The instance/VM does not appear in the Orion Web Console.

If a cloud instance/VM is a managed node, the Delete option appears on the Node Details page. If you click Delete, the node is removed from the cloud service and Orion Web Console. Consumed SolarWinds product licenses are released.

1. In the Orion Web Console, select My Dashboards > Cloud.
2. On the Cloud Summary page, locate the instance/VM in the Cloud Instances/VMs Status Summary or Cloud Server Infrastructure resource.
3. Click the instance/VM to open its Details page. If an instance/VM is managed as node, this page is called "Node Details."
4. Click Delete in the Cloud Instance/VM Management resource.
5. When prompted to confirm the deletion, click Yes.

⚠️ Deleting an instance/VM permanently removes it, along with all associated data, from AWS or Azure.

The instance/VM is removed from the Orion Web Console and is no longer monitored.

Note that a cloud instance/VM managed as a node is not removed from the Orion Platform until you delete it. To delete the node and release licenses:

1. Select Settings > All Settings, click Manage Nodes.
2. Locate the managed node.
3. Click Delete.
Unmanage and manage a cloud instance/VM

Use the Unmanage/Manage option to pause and restart polling between the Orion Platform and a cloud instance/VM that is managed as a node. When polling is active (and managed), this option appears as Unmanage.

- In the Orion Web Console, select My Dashboards > Home > Cloud.
- On the Cloud Summary page, locate the instance/VM in the Cloud Instances Status Summary or Cloud Server Infrastructure resource.
- Click the instance/VM to open its Details page. If an instance/VM is managed as a node, the Node Details page appears.
- In the Management resource, select Unmanage for an active node (or Manage for a paused node).
- When prompted to confirm, click Yes to unmanage (or manage).

If you plan to delete a node, do not unmanage the node before deleting it. This will cause the node to enter an Unknown state. See Delete a cloud instance/VM.

Poll a cloud instance/VM immediately

By default, the Orion Platform polls cloud services every five minutes. Use the Poll Now option to initiate an immediate poll and retrieve data from cloud service APIs.

- In the Orion Web Console, select My Dashboards > Cloud.
- On the Cloud Summary page, locate the cloud instance/VM in the Cloud Instances Status Summary or Cloud Server Infrastructure resource.
- Click the instance/VM to open its Details page. If an instance/VM is managed as a node, the Node Details page appears.
- Click Poll Now.
Manage monitoring for cloud service accounts

You can toggle monitoring on and off for a cloud service account, which will affect all cloud instances/VMs linked to the account. The Orion Platform halts monitoring metrics account instances/VMs related but cloud service APIs continue checking instance/VM status, as displayed in the Orion Web Console.

1. **Access the Cloud Infrastructure Monitoring Settings page.**
2. Click Manage Cloud Accounts.

![Cloud Infrastructure Monitoring Settings](image)

3. Navigate to the account for which you want control monitoring and click Choose Instances/VMs.
4. Locate the cloud instance/VM in the list that appears and toggle monitoring on or off.

Manage a cloud instance or VM as an Orion Platform node

You can configure a cloud instance/VM as a managed node in the Orion Web Console to leverage the full capabilities of the Orion Platform, including the ability to:

- Use SolarWinds **SAM** to:
  - Monitor the performance, capacity, and health of Linux and Windows apps across data centers, remote offices, and the cloud.
  - Poll specific **OS metrics** beyond the basic metrics gathered by cloud service APIs, including instance/VM memory and other metrics retrieved by SAM application monitors.
  - Track cloud instances/VMs that do not support agentless monitoring.
  - Monitor multi-vendor applications, servers, databases, and storage.
  - Develop and deploy custom script monitors for PowerShell, Nagios, Linux/Unix, and Windows.
  - Leverage **SAM application monitors and templates** to poll for app health and performance metrics to pinpoint the root cause of application issues.
  - Track dependencies and troubleshoot issues via interactive visual mapping in **AppStack**.
  - Monitor network interfaces on Windows servers managed by WMI with SolarWinds **Network Performance Manager (NPM)**.
Use SolarWinds Virtualization Manager (VMAN) to:
- Fix vSphere and Hyper-V issues in minutes through performance recommendations and monitoring.
- Assign Custom Properties to nodes.
- Reduce downtime with proactive alerts and recommendations.
- Save time by fixing issues faster with active performance alerts.
- Reclaim an average of 23% of virtual resources using VM sprawl recommendations.

VMAN recommendations that trigger actions in virtual environments such as vCenter do not impact cloud instances/VMs.

Use SolarWinds SAM and VMAN together to:
- Poll the server hardware health of VMware ESXi hosts.
- Collect asset inventory data for VMs and ESXi hosts.
- Reboot the server from within the Orion Web Console.
- Utilize the Real-time Event Log Viewer, Real-time Process Explorer, and Service Control Manager.

Before configuring a cloud instance/VM as a managed node, note these details:
- Before performing maintenance on a managed cloud instance/VM, use the Unmanage/Manage toggle to release the license and halt polling. See Perform actions against cloud instances/VMs.
- If you halt polling for a managed node, the cloud service API stops polling for metrics but continues to monitor the node for status.
- Depending on how Azure subscriptions are configured, deploying an Orion agent on an Azure VM may require different Azure credentials. See Configure a VM for use as a managed node in the Orion Platform and consult your subscription administrator, as necessary.
- Managing a cloud instance/VM as a node consumes VMAN sockets and SAM licenses.

Configure a cloud instance/VM as a managed node

To manage a cloud instance/VM in the Orion Web Console:
1. Deploy an Orion agent to an instance/VM. See Deploy Windows agents in the cloud.
2. Click My Dashboards > Cloud.
3. On the Cloud Summary page, click the instance/VM in the Cloud Instances Status Summary list to display its Details page.

![Cloud Summary](image1)

4. On the Details page, click Manage Instance/VM As Node.

![Manage Instance As Node](image2)

5. When the Manage As Node dialog box appears, select an IP address.

6. Click Yes, Manage This Node.

7. Follow the instructions provided in the Add Node wizard.

Note these details about wizard options:

- For Polling Method, select a method that supports cloud instances/VMs — Agent, WMI, or SNMP.

  ![Info](image3)

  If you select External Node or Status Only (ICMP), the instance/VM is not related to the node and cloud metrics do not appear on the Node Details page.

- The Orion Platform can use these methods to poll a cloud instance/VM managed as a node:
  - An Orion agent with or without a VPN. See [Deploying an Orion agent](#).
  - WMI with a VPN connected to an AWS Virtual Private Cloud (VPC) or Azure Virtual Network (VN).
  - SNMP with a VPN connected to an AWS VPC or Azure VN.

  ![Info](image4)

  Before nodes can connect to cloud instances/VMs, the Orion Platform must poll for IP and MAC addresses, which can take 10 to 15 minutes. After data is retrieved, polling starts and node metrics appear in the Orion Web Console.
Configure a VM for use as a managed node in the Orion Platform

There are many ways organizations can set up and use Azure. Depending on how Azure subscriptions are configured for your organization, you may need to change VM settings in Azure before configuring a VM as a managed node in the Orion Platform. Consult your subscription administrator, as necessary.

1. Log into the Azure Portal.
2. Navigate to the VM.
3. In the VM’s Network Interface security rules, open ports required to monitor the VM with an Orion agent.
   a. Click Virtual network/subnet.
   b. On the Resource Group Details page, open network interface details for the Connected device.
   c. Click Network security group.
   d. Edit Inbound and Outbound security rules.
4. Allow communication using ports required by Orion Agent.
   a. Use * to open all ports or define a range (for example, 8080-8088).
   b. Review Agent requirements and make changes, as necessary.
   c. Change the agent port.
5. Verify that the VM has a static public IP address.
   a. Navigate to the VM Overview page.
   b. Click Public IP Address.
   c. Make sure a static IP address is selected.
6. Configure the firewall on the VM.
   a. Use a Remote Desktop Protocol (RDP) to log into the Azure VM.
   b. Open a port for the Orion agent. See Agent Requirements.
   c. Use PowerShell to disable the firewall the Set-NetFirewallProfile cmdlet.
      
      ```
      PS C:\> Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False
      ```
   d. Press Enter.

Remove a cloud account

If you remove a cloud account, the Orion Platform stops monitoring instances/VMs related to the account.

1. Access the Cloud Infrastructure Monitoring Settings page.
2. Click Manage Account.
3. On the Manage Cloud Accounts page, select the check box next to the account.
4. Click Remove Account.
5. When prompted, click Remove Account again to confirm.
Edit retention settings for cloud-related statistics

Retention settings determine how long cloud-related statistics remain in the Orion SQL database.

1. **Access the Cloud Infrastructure Monitoring Settings page**.
2. Click Retention Settings.
3. Enter a value for the amount of days prior to taking action on data.
   - Detailed Statistics Retention summarized into hourly statistics after the configured period of time.
   - Hourly Statistics Retention summarized into daily statistics after the configured period of time.
   - Daily Statistics Retention deleted from the database after the configured period of time.
4. Click Submit.

Edit global thresholds for cloud monitoring

Set global thresholds for cloud monitoring to identify the warning and critical values for monitored metrics. These thresholds affect polled data from cloud services for status and Orion alerts that are triggered when values reach or surpass warning and critical thresholds.

1. **Access the Cloud Infrastructure Monitoring Settings page**.
2. Click Edit Global Thresholds.
3. Adjust the following default values, as necessary.

<table>
<thead>
<tr>
<th>Monitored cloud metric</th>
<th>Default warning threshold</th>
<th>Critical threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Load (percentage)</td>
<td>80%</td>
<td>90%</td>
</tr>
<tr>
<td>Network Receive Rate (kB/seconds)</td>
<td>5,000 kB/s</td>
<td>100,000 kB/s</td>
</tr>
<tr>
<td>Network Transmit Rate (kB/second)</td>
<td>50,000 kB/s</td>
<td>100,000 kB/s</td>
</tr>
<tr>
<td>Network Usage Rate (kB/second)</td>
<td>100,000 kB/s</td>
<td>200,000 kB/s</td>
</tr>
<tr>
<td>Read IOPS (/second)</td>
<td>50,000 /s</td>
<td>100,000 /s</td>
</tr>
<tr>
<td>Write IOPS (/second)</td>
<td>50,000 /s</td>
<td>100,000 /s</td>
</tr>
<tr>
<td>Total IOPS (/second)</td>
<td>50,000 /s</td>
<td>100,000 /s</td>
</tr>
<tr>
<td>Disk Read (Bytes/second)</td>
<td>700,000 B/s</td>
<td>900,000 B/s</td>
</tr>
<tr>
<td>Disk Write (Bytes/second)</td>
<td>700,000 B/s</td>
<td>900,000 B/s</td>
</tr>
</tbody>
</table>

4. Click Submit.
Create cloud application monitors and templates

SAM includes built-in templates that offer a powerful, customizable way to monitor components and applications in a cloud infrastructure. Templates are comprised of application and component monitors, configuration settings, and scripts that collect data for applications and nodes. Script monitors also provide an array of options for developing custom scripts to process requests and return metrics. You can use built-in templates and scripts, or create your own.

After configuring cloud instances/VMs as managed nodes in the Orion Platform, assign templates to them to gather metrics for monitoring performance and thresholds, troubleshooting, and tracking application health. For details, see the SAM Custom Template Guide, as well as these resources:

- SolarWinds Success Center
- Understanding Application Templates video
- SAM Template Showdown video
- Additional SAM templates on THWACK

SolarWinds supports templates and monitoring scripts included in the SAM product. To solicit feedback from the SolarWinds IT community about custom templates and scripts, visit THWACK.

Here is an high-level example about creating a custom template to monitor a Linux OS on a cloud instance:

1. In the Orion Web Console, configure the cloud instance as a managed node.
2. Click Settings > All Settings > SAM Settings > Manage Templates.
3. Select the built-in Linux CPU Monitoring Perl application template and click Copy.
4. Modify existing component monitors as needed for Linux on the cloud.
5. Add any component monitors as needed.
6. Assign the template to the Linux-based managed node to begin polling and display results in the Orion Web Console, as shown in this example.
Manage cloud monitoring alerts

Cloud monitoring alerts can trigger events and notify users when events occur, such as when:

- **Polling** reaches or surpasses a set threshold for API requests.
- Polling exceeds free request limits set by cloud services.
- The status of a cloud instance/VM or volume changes.
- A cloud service **throttles** API requests to control the consumption of resources used by an instance/VM.

To manage cloud-related alerts in the Orion Web Console, click Alerts & Activity > Alerts > Manage Alerts, and type "cloud" in the search field. You can also display alerts in the Cloud Summary and Cloud Instance/VMs Details pages, as shown in the following example:

Many alerts include email notifications and reset actions that can be customized on the Manage Alerts page in the Orion Web Console.

Some events that trigger alerts and notifications are actions that can be performed against instances/VMs including Stop, Reboot, Delete, and Unmanage.

⚠️ The Orion Platform does not record actions that occur in the AWS Management Console or Azure Portal for auditing purposes or list them as events in the Orion Web Console.

The following cloud monitoring alerts are available in the Orion Platform:

<table>
<thead>
<tr>
<th>Alert</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS cloud instance is in a warning or critical state</td>
<td>A cloud instance encounters polling or access issues triggering a warning or critical state. The alert triggers based on global cloud thresholds.</td>
</tr>
<tr>
<td>Alert</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Alert me when AWS throttling is applied for cloud account</td>
<td>The Orion Platform aggregates throttling is applied for instances or volumes into a single alert and continue checking each minute for throttled instances or volumes. The email notification indicates the number of affected instances and volumes. Affected instances and volumes display in an Unknown - AWS Throttling Applied state. See Manage AWS throttling.</td>
</tr>
<tr>
<td>Alert me when AWS throttling is applied for cloud instance</td>
<td>Disabled by default, this alert checks every minute if throttling is applied to cloud instances. Conditions check for the instance status of Unknown and AWS Throttling applied through EC2 API calls. See Manage AWS throttling.</td>
</tr>
<tr>
<td>Alert me when AWS throttling is applied for cloud volume</td>
<td>Disabled by default, this alert checks every minute if throttling is applied to cloud attached volumes. Conditions check for the attached volume status of Unknown and AWS Throttling applied through EC2 API calls. See Manage AWS throttling.</td>
</tr>
<tr>
<td>AWS CloudWatch polling limit threshold exceeded</td>
<td>AWS CloudWatch provides a 1 million free polling requests limit per calendar month for all API metric polling. If the polling limit threshold is exceeded, this alert triggers.</td>
</tr>
</tbody>
</table>

⚠️ Amazon Web Services does not halt polling or CloudWatch metrics. They charge an additional cost for the month based on the exceeded polls for the remaining time frame.

| Azure throttling is applied for cloud account | This alert notifies you when Azure throttling is applied while calling Azure Monitor API for Cloud Account. See Azure throttling. |
| Azure throttling is applied for VM | This alert will notify you when Azure throttling is applied on VM while calling the Azure Monitor API. See Azure throttling. |
| Azure throttling is applied for cloud volume | This alert notifies you when Azure throttling is applied on cloud volume while calling Azure Monitor API. See Azure throttling. |

Events display with warning and critical indicators based on errors and exceeded thresholds. If a number of events trigger for an instance/VM or volume, SAM and integrated VMAN aggregate the events into a single event without overwhelming the event list and essential monitoring. The following example displays an aggregated critical event:

1/16/2017 1:19 AM
Error polling instances for cloud account SysAdminAWS and region aws-west-1: Error making request with Error Code: InternalServerError and Http Status Code: InternalServerError. No further error information was returned by the service.

To learn about troubleshooting cloud-related alerts, see Troubleshoot cloud monitoring.
Managing cloud service alerts

Although you cannot edit out-of-the-box alerts, you can use an existing alert as a template to create new alerts with custom triggers, conditions, and actions.

The Orion Platform Cloud Infrastructure Monitoring feature does not import alerts or alarms from cloud service platforms.

Here is an overview about duplicating existing cloud alerts to create custom alerts. See Create new alerts to monitor your environment for details.

1. Click Alerts & Activity > Alerts, click Manage Alerts.
2. In the search field, enter Cloud.
3. Select an alert and click Duplicate & Edit.
4. Change the name of the alert and add a description to describe the intent of the alert.
   For example, duplicate the alert for a cloud instance in a warning or critical state to add conditions for specific polled metrics and actions to stop the instance and send notifications.
5. Follow the alert wizard prompts to set conditions and actions.
6. Review and save the alert when complete.

Alerts use the following terminology:

- **Conditions** set triggers for alerts. Create as many conditions as needed for multiple scenarios where one or all conditions are met, including custom properties.
  
  Example: Trigger alert when CPU load spikes above 90% for over 5 minutes.

- **Reset conditions** configure the event that resets an alert.
  
  Example: If an alert triggers when the power state is off, set it to reset when the cloud power state is on.

- **Actions** and escalation steps are completed by the Orion Web Console when an alert is triggered. Create as many actions and escalations as needed.
  
  Example: Send an email notification every 10 minutes until the alert is acknowledged. If the alert is not acknowledged within 10 minutes, send an escalation email to management. Use a management action as needed such as stop or reboot.

- **Reset Actions** occur when the alert is reset.
  
  Example: Write an event and data to the log when the alert actions complete.

- **Alert Integration** triggers the alert in other SolarWinds products integrated with the Orion Platform including ServiceNow Integration and Web Help Desk.

Troubleshoot cloud monitoring

This section details potential performance, usage, and polling issues you may encounter while monitoring cloud instances and VMs.
The Orion Platform tracks cloud events in the Alerts & Events > Events manager and displays alerts and events on the Cloud Summary page as well as Details pages for instances/VMs. For instances/VMs managed as nodes, check the Node Details page.

If an issue occurs on the cloud service side, explore the AWS Management Console or Azure Portal. Orion Platform issues may be related to cloud account configuration, throttling, or polling. Also, review cloud monitoring recommendations and requirements. Consult your system administrator as necessary.

If you contact SolarWinds Customer Support, make sure you have cloud account credentials available.

This section contains the following topics:

- Common issues
- Azure messages
- Expand troubleshooting
- SolarWinds Success Center
- THWACK

Common cloud monitoring issues

**Issue: The Orion Platform cannot access a cloud service account.**

If the Orion Platform cannot access a cloud account after entering credentials on the Add Cloud Account page, make sure you entered valid credentials. Consult your system administrator to confirm account configuration.

The Orion Platform supports VMs deployed via the Azure Resource Manager but not VMs created using a classic deployment model.

**Issue: "You are not authorized to perform this operation."**

This message appears if you lack adequate permissions to manage a cloud instance/VM. Check credentials and account configuration. Azure account requires the User Access Administrator role to manage account permissions and perform actions against VMs, such as stopping polling.

**Issue: Data does not display in resources on Cloud Summary or Cloud Instance/VM Details pages.**

Check credentials and account configuration. Navigate to the Cloud Summary and Cloud Instance/VM Details pages to determine if cloud services are throttling instances/VMs. For instances/VMs managed as nodes in the Orion Platform, check the Node Details page.

To ensure the Orion Platform can collect data using publicly available APIs accessed via HTTPS protocol, the Orion server must be configured to communicate with public services. Use the default setting — public — in community strings for polled devices.
**Issue: Slowed performance when polling data.**

Check the amount of cloud resources. For optimal performance, SolarWinds recommends the following limits:

- Up to 10 cloud service accounts
- Up to 1,000 instances/VMs to monitor
- Up to 1,000 volumes to monitor
- Up to 1,000 instances/VMs managed as nodes
- Up to 1,000 instances/VMs managed as nodes

If you exceed recommended limits, polling may slow or be throttled by cloud services. Consider expanding hardware, server sizing, CPU resources, memory, etc.

**Issue: "Error polling instance/VM. Error polling volume."**

This message appears if one or more polling issues reduced the amount of events and alerts that display in the Orion Web Console. A description is included, along with the specific instance/VM or volume. The message appears if the following issues occur:

- Error polling one or more metrics for an instance/VM
- Access error when polling an instance/VM
- Access error when polling a volume

Review the following potential issues and resolutions:

- For metric polling errors, check the log file.
- For cloud service access issues, check account credentials and permissions in the AWS Management Console, Azure Portal, and Orion Web Console. See [Configure cloud accounts for the Orion Platform](#).
- To ensure that the Orion Platform can collect data from cloud service APIs, make sure the Orion server uses the HTTPS protocol. Community strings for polled devices must use the default setting — public.

**Issue: "Error polling instances for cloud account."**

This message lists AWS instances that could not be polled or accessed.

Check [account credentials](#) and permissions in the AWS Management Console, as well as [account information](#) in the Orion Web Console. See [Configure AWS for cloud monitoring](#).

**Issue: "Error polling volumes for cloud account."**

This message lists volumes that could not be polled or accessed.

Check [account credentials](#) and permissions in the AWS Management Console, Azure Portal, and Orion Web Console.

**Issue: "Error polling VMs for cloud account."**

This message lists Azure VMs that could not be polled or accessed.

Check [account credentials](#) and permissions in the Azure Portal, as well as [account information](#) in the Orion Web Console. See [Configure Microsoft Azure for cloud monitoring](#).
Credentials required to add AD apps and/or deploy Orion agents to VMs may vary based on how Azure is configured for your organization. Ask your subscription administrator for details.

Issue: "Error polling auto-scaling groups for cloud account."

This message lists auto-scaling groups that allocate resources to match performance requirements could not be polled or accessed.

Troubleshooting: Check account credentials and permissions in the AWS Management console, Azure Portal, and Orion Web Console. See Configure cloud accounts for the Orion Platform.

Issue: Throttling applied at the account, instance/VM, or volume level. The instance/VM displays as Unknown - Throttling Error.

Cloud service APIs constantly check incoming monitoring requests against account limits. If polling requests exceed default or custom thresholds, cloud services return the HTTP status code 429 and apply throttling to block requests.

Cloud service throttling triggers default alerts in the Orion Platform that appear on the Cloud Summary and Cloud Instance/VM Details pages. Verify Orion Platform alerts and review cloud service usage plans. To prevent throttling issues, consider extending polling intervals and/or disabling API polling for specific resources. See AWS throttling and Azure throttling.

Issue: "AWS CloudWatch polling limit threshold exceeded."

AWS CloudWatch provides 1 million polling requests limit per calendar month at no charge. If the polling limit threshold is exceeded, verify Orion alerts, and review AWS usage.

To display estimated usage for the month, edit cloud account properties and review the CloudWatch API polling section. You can request a limit increase from AWS and/or disable CloudWatch polling at the account level. See AWS polling.

To avoid exceeding polling limits, consider toggling Auto Monitoring off when adding a cloud account to block polling for new instances launched and then discovered for an account. You can enable monitoring for individual instances later.

If you disable CloudWatch polling at the account level in the Orion Web Console, cloud services stop polling for metrics but continue to check resource status. After monthly free request limits are exceeded, costs are incurred for the remaining time frame.

Issue: "Azure polling limit threshold exceeded."

Azure provides 1 million standard API calls per calendar month at no cost and out-of-the-box alerts are included to alert you when polling limits are exceeded. Azure measures API requests according to the amount of data points returned; see Azure polling limits. Azure will charge a subscription or tenant account for overages, depending how Azure is configured.

To avoid exceeding polling limits, consider toggling Auto Monitoring off when adding a new cloud account to block polling for new VMs discovered for an account. You can enable monitoring for individual VMs later.
**Issue: Azure volumes do not display many statistics.**

Cloud services typically gather more data for instances/VMs than for volumes. The Orion Platform retrieves data from cloud services so data displayed for instances/VMs in the Orion Web Console may exceed data displayed for volumes.

If your organization uses both AWS instances and Azure VMs, you may notice that more information appears in the Cloud Volume Details resource for AWS instances. This is due to the fact that Azure does not provide individual metrics for Azure VM volumes. For example, Azure volumes always display the Up state because Azure does not yet provide volume status via API.

To retrieve more metrics, [manage VMs as nodes](#) in the Orion Platform.

**Issue: Why do Azure volumes always display as in an "Up" state in the Volume Details resource?**

Azure volumes always display the Up state because Azure does not yet provide volume status via API so the Orion Platform cannot retrieve and display that data.

**Issue: The following SocketException message "An operation was attempted on something that is not a socket" displays in the logs.**

This exception may occur if a large number of connections are open, which is common when more than 10 cloud accounts are polled simultaneously. Reduce the number of cloud accounts for optimal performance, as described in [Cloud monitoring recommendations](#).

**Issue: What does the SendAzureRequestsInBatch setting on the Advanced Configuration page control?**

When the SendAzureRequestsInBatch option is enabled, the Orion Platform uses batch operations to poll Azure VMs. If a Microsoft Azure account includes over 1000 VMs, the Orion Platform may receive a Status Code 503 - Service Unavailable error, as recorded in the VMwareJobs log file stored in the SolarWinds\Logs\VIM\Jobs folder.

Per [Cloud monitoring recommendations](#), limit the number of cloud VMs/instances to 1000 for optimal performance. Another option is to disable batch operations for Azure polling.

2. Disable the SendAzureRequestsInBatch setting.
3. Increase the AzureOneTimeJobTimeout value from 00:03:00 to 00:06:00 to allow extra time to add Azure accounts when SendAzureRequestsInBatch is disabled.

**Issue: The Azure Portal uses two terms for the same value: Tenant ID and Directory ID.**

Tenant ID and Directory ID are the same value but are referred to both ways in the Azure UI and documentation. Azure also refers to the Client ID as the Application ID and Application Key. See [Find cloud account credentials](#) for details.
Issue: The number of Azure requests in the Edit Account wizard varies from the number of requests in the Edit Account wizard.

As described in Understand Azure polling limits, Azure uses datapoints to calculate the number of API requests; each request is equal to 1440 datapoints but individual API requests may consume more or less points. The Orion Platform displays the total of individual API requests in the Edit Account wizard so the number of Azure requests should be close but may not match exactly.

Issue: VMAN recommendations do not affect cloud instances/VMs.

VMAN recommendations that trigger actions in virtual environments such as vCenter do not impact cloud instances/VMs.

Azure messages

The following messages may appear when performing actions against Azure VMs.

- "Authentication_Unauthorized."
- "No subscription found in the context."
- "Your Azure account does not have authorization to perform action 'Microsoft.Authorization/roleAssignments/write' over scope '/subscriptions/{guid}'."

These messages appear if an Azure account does not have permission to register the AD app that provides read access to the Orion Platform so it can poll for status and metrics. Typically, this occurs if an organization only allows administrators to register apps and an account is not linked to an administrator role. Ask the subscription administrator to either assign an administrator role to the Azure account or enable users to register apps. See Configure Microsoft Azure for cloud monitoring.

- Credentials required to add AD apps and/or deploy Orion agents to VMs may vary according to how your organization uses Azure. Ask your subscription administrator for details.

Expand troubleshooting

To better manage and troubleshoot cloud instances/VMs and volumes:

- Troubleshoot cloud monitoring with PerfStack to compare metrics, data, and logs across collected for nodes and Orion Platform products.
- Create cloud application monitors and templates for SAM-managed applications, OS, and cloud instances/VMs managed as nodes with out-of-the-box component monitors and custom scripts.

Check the following logs that are related to cloud monitoring:

- Business Layer logs:
  - C:\ProgramData\Solarwinds\Logs\CloudMonitoring
- Polling jobs:
  - C:\ProgramData\Solarwinds\Logs\VIM\Jobs
  - Search for “Cloud” in the log files.
- Collector logs:
  - C:\ProgramData\Solarwinds\Collector\Logs
  - Search for "Cloud" in the log files.
Troubleshoot cloud monitoring with PerfStack

Use the Performance Analysis Dashboard (PerfStack) to troubleshoot multi-faceted issues in cloud applications and infrastructure. Create consolidated data views as charts and graphs to collect and compare metrics, data, and logs for end-to-end hybrid troubleshooting for monitored and managed nodes and more.

Instead of reviewing numerous views and resources in the Orion Web Console depending on the Orion products, features, metrics, and nodes involved, use the Performance Analysis dashboard to:

- Visualize correlated data to analyze metrics, relationships, and data.
- Compile all metrics into a single dashboard to analyze and find key issues.
- Merge metrics into charts to see gaps and spikes.
- Spot trending issues by examining the history of alerts, metrics, usage, and more.
- Determine when performance starts to ebb and flow across resources and applications.
- Continue monitoring resources after resolving issues to verify performance.

For example, if a monitor detects an issue for a cloud-based application, an alert may be triggered to notify the application owner who may escalate the issue to a network or system administrator. Instead of searching for alerts on Node Details pages for the monitored application, server, and network, the owner can create a project on the PerfStack dashboard to investigate the issue and send those details to administrators to speed resolution and reduce downtime.

To access PerfStack in the Orion Web Console, click My Dashboards > Home > Performance Analysis. Add Entities to create a new analysis project and search for the element experiencing performance issues. For details, see Troubleshoot network issues with Performance Analysis dashboards in the SolarWinds Success Center. The SolarWinds online IT community, THWACK, also includes PerfStack information and videos.
Monitor container services in the Orion Platform

Containers are lightweight, executable packages of software that include everything needed to run an application: code, system tools, system libraries, and settings. Instead of shipping a full OS and software, application containers include an application’s code, configurations, and dependencies into a single package, resulting in enhanced environmental consistency, operational efficiency, and version control.

Similar to VMs, containers isolate applications and their dependencies into self-contained units that can run anywhere without interfering with each other. Unlike VMs that each have their own virtual OS and hardware, containers share the host system kernel with other containers to save space, increase efficiency, and improve developer productivity.

The Orion Platform supports monitoring for containers deployed to Linux nodes in the Docker, Docker Swarm, Kubernetes, and Apache Mesos environments. After adding container services in the Orion Web Console, you can display details about your container infrastructure, including container hosts and deployments. Various widgets provide container status and performance metrics such as CPU usage and memory.

You can display container service metrics in different places in the Orion Web Console, including:

- The AppStack Environment
- Performance Analysis dashboards (PerfStack)
- Node Detail pages
- Orion Maps

For example, the following screenshot shows how you can hover over a container service in the AppStack Environment to display details about it:
Here is an example of a container widget created in PerfStack:

![Container Widget Example](image)

**Container lifespans and the Orion Platform**

Some containers are created for long-term use but many are created for a specific, temporary purpose and deleted afterward. When you add a container service, the Orion Platform deploys an Orion Monitor container to each node in a cluster and deploys an Orion Aggregator container to the master node in the cluster. While other containers are created and deleted, the Orion Aggregator container remains on the master node to report status and metrics for Orion Monitor containers. After seven days with no activity, containers stop appearing in container widgets displayed in the Orion Web Console.

![Tip: Orion Platform deploys Orion agents to nodes for container monitoring. To learn more about Orion agents, see the Orion Platform Administrator Guide.]

**Container service monitoring requirements**

Before adding container services to the Orion Platform, review [Supported container environments](#). Each environment has unique requirements and steps to remove container data if you decide to delete container services later.

![Warning: When you add a container service, the Orion Platform credentials are stored in a plain text file that stays in memory for two hours. SolarWinds recommends creating an Orion user account specifically to add container services so no actual user credentials are exposed.]

**Container service monitoring and licensing**

Only container services being monitored on host servers added as Orion nodes count against licenses. To monitor all containers in a single cluster, add each server from the cluster as an Orion node.
Manage container services

With the necessary Administrator privileges, you can add container services on the Container Services page to begin monitoring them. This page lists container services connected to the Orion Platform, including name, status, number of containers, environment type, and the IP address of the Orion Aggregator container host server. The Last Seen values indicate the last date and time the Orion Aggregator container reported data to the Orion Platform.

Deleted container services continue to appear on the Container Services page for seven days, by default. See Container lifespans.

To access the Container Services page:

1. Click Settings > All Settings.
2. Under Node & Group Management, click Manage Container Services.

Add a container service

You can use the Add Container Service wizard to specify details about a service and generate an environment-specific script that will:

- Download a deployment file to a single node — usually an orchestrator’s master node — in the container environment.
- Deploy an Orion Monitor container to every node in the cluster to track node status and metrics.
- Deploy an Orion Aggregator container to a single node in the container environment to collect data from Orion Monitor containers. The Orion Aggregator container reports its own status, plus status and metrics for each Orion Monitor container, to the Orion server every five minutes.

Two types of agent plug-ins are also deployed:

- A CleanUp agent plug-in runs daily to clear all data, including images and environment variables, for containers reported as being deleted for over 7 days.
A StatusSetUp agent plug-in checks the status of the Orion Aggregator container every minute.

- If the Orion Aggregator container fails to connect to the Orion server for two, consecutive five-minute intervals, the container service status changes to Down and the container status switches to Unknown.
- If the Orion Aggregator container fails to report metrics from Orion Monitor containers for two, consecutive five-minute intervals, the container status switches to Unknown.

⚠️ When you add a container service, credentials are stored in a plain-text file that stays in memory for two hours. SolarWinds recommends creating an Orion user account specifically for use when adding so no actual user credentials are exposed.

To add a container service:

1. Review requirements for [Supported container environments](#).
2. Click Settings > All Settings.
4. When the Container Services page appears, click Add.

5. On the first page of the Add Container Service wizard, provide service details, and then click Next.
6. On the Orion credentials page, provide a Username and select the optional "User secure connection" check box. Click Next to advance to the Script page.
7. On the Script page, click the Copy icon to save the command generated by the Orion Platform to the Windows Clipboard.

8. With an SSH client, connect to the node, open a command line, and run the script that performs different actions based on the environment type. See Supported container environments for details.

   Need an SSH client? Try the free SolarWinds Solar-PuTTY tool.

9. Return to the Orion Web Console and click Close to exit the wizard.

10. Refresh the Orion Web Console to display the new service on the Container Services page. This may take up to 5 minutes.

You can adjust polling intervals for container services on the Global tab of the Advanced Configuration page (http://localhost/Orion/Admin/AdvancedConfiguration/Global.aspx). Changes apply to future container services added to the Orion Platform.

Delete a container service

To delete a container service in the Orion Web Console:

1. Follow environment-specific steps to remove container data from nodes. See Supported container environments for details.

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


   The container service status should have switched to Down when you removed container data. If not, repeat step 1.
4. On the Container Services page, select the container service you want to delete.
5. Click Delete.

Wait for the list of container services to refresh. This may take up to 10 minutes — the equivalent of two polling intervals.

**Supported container environments**

The Orion Platform supports the several container environments (also called "orchestrators"), as described in the following sections:

- [Docker requirements, installation script examples, and container removal steps](#)
- [Docker Swarm requirements, installation script examples, and container removal steps](#)
- [Kubernetes requirements, installation script examples, and container removal steps](#)
- [Apache Mesos requirements, installation script examples, and container removal steps](#)

If you decide to **delete a container service** later, follow environment-specific steps to remove Orion container data from the node manually before deleting the service in the Orion Web Console.

**Docker requirements, installation script examples, and container removal steps**

To monitor Docker containers in the Orion Platform, you'll need:

- Docker Engine 17.12 or later
- Compose file 3.5 or later
- SSH access to the master server
- Sudo privileges on the master server
Docker installation script

When you add a container service on the Container Services page, the Add Container Service wizard generates a script that you can copy to the Windows Clipboard. Connect to the master server via SSH, open a command line, and run the script, which looks something like this:

```
curl -o docker-compose.yaml #endpoint#
sudo docker-compose up -d
```

SolarWinds recommends that you execute script commands in a directory that does not already have a docker-compose.yaml file. Consider creating a new Orion directory on the server where you can run script commands.

The script downloads the docker-compose.yaml file and runs it with superuser privileges.

Remove Orion container data from nodes in Docker

Before you delete a container service in the Orion Web Console, remove Orion containers and images from the node manually with Docker commands.

1. Connect to the node via SSH.

   Need an SSH client? Try the free SolarWinds® Solar-PuTTY tool.

2. Get the IDs for the sw_orionaggregator and sw_orionmonitor containers by running:

   ```
sudo docker ps | grep sw_
```

3. Remove the sw_orionaggregator and sw_orionmonitor by running the following commands for each ID:

   ```
sudo docker stop [container_id]
sudo docker rm [container_id]
```

4. Get a list of images and note the IDs for the docker.dev.local/scope2orion and weaveworks/scope:latest containers.

   ```
sudo docker images
```

5. Run the following command for each image ID and container acquired in step 4:

   ```
sudo docker rmi [image_id]
```

The service status switches to Down on the Container Services page. Now you can delete the container service by selecting its check box and clicking Delete.
Docker Swarm requirements, installation script examples, and container removal steps

To monitor Docker Swarm containers in the Orion Platform, you'll need:

- Docker Engine 17.12 or later
- Docker Compose file format 3.5 or later
- SSH access to the master server
- Sudo privileges on the master server

Docker Swarm installation script

When you add a container service on the Container Services page, the Add Container Service wizard generates a script that you can copy to the Windows Clipboard. Connect to the master server via SSH, open a command line, and run the script, which looks something like this:

```
curl -o cman-swarm.yaml #endpoint#
sed -i "s/%HOSTNAME%/$(hostname)/g" cman-swarm.yaml
sudo docker stack deploy -c cman-swarm.yaml sw
```

The script downloads the cman-swarm.yaml file, sets the hostname in the file to the master server, and starts a service named "sw" to deploy an sw_orionmonitor container to each server in the swarm.

Remove Orion container data from nodes in Docker Swarm

Before you delete a container service in the Orion Web Console, remove Orion containers and images from the nodes (or cluster of nodes) manually.

1. Connect to the node via SSH.

   Need an SSH client? Try the free SolarWinds Solar-PuTTY tool.

2. Run the following commands to remove the sw_orionaggregator and sw_orionmonitor services:

   ```
sudo docker service rm sw_orionaggregator
sudo docker service rm sw_orionmonitor
   ```

3. Run the following command to get a list of images and note the IDs for docker.dev.local/scope2orion and weaveworks/scope:latest.

   ```
sudo docker images
   ```

4. Run the following command for each image:

   ```
sudo docker rmi [image_id]
   ```
The service status switches to Down on the Container Services page. Now you can delete the container service by selecting its check box and clicking Delete.

Kubernetes requirements, installation script examples, and container removal steps

To monitor Kubernetes containers in the Orion Platform, you'll need:

- A Kubernetes platform with one of the following API versions enabled:
  - v1
  - rbac.authorization.k8s.io/v1beta1
  - rbac.authorization.k8s.io
  - apps/v1beta1
  - extensions/v1beta1
  - Kubelet agent listening on port 10255
- SSH access to the master server
- Sudo privileges on the master server

Kubernetes installation script

When you add a container service on the Container Services page, the Add Container Service wizard generates a script that you can copy to the Windows Clipboard. Connect to the master server via SSH, open a command line, and run the script, which looks something like this:

```
curl -o orion-kubernetes.yaml #endpoint#
sudo kubectl apply -f orion-kubernetes.yaml
```

The script downloads an orion-kubernetes.yaml file to define an orion namespace and deploys the Orion Aggregator and Orion Monitor containers to the namespace.

Remove Orion container data from nodes in Kubernetes

Before you delete a container service in the Orion Web Console, delete the Orion namespace from the node. For Kubernetes, namespaces are logical entities that represent cluster resources for usage of a set of users — in this case, the “user” is the Orion Platform. Remove the namespace, to delete Orion containers and images from a node.

1. Connect to the node via SSH.

   ![tip] Need an SSH client? Try the free SolarWinds Solar-PuTTY tool.

2. Run the following command:

   ```
sudo kubectl delete namespaces orion
   ```
The service status switches to Down on the Container Services page. Now you can delete the container service by selecting its check box and clicking Delete.

Apache Mesos requirements, installation script examples, and container removal steps

To monitor Apache Mesos containers in the Orion Platform, you'll need:

- Docker Engine 17.12 or later
- Apache Mesos
- An SSH connection to the master server
- Sudo privileges on the master server

Apache Mesos installation script

When you add a container service on the Container Services page, the Add Container Service wizard generates a script that you can copy to the Windows Clipboard. Connect to the master server via SSH, open a command line, and run the script, which looks something like this:

```
curl -o cman-mesos.sh #endpoint#
sudo bash cman-mesos.sh
```

This script downloads a cman-mesos.sh bash script and runs it with superuser privileges to deploy required Apache Mesos applications:

- An OrionAggregator application on the master server, and
- OrionMonitor applications on each node in the cluster.

Remove Orion container data from nodes in Marathon

Before you delete a container service in the Orion Web Console, delete the orion-aggregator and orion-monitor. Apache Mesos applications deployed on the master server: The following steps describe how to remove container data via the Marathon web page but you can also use API commands or another Mesos framework to remove applications from nodes.

1. Open the Marathon web page.
2. If necessary, adjust the default loopback IP address, 127.0.0.1, to match the address in the master state.json file.
3. Navigate to the orion-aggregator application.
4. Click the gear icon, and then click Destroy.
5. Repeat steps 3 and 4 for the orion-monitor application.

The service status switches to Down on the Container Services page. Now you can delete the container service by selecting its check box and clicking Delete on the Container Services page in the Orion Web Console.

Troubleshooting Mesos issues

The following services must be running on the Mesos master server:

- docker
- mesos-master
- zookeeper
- marathon

These services must be running on every Mesos agent:

- docker
- mesos-agent

To check the status of a service, run:

```
sudo service [service_name] status
```

If the Mesos master can't reach the Mesos agents, try flushing the IP tables with this command:

```
sudo iptables -F
```
Monitor virtual infrastructure

SolarWinds Virtual Infrastructure Monitor (VIM) is the feature that enables virtual monitoring directly from the Orion Web Console.

It is available as a feature of SolarWinds NPM or SolarWinds SAM, in integration with SolarWinds VMAN, or as a standalone solution.

VIM monitors the following:

- ESXi and ESX Server version 4.1 or later
- VMware vSphere version 4.1 or later

Prerequisites to monitoring virtual infrastructure

- SolarWinds NPM or SolarWinds VIM is installed.
- SNMP on your virtual servers is enabled.
- VMware Tools are installed on all virtual machines you want to monitor.

If your virtual machines are on monitored ESXi and ESX servers, VMware Tools are not a requirement but provide access to additional information, such as IP addresses.

- ESX credentials on ESX servers are created.
- You virtual infrastructure is discovered.

Create ESX server credentials for SolarWinds Orion products

For polling performance data, you must create credentials on your ESX Servers for the SolarWinds Orion polling engine.

To create the credentials, log in to the ESX server, and create a user. For more information, consult your vendor documentation.

Credentials created for the polling engine must have read-only rights as a minimum.

Enable SNMP on VMware ESXi and ESX servers

SolarWinds Orion uses SNMP to poll performance data from VMware ESXi and ESX Servers. In order to make this performance data available to SolarWinds Orion, you must enable SNMP on your ESXi and ESX Servers.

Consult VMware's documentation for information on enabling SNMP.
VMware only makes a limited amount of information available to SNMP queries for VMware ESXi and ESX Servers version 4.0 and higher. To access additional information on these versions, we use the VMware API.

**Change VMware credentials in the Orion Web Console**

If credentials for a VMware account change on the device, update the credentials in the Orion Web Console. You must keep your VM credentials updated in the Orion Web Console to provide access for management tools and monitor data.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Virtual Devices.
4. Click the VMware Credentials Library tab.
5. Select the credential you want to update, and click Edit Credential to make the necessary changes.

**Add virtual servers for monitoring**

To fully monitor and manage Hyper-V nodes, VMware vCenter, ESX servers, and virtual machines in the Orion Web Console, you should add the virtual system as a node. You can add a node through discovery automatically or manually by adding a node.

Add the nodes using [Network Sonar Discovery](#).

1. Log in to the Orion Web Console as an administrator.
2. Launch Network Discovery in the Orion Web Console through Settings > Network Discovery > Add New Discovery.
3. On the Virtualization page, select Poll for VMware, and if the vCenter or ESX Credentials are not listed, add them.
   
   Credentials allow you to use management tools directly through the Orion Web Console.
5. Complete the wizard and import the results.
Assess the status of the virtual environment

The Virtualization Summary view shows the overall status of your virtualized infrastructure.

1. Log in to the Orion Web Console.
2. Click My Dashboards > Home > Virtualization in the menu bar.
View ESX host details

Click an ESX Host server in the Virtualization Summary page to open the ESX Host Details view.
Monitor Quality of Experience metrics

On the Quality of Experience (QoE) dashboard you can monitor traffic on your network. QoE uses Packet Analysis Sensors to provide packet-level traffic information about key devices and applications.

With QoE, you can:

- Compare statistics, such as network response time (TCP Handshake) and application response time (Time to First Byte) to determine if a bottleneck is on the application or the network.
- Use data volume trends to pinpoint traffic anomalies and investigate the cause.
- Monitor risky types of traffic, for example, traffic that might bypass firewalls or lead to data leaks.

With the ability to analyze packet traffic, QoE provides real observed network response time (NRT) and application response time (ART). In addition, Packet Analysis Sensors can classify and categorize traffic for over 1000 different applications by associated purpose and risk-level.

Traffic data is captured using Packet Analysis Sensors. These sensors collect packets using either a dedicated Windows SPAN or mirror port monitor or directly on your Windows server. Packet Analysis Sensors capture packets from the local network interface (NIC) and then analyze collected packets to calculate metrics for application performance monitoring. These metrics provide information about application health and allow you to identify possible application performance issues before they are reported by end-users.
For more information about specific implementations of QoE, see Common Packet Analysis Sensor deployment scenarios.

How SolarWinds Packet Analysis Sensors work

SolarWinds provides two types of Packet Analysis Sensors to monitor and analyze your network traffic.

- Packet Analysis Sensors for Networks (network sensor) collect and analyze packet data that flow through a single, monitored switch for up to 50 discrete applications per node.
- Packet Analysis Sensors for Servers (server sensor) collect and analyze packet data of specific applications that flow through a single node.

After a sensor is deployed and configured, it captures packets and analyzes them to calculate performance metrics for the monitored applications. An included communication agent allows the sensor to send back sampled packet data to the Orion server, which includes statistics such as volume, transactions, application response time, and network response time for each application on a node. The packet data are then saved to the SolarWinds Orion database. The information is used to populate your QoE dashboard. You can configure how long you retain the packet data in the Database Settings section of the Polling Settings screen.

Network Packet Analysis Sensor (NPAS)

Your network administrator must create a dedicated SPAN, mirror port, or in-line tap monitor on the physical or virtual switch before you can deploy or configure a network sensor.

After you deploy and configure the network sensor to the node monitoring the switch, the sensor captures all packets that flow through the switch and categorize the packets by application.

Packets that correspond to monitored applications are analyzed for QoE metrics, such as response times or traffic volume. Data are then sent to the Orion server using the SolarWinds agent.

Server Packet Analysis Sensor (SPAS)

A SPAS can monitor:

- packet traffic on a single node
- up to 50 applications per node

A SPAS captures packets traveling to and from the node. It identifies packets that are sent to or from the monitored application and analyzes them for QoE metrics, such as response time or traffic volume. Data are then sent to the Orion server using the agent.

Limitations to Packet Analysis Sensors

The number of nodes you can monitor is limited by the data throughput per node, the number of cores, and the amount of RAM available on the monitoring server.
The system requirements increase for every 100 Mbps of traffic.

<table>
<thead>
<tr>
<th>sensor limitations</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum throughput (NPAS and SPAS)</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>Maximum number of nodes per sensor (NPAS)</td>
<td>50 nodes</td>
</tr>
<tr>
<td>Maximum number of node and application pairs (NPAS and SPAS)</td>
<td>50,000 pairs</td>
</tr>
<tr>
<td>Maximum number of sensors deployed on your network</td>
<td>1,000 sensors</td>
</tr>
<tr>
<td>Maximum number of applications per node or sensor (NPAS and SPAS)</td>
<td>1,000 applications per node</td>
</tr>
</tbody>
</table>

Common Packet Analysis Sensor deployment scenarios

After you install your Orion platform product, deploy network sensors on a server dedicated to monitoring a network switch or deploy server sensors directly on physical or virtual servers or workstations.

If you select QoE during the installation, a sensor is already on your SolarWinds Orion server collecting data about applications that SolarWinds Orion is using.

Based on how you want to aggregate the returned QoE metrics, there are three main deployment scenarios per sensor type.

<table>
<thead>
<tr>
<th>Aggregation level</th>
<th>Sensor Deployment</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>I have access to my network (NPAS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per application</td>
<td>Deploy an NPAS to a port mirror that monitors all traffic to and from the application</td>
<td>Automatic</td>
</tr>
<tr>
<td>Per site</td>
<td>Deploy an NPAS to a port mirror that monitors all traffic to and from the site</td>
<td>Add a sampling of endpoints to the NPAS as managed nodes</td>
</tr>
<tr>
<td>Per client</td>
<td>Deploy an NPAS to a port mirror that monitors all traffic to and from the site</td>
<td>Add all of the endpoints to the NPAS as managed nodes</td>
</tr>
<tr>
<td>I have access to my application servers (SPAS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per application</td>
<td>Deploy the SPAS directly on the application server</td>
<td>Automatic</td>
</tr>
<tr>
<td>Per site</td>
<td>Deploy the SPAS to select endpoints</td>
<td>Automatic</td>
</tr>
<tr>
<td>Per client</td>
<td>Deploy the SPAS to all endpoints</td>
<td>Automatic</td>
</tr>
</tbody>
</table>
When deploying both network and server sensors on the same network, ensure that you do not monitor the same node with multiple sensors. This impacts the QoE metrics.

- All monitored nodes must be managed by your Orion Platform product before they can be monitored by sensors.
- Applications and nodes are detected by default if the node is managed by your Orion server. If packet data is not collected, navigate to Settings > All Settings, and click on QoE Settings. Click Manage Global QoE Settings, and activate the auto-detect option. You can also manually monitor applications and managed nodes or ignore them.

Aggregation per application

This deployment scenario provides a broad indication of the overall response time between computers and the monitored application.

Aggregation with access to network (NPAS)

- Create a port mirror, SPAN, or network tap on the switch with all the network traffic to or from the application.
- You can monitor multiple applications using the same NPAS.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor.
3. Select the Network option, and then click Add Nodes.
4. Choose the node with the port mirror, SPAN, or network tap setup to monitor your network switch.
5. Assign and test the credentials for the selected node.
6. Click Add Nodes and Deploy Agents to deploy the network sensor to the node.

Aggregation with access to application servers (SPAS)

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor.
3. Select the Server option, and then click Add Nodes.
4. Choose the nodes with the application you want to monitor.
5. Assign and test the credentials for each node.
6. Click Add Nodes and Deploy Agents to deploy a sensor on the node.

Aggregation per site

This deployment scenario provides an aggregated response time per monitored site or network to the application. For example, the response time from your Detroit office to your datacenter is one second, but the response time from Boston to your datacenter is seven seconds. If you used the aggregation per application deployment method, the response time for the application is four seconds.

This method requires you to identify users who best represent how the application is used. You then use the users' computers as data points to monitor with Packet Analysis Sensors.
Aggregation per site with access to network (NPAS)

- Create a port mirror, SPAN, or network tap on the switch with all the network traffic to or from the application.
- You can monitor multiple applications using the same NPAS.
- Identify a sample set of users whose computers are monitored by the NPAS.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor.
3. Select the Network option, and then click Add Nodes.
4. Choose the node with the port mirror, SPAN, or network tap setup to monitor your network switch.
5. Assign and test the credentials for the selected node.
6. Click Add Nodes and Deploy Agents to deploy the network sensor to the node.
Aggregation per site with access to application servers (SPAS)

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor.
3. Select the Server option, and then click Add Nodes.
4. Choose the nodes with the application you want to monitor.
5. Assign and test the credentials for each node.
6. Click Add Nodes and Deploy Agents to deploy a sensor on the node.

Aggregation per computer

This deployment scenario provides highly granular response times for the application because metrics for each computer are recorded.

One or two workstations can experience long response times, which may not be caught when aggregated per site or per application.

This method requires all workstations to be managed within your Orion Platform product.
Aggregation per computer with access to network (NPAS)

1. Create a port mirror, SPAN, or network tap on the switch with all the network traffic to or from the application.
2. You can monitor multiple applications using the same NPAS.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor.
3. Select the Network option, and then click Add Nodes.
4. Choose the node with the port mirror, SPAN, or network tap setup to monitor your network switch.
5. Assign and test the credentials for the selected node.
6. Click Add Nodes and Deploy Agents to deploy the network sensor to the node.
Aggregation per computer with access to application servers (SPAS)

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor.
3. Select the Server option, and then click Add Nodes.
4. Select the all user computers to monitor.
5. Assign and test the credentials for each node.
6. Click Add Nodes and Deploy Agents to deploy an agent on the node.

Monitor traffic to and from a port mirror, SPAN, or network tap

Network sensors monitor all packets that flow through the switch and categorize the packets by application.

After you deploy a network sensor to the port mirror, SPAN, or network tap, the sensor monitors packets to and from the node, identifies the application or the URL, and analyzes the packets for QoE metrics, such as response time or traffic volume.

Before you begin

- Data from sensors is directed to the polling engine assigned to the node when the sensor was deployed.
- A high number of applications or nodes can cause performance issues with the sensors.
The network sensor must be installed on a Windows computer that is monitoring the switch's SPAN or mirror port.

Install the network sensor

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor.

3. Select Network, and click Add Nodes.

4. Move the node that monitors your switch to the Selected Nodes panel, and click Add Selected Nodes.

⚠️ Make sure you select the Windows machine that is monitoring the SPAN or mirror port of the switch.

5. Assign and test the credentials for the node, and click Submit.
6. Click Add Nodes and Deploy Agents.

When the sensors are successfully deployed, a message is displayed in Notifications.

Deploying the sensor and receiving the first set of data can take several minutes. When the deployment is finished, select the sensor on the Manage Quality of Experience (QoE) Packet Analysis Sensors page, click Edit Sensor, and verify the selected NIC.

Monitor website traffic based on domains

After you deploy a network sensor, you can filter application traffic based on domain names instead of all http traffic.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage Global QoE Settings.
3. Set the HTTP application domain detection level.

![Global QoE Settings](image)

4. Set the Auto-detect QoE applications option to Active, and click Submit.

QoE can automatically detect the first 50 applications, or you can add specific applications.

Discovered applications have the "No Risk" Risk Level and the "Both Business and Social" Productivity Rating associated with them. To modify the Risk Level and Productivity Rating, click QoE Settings > Manage (QoE) Applications, and edit the application.

Use the Global QoE Settings page to disable monitoring or discovery of multiple applications. Select the applications, and click Disable Monitoring or Disable Discovery.

Nodes are automatically detected and added by default. To specify which nodes and applications to monitor manually, see Monitor QoE applications and nodes.

### Monitor traffic to and from a specific node

After you deploy a server sensor to the application node, the sensor monitors packets to and from the node, identifies the application or the URL, and analyzes the packets for QoE metrics, such as response time or traffic volume.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors, and click Add Packet Analysis Sensor.

![Manage Quality of Experience](image)

3. Select Server, and click Add Nodes.

![Packet analysis sensor type:](image)

4. Move the Windows nodes that will host the server sensors to the Selected Nodes panel, and click Add Selected Node.
5. Assign and test credentials for each node, and click Submit.
6. Click Add Nodes and Deploy Agents. QoE auto-discovers the applications on the servers.

When the sensors are successfully deployed, a message is displayed in Notifications.
Deployment may take some time and will run as a background process. QoE automatically chooses settings, including the interface to capture traffic data and limits to memory and CPU, during deployment. You can change these settings after deployment is complete by selecting the sensor and clicking Edit. You can confirm the deployment status on the Manage QoE Packet Analysis Sensors page.

To specify manually which applications to monitor, see Monitor applications for QoE. Applications are automatically detected and added by default.

Remove a sensor

Removing a sensor from a node is a two-step process. First delete the sensor using the Orion Web Console, and then remove the communication agent directly from the node.

1. Delete the sensor using the Orion Web Console:
   a. Click Settings > All Settings in the menu bar.
   b. Click QoE Settings > Manage QoE Packet Analysis Sensors.
   c. Select the node.
   d. Click Delete Sensor.
   e. Click Delete when prompted.

2. Remove the agent directly from the node:
   a. Log in to the computer with administrative credentials.
   b. Navigate to Control Panel > Programs and Features.
   c. Select SolarWinds Agent.
   d. Click Uninstall.
   e. Follow the onscreen prompts to completely uninstall the agent.

The sensor is removed from the list and the communication agent is uninstalled and cannot gather traffic data or send data.

Monitor QoE applications and nodes

By default nodes and applications are automatically monitored by QoE when you deploy a Network or Server Sensor. You can automatically filter which nodes or applications are monitored.

See Global QoE Settings for more information on changing these settings.

Server Sensors automatically monitor the top 50 applications on the node they are installed on based on the global settings. You can change which applications are monitored after the sensor is deployed.
Manage global QoE settings

You can control how Packet Analysis Sensors behave by changing the settings on Manage Global QoE Settings page. Settings are distributed to sensors regularly when the agent is updated. You can manually update an agent from the Manage Agents page.

QoE applications

Control how you monitor QoE applications for both Network Packet Analysis Sensors and Server Packet Analysis Sensors.

Auto-detect QoE applications

Use this to detect and monitor traffic associated with all applications that fulfill the auto-detection rules defined on this page. This is active by default. You must select applications manually when this option is disabled.

If you automatically detect nodes, you should also automatically detect applications to receive all metrics.

HTTP application domain detection level

Choose how QoE breaks up monitored http traffic.

- Top level (http://*) - Monitor all http traffic.
- Second level (http://hostname/*) - Separate and monitor http traffic based on domains.
- Third level (http://hostname/path1/*) - Separate and monitor http traffic based on the domain and first level directory within each domain.

Add auto-detected applications

Refine the monitored applications by choosing to monitor all application traffic sources, traffic destinations, or all application traffic. Packet sources and destinations are based on the source or destination IP address included in the packet.

- Transaction destinations (servers) - Monitor applications that receive traffic based on the destination IP address of the packet.
- Transaction sources (client) - Monitor applications that generate traffic based on the source IP address of the packet.
- Either a source or destination - Monitor all application traffic.

For each node, include top X application that have at least Y% of total QoE traffic.

Filter the number of monitored applications to applications that generate a certain amount of network traffic.

Nodes with QoE traffic

Control how you monitor QoE nodes for Network Packet Analysis Sensor.
Auto-detect QoE nodes

Use this to detect and monitor the first 50 nodes with network traffic. This is active by default. You must select nodes manually when this option is disabled.

If you automatically detect nodes, you should also automatically detect applications to receive all metrics.

Add auto-detected monitored nodes

Further refine the nodes that are monitored by choosing to monitor all nodes that are traffic sources, traffic destinations, or all nodes that generate or receive network traffic. Packet sources and destinations are based on the source or destination IP address included in the packet.

- Transaction destinations (servers) - Monitor nodes that receive traffic based on the destination IP address of the packet.
- Transaction sources (client) - Monitor nodes that generate traffic based on the source IP address of the packet.
- Either a source or destination - Monitor all traffic.

Manage QoE Packet Analysis Sensors

Nodes that are defined as QoE Sensors appear on this page, as well as the nodes and applications that are being watched by each node.

- Each sensor can support up to 50 applications.
- PPPoE packets are not processed by QoE sensors.

Add a Packet Analysis Sensor to a node

Use the Add Packet Analysis Sensor wizard to select the nodes on which you want to deploy packet analysis sensors.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors.
3. Click Add Packet Analysis Sensor.
4. Select either the Server or Network sensor type option.
   - Server sensor - Installs an agent and QoE sensor on the selected Windows servers, then collects data locally on those servers.
   - Network sensor - Installs an agent and QoE sensor on dedicated Windows servers monitoring SPAN or mirror ports. Collects packet data for any specified nodes/applications sending traffic through the monitored port.
5. Click Add Nodes.
6. Choose the Windows nodes that you want to deploy your sensors on.
7. Test the credentials for each node.
8. Click Add Nodes and Deploy Agents to deploy an agent on the node. Deployment may take some time and will run as a background process.

   QoE automatically chooses settings such as interface to capture traffic data, as well as memory and CPU limits, during agent deployment. You can change these settings once deployment is complete by selecting the sensor and clicking Edit.

   When deployment is complete, a message is added to the notification area. You can also check the status on the Manage QoE Packet Analysis Sensors page.

9. Specify which nodes and applications to monitor. The steps for specifying nodes and applications can be found in Monitor QoE applications and nodes.

Disable a sensor

Sensors are enabled by default. You can disable a sensor as a troubleshooting tool or to disable a sensor if it is overloaded with traffic. A disabled sensor will not collect traffic information about any of the nodes listed for that sensor.

   1. In the Manage Quality of Experience (QoE) Packet Analysis Sensors page, select the sensor and click Disable Sensor.

Delete a sensor

Deleting a sensor also deletes all of the nodes and applications associated with the sensor. It does NOT delete the nodes from Orion or the applications from the Manage QoE Applications page).

   1. In the Manage Quality of Experience (QoE) Packet Analysis Sensors page, select the sensor and click Delete Sensor.

Delete nodes from Network sensors

Nodes cannot be deleted from Server sensors since they only record traffic on the node the sensor is installed on.

View the status of the Sensor

A status can be whether sensor is connected or not, if it is in the process of being deployed, and so forth. You can also access the Manage Agents page from here by clicking Manage Agent next to the sensor's status.

   1. In the Manage Quality of Experience (QoE) Packet Analysis Sensors page, view the Agent Status column.

Monitor applications for QoE

Applications are automatically monitored when traffic is detected by the Packet Analysis Sensor. However, you can manually select specific applications to monitor. QoE installs with the ability to monitor over 1000 pre-defined applications, including FTP, RDP, CIFS, SQL, and Exchange. You can also define your own custom HTTP applications.
Because of the hardware requirements needed to process large amounts of traffic, SolarWinds recommends that you preferentially monitor business-critical nodes and applications.

- You should not assign more than 50 applications to a single node due to potential performance issues. However, you can monitor up to 1000 applications.

Monitor QoE applications automatically

While QoE sensors automatically detect and monitor applications by default, the settings may have changed or you may have upgraded from a version of QoE that does not automatically monitor applications.

- Only applications that meet the criteria selected in QoE Applications are monitored automatically.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage Global QoE Settings.
3. Select Active in Auto-detect QoE applications.
4. Change other settings to refine the number of applications you automatically monitor. See Global QoE Settings for more information on the settings.
5. Click Submit.

It may take some time for the settings to apply.

Monitor applications manually

You may choose to add monitored applications manually to QoE.

1. Click Settings > All Settings in the menu bar.
2. In the Settings grouping, click QoE Settings > Manage QoE Applications.
   - Applications are only listed if there are monitored nodes. You must first add a Network or Server Sensor before you can enable any applications.
   - Enabled applications are currently being monitored on at least one node.
   - Applications can be disabled, which means that no traffic for the application is currently collected on any node.
3. Click Add New.
4. Select Choose a pre-configured application.
   - Applications that are already enabled do not display in the list.
5. Use the Search or Group By options to find the application you want to monitor, select it, and then click Next.
6. On the Configure Application view, edit the Category, Risk Level, or Productivity Rating as necessary, and then click Next.
7. On the Specify Nodes view, choose the nodes you want to monitor for this type of traffic.
Only nodes that have already been specified as nodes to monitor on the Manage QoE Nodes page display in this list.

8. Click Next.
9. Review your choices on the Summary page, and then click Finish.

Your newly enabled application will display on the Manage QoE Applications page in alphabetical order.

Monitor nodes with a network sensor

Nodes are automatically detected and monitored when network traffic originates from or terminates at a node. However, you can manually specify the nodes after the network sensor has been successfully deployed. For information about adding applications, see Monitor applications for QoE.

You can monitor up to 50 nodes per network sensor.

Add nodes automatically

While Network Sensors automatically detect and monitor nodes by default, the settings may have changed or you may have upgraded from a version of QoE that does not automatically monitor nodes. QoE automatically monitors the first 50 nodes with traffic.

Automatic node discovery may not be 100% accurate due to devices with the same IP addresses in your network.

Only nodes that meet the criteria selected in Nodes with QoE Traffic are added automatically.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage Global QoE Settings.
3. Select Active in Auto-detect QoE nodes.
4. Change other settings to refine the number of nodes you automatically monitor. See Global QoE Settings for more information on the settings.
5. Click Submit.

It may take some time for the settings to apply.

Add nodes manually

If a node is already monitored and you want to monitor it with a different sensor, you must delete the node from the original sensor before you can add it to the new network sensor.

1. Navigate to the Manage QoE Packet Analysis Sensors page.
2. Expand the Network sensor that you want to add a node to.
3. Click the Add Node to Monitor button.

4. On the Create QoE Node page, choose the managed nodes you want to monitor with this network sensor.

5. On the Select QoE Applications page, choose the applications you want to monitor for these nodes. See Monitor applications for QoE for more information.

6. Review your selections on the Summary page.

7. Click Finish.

View the nodes and applications selected by expanding the Network Sensor you just configured.

Ignore traffic from applications or nodes
You can ignore traffic generated by applications or from a specific node.

Ignore application traffic
If you decide to no longer monitor an application, disable discovery or monitoring for that application in the Manage QoE Applications page.

<table>
<thead>
<tr>
<th>Discovery ON</th>
<th>Monitoring ON</th>
<th>Monitoring OFF</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Applications are automatically discovered and application traffic is monitored</td>
<td>Applications are automatically discovered, but application traffic is not monitored</td>
</tr>
<tr>
<td>Discovery OFF</td>
<td>Applications cannot be automatically discovered, and application traffic is monitored</td>
<td>Applications cannot be automatically discovered, and application traffic is not monitored</td>
</tr>
</tbody>
</table>

Ignore node traffic
You can permanently ignore all traffic from specific nodes that you monitor on a network sensor. This is often used to reassign a node to a different network sensor.

| You cannot add a node back to its original network sensor. |

1. Click Settings > All Settings in the menu bar.

2. In the Settings grouping, click QoE Settings > Manage QoE Packet Analysis Sensors.
3. Select a network sensor, and click Edit.
4. Select the node you want to remove, and click Delete.

The node is removed from the sensor and all traffic to and from the node is ignored.

Define custom HTTP applications

In addition to choosing from predefined applications, you can define custom HTTP applications, and add them to nodes you are monitoring.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Applications.
3. Click Add New.
4. On the Select Application page, select Create a new HTTP application, and click Next.
5. On the Configure Application page, enter the name and description of the application you're creating, and then choose the Category, Risk Level, and Productivity Rating appropriate for the application.
6. Set the URL Filter. This specifies the HTTP application traffic to monitor. When you choose which filter to use in the drop-down, notice that the example changes to indicate how the accompanying text field will be used.

   For example, selecting Hostname contains changes the help text to http://*...*/path/page.html. Any text you enter will be included in the filter where the "..." is.

7. Enter the hostname or URL for your filter, and then click Next.
8. On the Specify Nodes page, choose the nodes to monitor for this type of traffic. Only nodes that have already been specified as nodes to monitor (on the Manage QoE Nodes page) will display in this list.
9. Click Next. Review your choices on the Summary page, and click Finish.

Your new application will display on the Manage QoE Applications page in alphabetical order.

Advanced sensor configuration

Sensors cannot be edited until they are fully deployed. An entry displays in the notification area when your sensor is deployed, or you can check the Manage QoE Packet Analysis Sensors page. The status of completely deployed and working sensors is Up.
When you click Edit Sensor, you can configure:

- the **monitored interface**
- the **allocated CPU cores and memory**
- QoE **thresholds**

### Configure which interface to monitor for traffic

When you deploy a sensor, the first available interface is monitored for traffic. Once the sensor is installed, you can go back and change the monitored interface.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors.
3. Select the sensor to edit.
4. Click Edit Sensor.
5. Select the desired interface from the Interface to capture QoE data drop-down list.
6. Click Save.

### Set the number of CPU cores and the amount of memory QoE can use

When a sensor is deployed, QoE automatically allocates one CPU core and 256 MB of memory to the sensor. After the sensor is installed, you can change the allocated CPU cores and memory.

For sensors, the memory usage scales with the traffic load. The more flows that are going on the line, the more memory you need.

<table>
<thead>
<tr>
<th>Number of CPU Cores</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Not Recommended</td>
</tr>
<tr>
<td>2</td>
<td>Suitable for 100 Mbps links</td>
</tr>
<tr>
<td>3 - 4</td>
<td>Gigabit links with low utilization</td>
</tr>
<tr>
<td>5 - 6</td>
<td>Gigabit links with medium utilization</td>
</tr>
<tr>
<td>7+</td>
<td>Gigabit links with high utilization</td>
</tr>
</tbody>
</table>

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors.
3. Select the sensor to edit.
4. Click Edit Sensor.
5. In the Memory field, select the number of GB you want to allocate to the sensor.
If you allocate less than the recommended amount of memory, you may see reduced performance.

6. In the CPU Cores field, select the number of CPU cores you want to allocate to the sensor.

   i  If you allocate fewer than the recommended number of CPU cores, you may see reduced performance.

7. Click Save.

Configure QoE thresholds

You can modify the application response time (ART), network response time (NRT), volume, and transaction thresholds that are used to alert you to irregularities in your network.

   i  We recommend that the sensors collect a few days' worth of data before setting thresholds.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Applications.
3. Select the application to edit, and click Edit.
4. Click Next, and then click Next again.
5. On the Summary page, click the plus sign by Thresholds.
6. Select Override Orion General Thresholds next to each data type.
7. Change the threshold. You can use specific thresholds or you can use a dynamic threshold based on the baseline established. The default baseline is seven days, which is configurable in the Orion Polling Settings page.
8. Click Finish.

Packet Analysis Sensor agents

The software that provides a communication channel between your SolarWinds server and the monitored object to which you have deployed your Packet Analysis Sensor is called an "agent". Agents are used to send the data that QoE collects back to the Orion server. The agent runs as a service, and it has a small installed footprint (under 100MB installed).
Poll devices with SolarWinds Orion agents

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

- Polling hosts and applications behind firewall NAT or proxies.
- Polling nodes and applications across multiple discrete networks that have overlapping IP address space.
- Secure, encrypted polling over a single port.
- Support for low bandwidth, high latency connections.
- Polling nodes across domains where no domain trusts have been established.
- Full, end-to-end encryption between the monitored host and the main polling engine.

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

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

Modify global agent deployment and update settings

Before you deploy agents or upgrade your Orion server, review the global agent settings to make sure the settings are appropriate for your environment. Additional agent settings can be modified locally on the agent.

Navigate to the Agent Settings page

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings.
3. Click Define Global Agent Settings.

Allow automatic agent registration

Select this option to register agents with the Orion server automatically when you use an Orion account without Administrator Rights to install agents. Registered agents can communicate with the Orion server.

When this setting is not selected and you install agents with a non-Orion administrator account, you must register waiting agents manually. Click Settings > All Settings > Manage Agents > Add Agent > Connect to a previously installed agent.

Agents installed using an Orion administrator account always attempt to register the agents automatically.
Automatically create node

When you deploy an agent on a new node, the node is automatically added to your Orion server.

Allow automatic agent updates

(Recommended, enabled by default) Select this option to automatically upgrade the agent software when updates are available. This process pushes a new version of the agent to client computers over the agent communication channel. After the agent receives the new version, it updates itself. This process typically does not require rebooting.

- If you do not enable this option, you will need to manually upgrade agents during product upgrades.
- If you have deployed a large number of agents and you have had bandwidth issues in the past, you may want to disable this option when you upgrade your products and manually upgrade agents in batches.
- Outdated agents may not be able to communicate with the server. Ensure all agent versions match the version of the server.

XX Hours

Control the length of time the agents are considered new in the Manage Agents list.

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 agents to nodes**

Agents provide an additional method to poll devices that are part of a separate network or have intermittent connectivity to the network with your Orion server. SolarWinds Orion products support multiple methods of deploying agent software.

- Deployment to Raspberry Pi devices may take longer.
- Before you deploy agents, verify your global agent deployment settings.

Software deployment - Deploy the agent software from the Orion server to one or more client computers.

- **Deploy an agent with the Add Node wizard**
- **Deploy agents to monitored nodes**

Manual deployment - Manually move the installer to the remote computer and then install and configure it locally.

- **Deploy the agent manually to a Windows computer**
- **Deploy an agent manually to a Linux/Unix-based computer**
Mass deployment - Mass deploy the agent software to multiple computers using a mass deployment technology, such as Group Policies, SolarWinds Patch Manager, or other automation software.

- Mass deploy an agent on Windows using MST files and a Group Policy
- Deploy agents on Linux/Unix-based computers through a repository
- Deploy with a Gold Master Image
- Prerequisites for deploying agents on Windows Core Servers

Cloud deployment - Deploy the agent to a computer in the cloud.

- Manually deploy an agent on Amazon Web Services
- Automatically deploy a Windows agent to established instances on Amazon Web Services
- Automatically deploy Orion agent on Azure VMs

Windows Core requires specific setup before you can install the agent software.

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 & Unix/Linux Servers: Agent as the Polling Method.
6. Select the operating system type of the remote computer.
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.

For more details, see What privileges do I need and Credentials and privileges used on Linux/Unix-based computers.

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

Deploy agents to monitored nodes

- The Orion server must be able to communicate with the remote nodes. To monitor Linux/Unix-based nodes, TCP port 22 (outbound) must be open on the Orion server or additional polling engine and open (inbound) on the node you want to monitor.

1. Click Settings > All Settings in the menu bar.

2. Under Node & Group Management, click Manage Agents.

3. Click Add Agent.

4. Select Deploy the agent on my network.

5. On the Deploy Agent on Network page, choose where you want to install the agent.

- The IP address field does not accept ranges.
- Enter an IP address or host name of a node that has not be managed.

6. Click Next.
7. Select a node and click Assign Credentials.

- These credentials are only used to connect to the remote device 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/Unix-based computers, you can connect with one credential set and then use another credential to use `su` or `sudo` for package installation. Most Linux/Unix distributions require the user's password when using `sudo`. Other distributions, such as SUSE, may require the root password. Depending on your Linux/Unix distribution, enter the required credential for the Include Credentials with Elevated Privileges to install the package.
- You can assign credentials to multiple locations or nodes by selecting multiple entries.

8. Click Deploy Agent.

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

**Deploy the agent manually to a Windows computer**

Selecting this deployment method may be helpful to troubleshoot connectivity issues with the Orion server. This method is also helpful when the Orion server cannot communicate directly with the computer where the agent will be installed.

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings > Download Agent Software.
3. Click Windows, and click Next.
4. Click Install Manually, and click Next.
5. Click Download MSI.
6. Copy the MSI file to the client machine, and run it.
7. In the Installation wizard, select **Agent Initiated Communication** or **Orion Server Initiated Communication**.
8. Enter the Orion server IP address or hostname, and the SolarWinds Orion administrator account credentials.

9. **Optional:** For **Server-initiated communication (passive)**, in the Orion Web Console:
   a. Click Settings > All Settings.
   b. Under Node & Group Management, click Manage Agents > Add Agent.
   c. Click Connect to a previously installed agent > click Next.
   d. Enter the name, IP address, and port number for the agent and click Server-initiated communication.

When the installation is successful and communication between the agent and the Orion server is successful, the agent is listed on the Manage Agents page.
Deploy an agent manually to a Linux/Unix-based computer

Use this method to install agents if you cannot use push deployment to Linux/Unix-based devices over SSH. For example, when the device is behind a NAT or is hosted in the cloud. This approach uses `wget`, `curl`, or `perl` to download the installation files from your chosen polling engine. This agent installation method is known as a pull deployment.

Pull deployment requires that the Orion Web Console is accessible from the target Linux computer.

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings > Download Agent Software.
3. Click Unix/Linux, and Next.
4. Click Manually Install by Downloading Files via URL, and click Next.
5. Select your Distribution and Communication Mode.
6. Enter the Connection Settings.
   - For Agent-initiated communication (active), select or enter the polling engine you want to collect the agent's data. If you connect through a proxy, click Advanced.
   - For Server-initiated communication (passive), enter the listening port number used to communicate with the Orion server or additional polling engine. By default, this is port 17790.
7. Click Generate Command.
8. Copy and paste the command in the terminal open to the Linux/Unix computer. The command downloads the software from the selected polling engine.
9. Optional: For Server-initiated communication (passive), in the Orion Web Console click Settings > All Settings > Node & Group Management > Manage Agents > Add Agent > Connect to a previously installed agent > Next. Enter the name, IP address, and port number for the agent and click Server-initiated communication.

When the installation is successful and communication between the agent and the Orion server has been established, the agent appears in the agent list on the Manage Agents page.

10. On the Manage Agents page, select the new agent, and then click Choose Resources.
11. Select the items you want to monitor, and click Submit.

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

You can choose to copy the installer file to the Linux/Unix computer manually and then install it instead of using `wget`, `curl` or `perl`.

1. On the Download Agent Software page, select your distribution.
2. Click Download Agent Software File for Manual Installation.
3. Move the file to the Linux/Unix computer and extract it.
4. Follow the instructions in the `readme.txt` file.
Select your distribution

Agents are supported on the following Linux/Unix operating systems.

- Amazon AMI, 64-bit
- CentOS 6.x, 32-bit
- CentOS 6.x, 7.x, 64-bit
- IBM AIX 7.x
- Oracle Linux 6.x, 7.x, 8.x, 64-bit
- Raspbian Jessie 8.0
- Red Hat Enterprise Linux 5.11, 6.x, 86-bit
- Red Hat Enterprise Linux 5.11, 6.x, 7.x, 8.x, 64-bit
- SUSE Linux Enterprise Server 11.x - 15.x, 64-bit
- SUSE Linux Enterprise Server 11.x, 86-bit
- Ubuntu 14.x - 16.x, 86-bit
- Ubuntu 14.x - 18.x, 64-bit

If your operating system is not listed, select the closest match to your Linux/Unix distribution. SolarWinds cannot guarantee that the software will work as intended on a non-supported OS, but will attempt to install the software for the distribution you select.

Credentials and privileges used on Linux/Unix-based computers

Agents installed on Linux/Unix-based computers can use three different credential sets to install and configure the agent. During this process, a service account is created to run the agent service.

You need sufficient privileges to be able to do the following to install and configure the agent:

- open an SSH connection remotely
- SFTP or SCP
- install software
- create a user
- create a group

Credentials are used to install and configure the agent and are not used at any other time. You may remove the credentials from the credential store once the agent is deployed.

SSH credentials

Agent installations require a credential set that allows the user to open an SSH session from a remote computer. This can be provided as either a user name and password or as a certificate.

Verify the credentials by opening an SSH connection to the remote computer.

For Linux/Unix-based computers, you may need to include another set of credentials to use `su` or `sudo` for package installation. You can add these credentials selecting the Include Credentials with Elevated Privileges.
Certificate credentials

You can use any certificate-based credential that is supported by SSH. Upload a private key file or paste the private key in PEM format.

Credentials with elevated privileges

To install the package, you need credentials with administrator or root-level privileges. Depending on your network security policies, some Linux/Unix-based computers do not allow user accounts to connect remotely and install software. If this applies to the computer you want to monitor, you can select Include Credentials with Elevated Privileges and enter credentials that have the correct privileges. Most Linux/Unix distributions require the user’s password when using `sudo`. Other distributions, such as SUSE, may require the root password. Depending on your Linux/Unix distribution, enter the required credential for the Include Credentials with Elevated Privileges to install the package.

When this is selected, we connect to the Linux/Unix-based computer using the provided SSH credentials and then switch users to the account with elevated privileges to install and configure the agent.

SNMP credentials

Select Include SNMP Credentials to collect SNMP data to use in Hardware Health, Asset Inventory, and SNMP component monitor information. This is required if SNMP v3 is installed. The agent software detects if you have SNMP installed on the computer and attempts to use your established SNMP credentials. No data is collected if the agent does not have the correct SNMP credentials.

> **i** Hardware Health and Asset Inventory are not supported on AIX devices.

Service account privileges

When the agent software is installed, we create a service account (SWIAgent), and add it to its own group.

This account does not have remote access privileges and cannot be used to log in to the computer.

The service account is used to run the `swiagentd` service. When updating the agent, a second service runs `swiagentd.update` for the duration of the update.

The service account and group are removed when the agent is deleted from the node.

For SAM users, if you do not enter credentials or select inherit from node, the monitor executes the script under the agent credentials (SWIAgent). These credentials may not have the elevated permissions required for executing scripts.

Mass deploy an agent on Windows using MST files and a Group Policy

If you are already using a mass-deployment technology, this deployment method is an easy way to get agents on a large number of computers.

Polling engine selection is important. When you download the MST file, the file includes the polling engine IP address and other vital information. When you deploy the agent using the MSI file, along with the MST file on the managed node, the agent is installed and pointed to the polling engine selected.
What is an MST file?

A Microsoft Transform (MST) file is a collection of specified changes applied to a base Windows Installer package file at the time of deployment. It is an overlay on top of an existing MSI file that defines what specific components or features of an application get installed. The MST file modifies the Microsoft Installer package.

After the software you want to install is packaged in the Windows Installer package format, you can use MST files to customize the software for your organization, such as installing only specific features. The modular design of Windows Installer packages simplifies deployment. When you apply transforms to an MSI file, Windows Installer can dynamically add or modify data in the installation database to customize the installation of the application. Additional information on creating MST files can be found on technet.microsoft.com.

Generate and download the MST file

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings > Download Agent Software.
3. Click Windows, and click Next.
4. Click Mass Deploy to Multiple Machines, and click Next.
5. Select the agent communication mode.
   - For **agent-initiated communication**, enter the polling engine you want the agent to use. You may need to manually enter the polling engine information if the IP address is different from what the Orion server reports. This happens when the monitored host is behind a NAT or proxy device. In these cases, enter the IP address of the Orion server or the additional polling engine as it is accessible from the host where the agent will be installed.
     - To use an existing polling engine, select Use Connection Details from Polling Engine, and then select a polling engine from the list.
     - To manually enter the polling engine IP address, select Enter Connection Details Manually, and then enter the host name and IP address. The IP address is required. Use the host name and IP address of the polling engine that you can access from the client.
     - If a proxy is required, expand Advanced, and specify the proxy settings.

   - For **server-initiated communications**, enter your agent communication port number. The default port is 17790.

6. Click Download .MSI, and save the file.
7. Click Download .MST, and save the file.

**Add the MST and MSI files to a Group Policy**

1. Share a folder containing the MST and MSI files.
2. In Active Directory, locate the container where you want to advertise the application, and then access the container properties.
   - A container is a site, domain, or organizational unit (OU).
3. Create a Group Policy object.
4. In Advanced Options, add the Software installation policy. Select the network path for the agent MSI and MST files.
Connecting passive agents to the Orion server

1. In the Orion Web Console click Settings > All Settings > Node & Group Management > Manage Agents > Add Agent > Connect to a previously installed agent > Next.
2. Enter the name, IP address, and port number for the agent and click Server-initiated communication.

The agent is deployed at login and is registered by the Orion server (if auto-registration is enabled).

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

Deploy agents on Linux/Unix-based computers through a repository

Use built-in package management tools, such as `yum`, `apt-get`, or `zypper`, to install agent software on your Linux/Unix-based computers.

To deploy agents on AIX computers, only the `yum` packet management tool is supported.

The Orion server and Additional Web Servers are Linux/Unix repositories for the agent. This method allows you to use automation tools to mass deploy agents on your Linux/Unix-based computers.

When installing the software, you may be prompted that you are using a deprecated command.

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings > Download Agent Software.
3. Click Unix/Linux, and Next.
4. Click Install via Package Management Tool, and click Next.
5. Select your distribution.
6. Copy the repository command and paste it to a terminal open to the Linux/Unix-based computer.
7. You may be prompted for the root password to add the repository.
8. After the repository is registered with the computer, run the install command, according to your package management tool, for example:

   ```
   yum install swiagent
   apt-get install swiagent
   zypper install swiagent
   ```

   The agent software is downloaded from the repository and installed on the computer.
9. In the terminal, type `/opt/SolarWinds/Agent/bin/swiagentaid.sh init`.
10. Configure the agent communication mode and polling engine information.
11. Enter 7 to save your changes.
12. **Optional:** For **Server-initiated communication (passive)**, in the Orion Web Console click Settings > All Settings > Node & Group Management > Manage Agents > Add Agent > Connect to a previously installed agent > Next. Enter the name, IP address, and port number for the agent and click Server-
initiated communication.

When installation is successful and communication between the agent and the Orion server has been established, the agent appears in the agent list on the Manage Agents page.

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

The Orion repository

The SolarWinds Orion repository is available when you install any SolarWinds Orion platform product running on version 2016.2 or later. To install the agent software, you must add the location of the repository to every Linux/Unix-based computer. Repositories are generally added by the root account. This can be automated by an automation tool.

Deploy with a Gold Master Image

Use a Gold Master image when you want to maintain a master image of agent software that is copied when a new Windows server is provisioned. This saves time for virtual machines and physical servers. Whenever a new server is brought online using this image, the agent will already be installed.

⚠️ Disable the SolarWinds Orion agent service before you create your gold master, and then start it on the remote computer when the gold master is cloned.

Install an agent offline

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings > Download Agent Software.
3. Click Windows, and click Next.
4. Click Distribute via a Golden Master Image, and click Next.
5. Select the agent communication mode.
   - For **agent-initiated communication**, enter the polling engine you want the agent to use. You may need to manually enter the polling engine information if the IP address is different from what the Orion server reports. This happens when the monitored host is behind a NAT or proxy device. In these cases, enter the IP address of the Orion server or the additional polling engine as it is accessible from the host where the agent will be installed.
     - To use an existing polling engine, select Use Connection Details from Polling Engine, and then select a polling engine from the list.
     - To manually enter the polling engine IP address, select Enter Connection Details Manually, and then enter the host name and IP address. The IP address is required. Use
the host name and IP address of the polling engine that you can access from the client.

- If a proxy is required, expand Advanced, and specify the proxy settings.

![Download Agent Software](image)

- For server-initiated communications, enter your agent communication port number. The default port is 17790.

6. Click Download .ZIP, and save the file.

7. Extract the contents of the ZIP file and copy the extracted files to the master image computer.

8. On the image computer, run the Command prompt as administrator. Without the administrator mode, you may not be able to copy files or create the scheduled task when you run the batch file.

9. In the command prompt, go to the directory where you copied the files and run `setup.bat`.

   This process creates a SolarWinds directory in AllUsersProfile, copies three files into the directory, and creates a scheduled task to install the client when the computer reboots.

10. Reboot the computer. During the reboot, the agent is installed and the scheduled task is removed.

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

Enable server-initiated communication on deployed agents

If you are deploying a server-initiated agent, you need to enable agent communication with your Orion server.

1. Click Settings > All Settings in the menu bar.

2. Under Node & Group Management, click Manage Agents.

3. Click Add Agent > Connect to a previously installed agent > Next.

4. Enter a name for the agent, and click Server-initiated communication.

5. Enter the IP address of the node where the agent is deployed.

   If you have set up a shared secret, provide the password.
6. Click Advanced and verify that you have specified the correct port for the agent. The default port is 17790.

7. Click Submit.

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

Deploy an agent with Patch Manager

You can only perform this deployment method if you have successfully configured Patch Manager to push software in your environment. This method contains four parts you must perform in order: download the installation files, build the package, add deployment rules, and publish the package.

Download the installation files

First, you need to download the Orion agent software installation files including an MSI and MST file.

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings > Download Agent Software.
3. Click Windows, and click Next.
4. Click Mass Deploy to Multiple Machines, and click Next.
5. Select the communication method and enter the required information. For more information, see Mass deploy an agent on Windows using MST files and a Group Policy.
6. Download and save the MSI and MST files to a location on your Patch Manager server.

Optional: Rename the SolarWinds agent files to SolarWinds Agent <version> for easier tracking.

Build the package

Next, create a package of the Orion agent installation files.

1. Launch SolarWinds Patch Manager.
2. In the navigation pane, expand Administration and Reporting > Software Publishing, and then click SolarWinds, Inc. Packages.
3. From the Actions pane, click New Package. This launches the Patch Manager Package Wizard.

![SolarWinds, Inc. Packages](image)

4. In the package information screen, enter the following minimum general information for the package:
   - Package Title: SolarWinds Orion Agent (version number) MSI
   - Description: SolarWinds Orion Agent
   - Classification: Tools
   - Vendor: SolarWinds, Inc.
   - Product: Orion Agent (This must be entered the first time)
   - Severity: None
   - Impact: Normal (Used to determine the push schedule)
   - Reboot Behavior: Can request reboot (Determines if the products requires a reboot)

   ![Tip](image)
   All other fields can be left empty.

5. Click Next. Continue adding deployment rules through the Patch Manager Package Wizard.

Add deployment rules

1. On the Prerequisite Rules window, click Add Rule.
2. Select Create Basic Rule.
3. Select Windows Version as the Rule Type, and enter the following information:

![Rule Editor]

- **Comparison:** Greater Than or Equal To
- **Major Version:** 6
- **Minor Version:** 1
- **SP Major Version:** 0
- **SP Minor Version:** 0
- **Build Number:**
- **Product Type:** Server

4. Click OK to save this rule, and click Next.

5. On the Select Package window, select the Package Type as a Microsoft Installer File (.msi), and select I already have the content for the package locally on my network.

6. Click the browse icon and locate the MSI file for the SolarWinds Orion agent. The Download URL field will automatically populate.

7. The GUID product code is extracted from the MSI file and displayed for review. Copy the GUID product code that you will use later.

   ![Guid Note]

   **Note:** The GUID is detected from the installer. Use the one displayed in your environment.

8. Select Includes additional files with the package, and click the button to the right to open the Package Content Editor.

9. In the Package Content Editor, click Add Files, and browse to the MST File for the SolarWinds Orion agent.

10. Click OK to close the Package Content Editor. To confirm that you want to add these files to the cache, click Yes.

11. Select None for the Binary Language.
12. In the Command Line field, enter: TRANSFORMS=(MST FILE NAME)
   
   Example: TRANSFORMS=SolarWinds_Agent_1.5.0.951.mst

13. Click Next.


15. Select Rule Type: Product Installed, and select Not Rule.

16. Enter the product code without the brackets, and leave all other fields empty.

17. On the Installed Rules window, click OK to save the rule, and then click Next.

18. Click Add Rule > Basic Rule.

19. For the Rule Type, select File Version with Registry Value. Enter the following values:
   
   a. Registry Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SolarWinds\Agent
   
   b. Registry Value: InstallDir
   
   c. Comparison: Equal To.
   
   d. Version: Version number of the agent

20. Click OK to save the rule, and click Next. Review the Summary Page, and enter notes at the bottom.

21. Click Next to save, and click OK.

When the file packaging and uploading completes, a Package Saved dialog displays.

Publish the package

1. In the SolarWinds, Inc. Packages view in Patch Manager, select the SolarWinds Orion Agent package that you created.
2. In the SolarWinds Orion Agent action pane, click Publish Packages.

![SolarWinds Orion Agent 1.0.0.866 MSI](image)

3. Accept the default selections, or choose a specific Windows Server Update Services (WSUS) server for publication, and then click Next.
4. You are notified when the package publishes.
5. Click Finish to close the Publishing Wizard.

Finally, approve the package:

1. In the Patch Manager Console, move up to Patch Manager / Enterprise / Update Services / (Your WSUS Server Name) / All Updates.
2. Click on the newly created and published package.
3. Right-click on it and select Approve. From here, you can determine which groups can get the new package and setup a schedule. Handle the package as you would any other patch package.

The package for the SolarWinds Orion agent is packaged and published to your WSUS server.

**Prerequisites for deploying agents on Windows Core Servers**

If you are installing the agent on a Windows Core Server, you must install .NET Framework 4.5 or later, the latest Windows service pack, and critical updates.

**Prerequisites to installing an agent on Windows Core**

- Start WoW64.
- Start the .NET 2.0 layer.
- Start the .NET 2.0 layer for WoW64.
- Download and install the .NET framework from [www.microsoft.com](http://www.microsoft.com).

> By default, no web browser is installed with Windows Core. Consider transferring the necessary files with FTP or a flash drive.

After the .NET Framework is installed, you may need to reboot the host server. The [agent can then be deployed](http://example.com) to the host server and operate normally.
Deploy Windows agents in the cloud

Agents can be deployed in the cloud for use with Amazon Web Services, Microsoft Azure, and other third-party cloud infrastructure services.

Manually deploy an agent on Amazon Web Services

You can manually deploy agents to a virtual machine using Remote Desktop Connection in two ways.

Requirements for manual agent deployment

- **Agent-initiated communication:** The poller must have a public IP address which is visible from the node with the agent installed. **Port 17778** must be open on the poller.
- **Server-initiated communication:** The node with the agent installed must have a public IP address. **Port 17790** must be open. You must also connect the agent to the Orion server by clicking **Settings > All Settings > Node & Group Management > Manage Agents > Add Agent > Connect to a previously installed agent > Next.** Enter the name, IP address, and port number for the agent and click Server-initiated communication.

Install through the command prompt

1. Click **Settings > All Settings** in the menu bar.
2. Under **Product Specific Settings**, click **Agent Settings > Download Agent Software.**
3. Click **Windows**, and click **Next.**
4. Click **Mass Deploy to Multiple Machines**, and click **Next.**
5. Download the MSI and MST files.
6. Run a command prompt as administrator from the context menu.
7. Enter the following command:

   `msiexec /i "SolarWinds-Agent.msi" TRANSFORMS="SolarWinds-Agent.mst"`

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

Deploy the agent manually using the interactive wizard

1. Click **Settings > All Settings** in the menu bar.
2. Under **Product Specific Settings**, click **Agent Settings > Download Agent Software.**
3. Click **Windows**, and click **Next.**
4. Click **Install Manually**, and click **Next.**
5. Click **Download MSI.**
6. Copy the MSI file to the client machine, and run it.
7. In the Installation wizard, select **Agent Initiated Communication** or **Orion Server Initiated Communication.**
8. Enter the Orion server IP address or hostname, and the SolarWinds Orion administrator account credentials.

9. **Optional:** For **Server-initiated communication (passive)**, in the Orion Web Console:
   a. Click Settings > All Settings.
   b. Under Node & Group Management, click Manage Agents > Add Agent.
   c. Click Connect to a previously installed agent > click Next.
   d. Enter the name, IP address, and port number for the agent and click Server-initiated communication.

When the installation is successful and communication between the agent and the Orion server is successful, the agent is listed on the [Manage Agents](#) page.

**Automatically deploy a Windows agent to established instances on Amazon Web Services**

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings > Download Agent Software.
3. Click Windows, and click Next.
4. Click Mass Deploy to Multiple Machines, and click Next.
5. Download the MSI and MST files.
6. Log in to your Amazon Web Services S3 account.
7. Create a bucket and upload the MSI and MST files.
8. Create a PowerShell script to run on each virtual machine when it is launched for the first time, downloading and executing the MST and MSI files on each virtual machine where you want to install the agent.
9. Log in to your Amazon Web Services account.

You can perform the following steps through the API or AWS command line interface.

10. Create an instance, and paste your PowerShell script under Advanced Details in the User Data text box. Select the As Text option.

11. For instances that are already created, take the following steps:
   a. Stop the instance where you want to deploy the agent
   b. Right-click the instance and click Instance Settings > View/Change User Data.
   c. Paste your PowerShell script in the text box as Plain Text.

12. **Optional:** For **Server-initiated communication (passive)**, in the Orion Web Console click Settings > All Settings > Node & Group Management > Manage Agents > Add Agent > Connect to a previously installed agent > Next. Enter the name, IP address, and port number for the agent and click Server-initiated communication.
When the installation is successful and communication between the agent and the Orion server is successful, the agent is listed on the Manage Agents page.

Automatically deploy Orion agent on Azure VMs

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings > Download Agent Software.
3. Click Windows, and click Next.
4. Click Mass Deploy to Multiple Machines, and click Next.
5. Download the MSI and MST files.
6. Upload the MSI and MST files to Azure Blob Storage.
7. Create a PowerShell script for each VM where you will install an agent. This script will run on each VM when launched, to download and deploy the agent.
8. In the Microsoft Azure portal, use the Create a Virtual Machine wizard to add the PowerShell script to each VM on the Virtual machine configuration page.

This step can also be accomplished via the Azure Management REST API command line interface.
View agent connections and status, update agents, or manage agents

Review agent connection and deployment status.

1. Click Settings > All Settings in the menu bar.
2. Under Node & Group Management, click Manage Agents.

The icon displayed next to each Agent/Node indicates the status of the node or an agent icon. The agent icon indicates one of the following:

- An Orion agent has been deployed to a server not managed as a node
- An Orion agent has been deployed to a managed node but the currently used polling method is not the agent

Choose a list of resources and statistics to monitor

This is only available for agents that are deployed on nodes.

- For a Single Agent: Select the nodes, click Choose Resources, and choose items on the node you want to monitor.
- For Multiple Agents: Select the nodes, click Choose Resources. The server uses Network Sonar Discovery to discover available resources on the agents you have selected. You can choose items on the nodes to monitor.

Manage the agent as a new node

Select the agent and click Manage as Node. The Add Node page opens and is pre-configured with the agent's details.

View installed agents details

Click More Actions > Viewed installed agent plug-ins to view the agent status, connection status, plug-in status, and plug-in version.

Click More Actions > View installed plug-ins report to view a report of the same information for all agents.

Reboot the node the agent is installed on

Click More Actions > Reboot Agent Machine.

This button is disabled by default. It is enabled when the installation of an agent requires a system reboot.
Update the agent manually

If you have disabled automatic updates of agents, you can see Update Required in the Agent Status column of the Manage Agents view when an update is available.

Update the agent to ensure compatibility with the version of Orion Platform your agent needs to communicate with.

Although agents may continue to work in a limited capacity when an upgrade is pending, SolarWinds recommends that you update the agent at the earliest opportunity.

To update an agent:

1. Select the agent.
2. Click More Actions > Update.

The agent is updated.

The Update button is disabled by default. It is enabled when:

- Automatic updates for the agent are disabled.
- The selected agent requires an update.

Re-establish a connection to an agent using server-initiated communication

The server tries to re-establish the connection to the passive agent when the connection is lost and automatic reconnection fails. This can also be used for connecting to an agent that was deleted but not uninstalled.

Click More Actions > Reconnect to passive agent.

Manage Agents table columns

The table on the Manage Agents page displays information on the status and connection of your agents.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent/Node</td>
<td>Name or IP address of the listed node.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Agent Status</td>
<td>Current status of the listed agent.</td>
</tr>
<tr>
<td></td>
<td>- Connected/OK: Everything is working.</td>
</tr>
<tr>
<td></td>
<td>- Unknown: The agent is connected but no communication is received. If the agent is in the Unknown status for a long time, try renewing the communication. Select the agent and click More &gt; Restart Agent Service.</td>
</tr>
<tr>
<td></td>
<td>- Update Available: The agent version is older than the version on the server and should be updated.</td>
</tr>
<tr>
<td></td>
<td>- Update in Progress: The agent is currently being updated.</td>
</tr>
<tr>
<td></td>
<td>- Reboot Required: The agent needs to be rebooted in order to finish the installation of plug-ins.</td>
</tr>
<tr>
<td></td>
<td>- Reboot in Progress: The agent is currently being rebooted. Once reboot is complete, the agent should finish installation of plugins.</td>
</tr>
<tr>
<td></td>
<td>- Reboot Failed: The agent cannot be rebooted. It may be temporarily offline or there may be some other issue.</td>
</tr>
<tr>
<td></td>
<td>- Restarting: The agent is restarting.</td>
</tr>
<tr>
<td></td>
<td>- Plugin Update Pending: A plugin on the agent has an older version than the one that is on the server and should be updated.</td>
</tr>
<tr>
<td>Connection Status</td>
<td>Current connection status of the listed agent.</td>
</tr>
<tr>
<td></td>
<td>- Connected/OK: The agent is connected.</td>
</tr>
<tr>
<td></td>
<td>- Unknown: The agent management service is not running.</td>
</tr>
<tr>
<td></td>
<td>- Service not Responding: The agent management service is running, but the agent is not connected.</td>
</tr>
<tr>
<td></td>
<td>- Deployment Pending: An agent deployment is going to start, but has not started.</td>
</tr>
<tr>
<td></td>
<td>- Deployment in Progress: The agent is being deployed to the target node.</td>
</tr>
<tr>
<td></td>
<td>- Deployment Failed: Agent deployment failed.</td>
</tr>
<tr>
<td></td>
<td>- Invalid Response: The status displayed if the agent responds in an unexpected manner.</td>
</tr>
<tr>
<td></td>
<td>- Waiting for Connection: The agent was approved, but has yet to connect to the Orion server.</td>
</tr>
<tr>
<td>Registered On</td>
<td>Date when the agent was added to the agent management system.</td>
</tr>
<tr>
<td>Mode</td>
<td>Agent communication type:</td>
</tr>
<tr>
<td></td>
<td>- Agent-initiated: The agent initiates the connection to the agent management system.</td>
</tr>
<tr>
<td></td>
<td>- Server-initiated: The agent listens on its designated port for connections from the Orion server.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the agent software. This is helpful in determining which agents should be updated.</td>
</tr>
</tbody>
</table>
When viewing Linux/Unix-based nodes monitored by Orion agents for Linux/Unix, the table includes additional columns. These columns include the following:

<table>
<thead>
<tr>
<th>Column Header</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent - Package Distro Name</td>
<td>Displays the distribution name of the installer package. This is the name of the common installer for Linux/Unix distributions. For example, suse displays as the common installer for all 64-bit SUSE distributions.</td>
</tr>
<tr>
<td>Agent - OS Distro Name</td>
<td>Displays the general distribution name of the Operating System. For example, opensuse displays for an installed SUSE distribution.</td>
</tr>
<tr>
<td>Agent - Operating System</td>
<td>Displays the installed Operating System name and version. This value will differ from the package installer version. For example, opensuse 42.1 x64 is the installed OS version for this SUSE distribution.</td>
</tr>
<tr>
<td>Agent - Package Operating System</td>
<td>Displays the installation package name and version for the distribution. The installer package version may differ from the installed Operating System version. For example, suse 10.0 x64 is the package version for this SUSE distribution.</td>
</tr>
</tbody>
</table>

Edit agent settings

Editing the configuration of an agent may be necessary if you experience problems and want to collect diagnostics.

1. Click Settings > All Settings in the menu bar.
2. Under Node & Group Management, click Manage Agents.
3. Select an agent, and click Edit Settings.

Agent settings and troubleshooting options

- Agent Name: change the display name displayed in Orion.
- Communication type: displays whether the agent uses server-initiated or agent-initiated communication.
- Allow automatic agent updates: choose whether the Orion server can update the agent software to the latest version available.
- Troubleshooting:
  - Log level: the amount of detail saved to the log.
  - Diagnostics: click Collect new diagnostics, and then Download to save to your local disk. Send the zip file to our support team if requested.
Track your polling method

If nodes are using different polling methods, you may want to keep track of the polling method of each node to troubleshoot issues more easily. There are several methods you can use to identify the polling method of nodes:

- Node Details page: view individually
- Application Details page: view individually
- Manage Nodes page: view as a list
- Create a report to identify agent usage

Identify the polling method from the Node Details page

1. From the Orion Web Console, click My Dashboards > Home > Summary.
2. In the All Nodes resource, expand a node tree and click a node to go to the Node Details page.
3. In the Polling Details resource, locate the Polling Method.

Identify the polling method from the Application Details page

1. From the Orion Web Console, click My Dashboards > Applications > Summary.
2. In the All Applications resource, expand an application tree and click an application to go to the Application Details page.
3. In the Application Details resource, click Management > Edit Application Monitor.
4. Expand the Advanced heading to locate the Preferred Polling Method.

> All applications default to agent-based polling, even when no agent is installed. Use this option to override the default behavior.

Identify the polling method from the Manage Nodes page

1. Click Settings > All Settings in the menu bar.
2. Under Node & Group Management, click Manage Nodes.
   - If you use the new Manage Entities page...
     a. Click More > Edit Row Properties.
     b. In the Available Properties panel, select System Properties > Polling Method.
     c. Click Save Changes at the top of the screen.
   - If you use the legacy Manage Nodes page...
     a. Add the Polling Method field by clicking >> in the upper-right of the table.
Create a report to identify agent usage

1. From the web console, navigate to Reports > All Reports.
2. Enter agent in the Search box.
3. Click Agent Inventory to view the report.

View the status of agent plug-ins

Agent plug-ins are components that help agents to handle various tasks, such as polling.

When you enable and disable features in the Orion Web Console, the Orion Platform deploys and removes plug-ins automatically.

When you have issues with an agent, check the status of the agent and its plug-ins.

1. Click Settings > All Settings in the menu bar.
2. Under Node & Group Management, click Manage Agents.

If you think a plug-in should be available and cannot find it in the list, you may need to review your purchased products or manually update your agent. New plug-ins and updates to existing plug-ins are installed when an agent is updated. It may take a few minutes before the status changes.

- **Up to 20 plug-ins are deployed simultaneously at a time.**

Plug-ins are deployed and removed as needed when you enable and disable features. It is normal for agents to have different plug-ins.

<table>
<thead>
<tr>
<th>Status</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>The plug-in is installed</td>
<td>The plug-in is installed, working correctly, and communicating with no problems.</td>
</tr>
<tr>
<td>Installation Pending</td>
<td>The plug-in is waiting to be deployed. It may be waiting for the computer it is installed on to reboot, or because some other process on the remote host has interrupted the installation process.</td>
</tr>
<tr>
<td>Unknown</td>
<td>The status is unknown due to networking interruptions, communication problems with the agent, or because the plug-in is no longer installed.</td>
</tr>
<tr>
<td>Error</td>
<td>The plug-in may have installed incorrectly or failed to load.</td>
</tr>
<tr>
<td>In Progress</td>
<td>The plug-in is either being installed or uninstalled.</td>
</tr>
</tbody>
</table>

Edit agent connection settings or reprovision the agent once deployed

You can modify settings such as the communication mode or to which polling engine the agent sends information by modifying the agent on the computer.
If the agent loses connectivity to the Orion server, is unable to connect after being manually installed, or if the Orion server has migrated, you can configure the agent's settings directly on the computer you are monitoring. This enables the agent to reconnect to the Orion server.

Windows devices

1. Log on with an administrator account to the computer with the agent installed on it.
2. Open Orion Agent Settings in the Control Panel.
   
   ❧ If you get an error when opening Agent Settings in the Control Panel, navigate to the C:\ProgramData\SolarWinds\Agent directory, and Permanently Grant Access to that directory for your user when prompted.
3. Select the Agent Communication Mode.
4. Edit the Connection Settings.
   
   ❧ The Agent Shared Secret is provided for security. When you install the agent, you must set a shared secret. When the Orion server connects to the agent, it verifies the secret to connect.
5. Click OK to save your changes.

When communication between the agent and the Orion server is successful, the agent is listed on the Manage Agents page with the updated communication mode.

Linux/Unix-based devices

1. Log on to the computer with the agent installed on it.
2. Open a terminal window.
3. Run the following command as root:
   
   `/opt/SolarWinds/Agent/bin/swiagentaid.sh swiagentd init`
4. Configure the agent communication mode and polling engine information.
5. Enter 7 to save your changes.

When communication between the agent and the Orion server is successful, the agent is listed on the Manage Agents page with the updated communication mode.

Connect to or register a previously installed agent to modify connection or update settings

You may need to connect and register an agent manually when agents are configured with server-initiated communication, when you migrate servers, or when Allow Automatic Agent Registration is not enabled. The steps are different depending on the agent communication mode. You should confirm the agent communication mode before connecting.
Connect to an agent using agent-initiated communication

1. Click Settings > All Settings in the menu bar.
2. Under Node & Group Management, click Manage Agents.
3. Click Add Agent.
4. Click Connect to a previously installed agent, and click Next.
5. Enter the name of the agent you want to connect to, and select Agent-initiated communication.
6. Select the agent from the Agent list.
7. Optional: Expand Advanced to change the proxy.

Disabling this option requires you to upgrade agents manually after upgrading your SolarWinds products and modules.

9. Click Submit.

When the connection is successful, the agent displays in the agent list on the Manage Agents page.

Connect to an agent using server-initiated communication

If the communication mode is server-initiated (passive), a shared secret was required during installation. This secret must be entered again here.

If you are migrating to a new Orion server, you must redeploy any agents using server-initiated communication.

1. Click Settings > All Settings in the menu bar.
2. Under Node & Group Management, click Manage Agents.
3. Click Add Agent.
4. Click Connect to a previously installed agent, and click Next.
5. Enter the name of the agent you want to connect to, and select Server-initiated communication.
6. Enter the IP address or hostname where the agent is installed.
7. Optional: Expand Advanced to change the port number, assign the agent to a different poller, or use a proxy to connect to the agent.

Disabling this option requires you to upgrade agents manually after upgrading your SolarWinds products and modules.

9. Click Submit.

When the connection is successful, the agent displays in the agent list on the Manage Agents page.
Migrate agents from one Orion instance to another

When you migrate your SolarWinds Orion server to a different computer, you may need to modify any agents that use agent-initiated communication so they communicate with the new server. Agents using server-initiated communication are migrated automatically.

If any of the following has changed, you must modify your agents:

- IP address
- DNS
- Database

Modify agents to point to the new server in one of the following ways:

- **Redeploy the agents** from the Orion server (Windows and Linux/Unix).
- **Manually change the Orion server IP address using the Control Panel** (Windows and Linux/Unix).
- Manually change the Orion server IP address by **reprovisioning** (Linux/Unix).
- Use the [Group Policy Administrative template](#) to redirect existing agents to the new Orion server. This requires endpoints be joined to an active directory domain (Windows).

If you have not cloned your certificates, you must migrate them to the new server.

Use a group policy to migrate agents on Windows

You can use a group policy to change the connection settings of the agents to the new instance of your Orion server. Use this method if you have one or a few agents deployed.

> It can take up to 15 minutes for an agent to successfully connect to the new Orion server.

1. After you migrate your server, create a domain-based Group Policy Object (GPO). You can use this Administrative Template (.admx) file on THWACK.

2. Copy the Administrative Template to the appropriate directory in the Central Store, and create the GPO within the Group Policy Management Console. For more information, search for "Editing Domain-Based GPOs Using ADMX Files" at [http://technet.microsoft.com](http://technet.microsoft.com).

3. Ensure the group policy will apply to the computer objects where the agent is installed. This can be done by linking to the appropriate Organizational Unit (OU) or filtering to specific computer objects or groups.

4. Ensure the policy is updated on the target computers.
    a. Open a command prompt in the Administrator context. (Right-click cmd.exe and select, Run as Administrator.)
    b. Enter `gpupdate /force` and then press Enter.

The following registry key is created when the GPO is applied:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SolarWinds\Agent
```

You can create your own Group Policy Object by editing the following registry key and providing the correct values: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SolarWinds\Agent`. 

page 232
<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Registry Type</th>
<th>Value</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TargetHost</td>
<td>REG_SZ</td>
<td>Enter the name of the Orion server to which the agent reports</td>
<td></td>
</tr>
<tr>
<td>TargetIp</td>
<td>REG_SZ</td>
<td>Enter the IP address of the Orion server to which the agent reports</td>
<td></td>
</tr>
<tr>
<td>TargetPort</td>
<td>REG_DWORD</td>
<td>The port used for agent communication</td>
<td>17778</td>
</tr>
</tbody>
</table>

Redeploy agents from the Orion Web Console to a monitored node

When you migrate your Orion server to new hardware or change the access rules, such as changing the IP address, firewall rules, routing rules, or DNS name, you must also modify your agents to communicate with the new location.

1. Click Settings > All Settings in the menu bar.
2. Under Node & Group Management, click Manage Agents.
3. Click Add Agent.
4. Select Deploy the agent on my network.
5. On the Deploy Agent on Network page, choose where you want to install the agent.

- The IP address field does not accept ranges.
- Enter an IP address or host name of a node that has not be managed.

6. Click Next.
7. Select a node and click Assign Credentials.

- These credentials are only used to connect to the remote device 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/Unix-based computers, you can connect with one credential set and then use another credential to use `su` or `sudo` for package installation. Most Linux/Unix distributions require the user’s password when using `sudo`. Other distributions, such as SUSE, may require the root password. Depending on your Linux/Unix distribution, enter the required credential for the Include Credentials with Elevated Privileges to install the package.
- You can assign credentials to multiple locations or nodes by selecting multiple entries.

8. Click Deploy Agent.

When redeployment is successful and communication between the agent and the Orion server is successful, the agent Connection Status is Connected/OK on the Manage Agents page.
Change the agent communication mode on the remote node

You can change how the agent communicates with the Orion server. You can select server-initiated or agent-initiated communication.

1. Log in to the node where the agent is installed.
2. Edit the connection settings.
   - For Windows, open Orion Agent Settings in the Control Panel.
   - For Linux, su to an account with elevated privileges and type `service swiagentd init` in the terminal.
   - For AIX, su to an account with elevated privileges and type `/opt/SolarWinds/Agent/bin/swiagentaid.sh swiagentd init` in the terminal.
3. Select an agent communication mode.
   - **Agent-initiated communication**: The agent initiates communication with the Orion server on port 17778. This port must be open on the Orion server firewall so the agent can connect. No changes to the firewall rules are required on the agent-monitored device.
   - **Server-initiated communication**: The agent waits for requests from the server on a specified port. This port must be open on the firewall of the agent computer so the Orion server can connect. No changes to the firewall rules are required on the Orion server.
4. Save your changes.

If you switch from agent-initiated to server-initiated communication, you must register the agent with the Orion server manually.

When communication between the agent and the Orion server is successful, the agent is listed on the Manage Agents page with the updated communication mode.

Change the agent port to match the open port on the Orion server

This only applies to agents in agent-initiated communication mode.

Agents connect to port 17778 on the Orion server or Additional Polling Engine by default. You must change the messaging port on the Orion server or Additional Polling Engine AND on each agent in agent-initiated communication mode.

Manually change the port on the Orion server or Additional Polling Engine

1. On the Orion server or Additional Polling Engine, edit the following configuration file using a text editor:
   
   ```
   C:\Program Files (x86)\SolarWinds\Orion\AgentManagement\SolarWinds.AgentManagement.ServiceCore.dll.config
   ```
2. Change the port number on the following line:
   
   ```xml
   <agentManagementServiceConfiguration messagingPort="17778"/>
   ```
3. Save the file.
4. Restart the SolarWinds Orion Module Engine service.
5. Ensure your firewall rules are updated to allow communication through the new port.

- If you installed the agent manually, you can change the port number during installation through the wizard in the web console.
- If you deployed the agent from the server, the port number is set automatically.
- If you used the MST file for mass deployment, you must download a new MST file from the server after you change the port number.

Update the port on agents deployed on Windows

1. Log in to the computer with the deployed agent.
2. Open Orion Agent Settings in the Control Panel.
3. Enter a new port number, and click OK.

The agents direct communications with the server to the new port number.

Update the port on agents deployed on Linux/Unix-based devices

1. Log on to the device with the agent installed on it. You may need to su to an account with root-level privileges.
2. In the terminal, type `/opt/SolarWinds/Agent/bin/swiagentaid.sh swiagentd init`.
3. Choose option 3 and enter the new port number.
4. Enter 7 to save your changes.

The agents direct communications with the server to the new port number.

Agent polling method

When the Agent Polling Method is selected, an agent is deployed to the node and installed using the credential you selected. After the agent is installed, it operates under a local account.

Check nodes polled by agents for changes

While normal discovery finds new nodes and adds them to the Orion server, this is not true for nodes using the Agent. Agent discovery is an extension to the standard discovery process.

A discovery profile may contain:

- Nodes using both the Agent and non-Agent nodes
- Non-Agent nodes
- Agent nodes

On the Agents tab in the Network Discovery wizard, you can specify whether you want the wizard to check Agent-polled nodes for updates.

Checking the nodes might be time-consuming, so the option is disabled by default.
Updating Agent-polled nodes ignores the IP ranges, subnets, IP addresses or Active Directory settings provided in the Network Selection step.

However, if you have deployed multiple polling engines, note the polling engine selected in the Network Selection step. Only the Agent-polled nodes assigned to the selected polling engine will be checked for updates.

To enable checking the Agent-polled nodes during scheduled discoveries, select the Check existing nodes... box and specify the Agent-polled nodes to be checked for updates:

- To check all Agent-polled nodes, select Check all.
- To check only specific nodes:
  a. Select Check only specific set of nodes.
  b. Use properties and operators in the drop-downs, and provide a value as necessary.
  c. Click Preview to display nodes covered by your current condition.
  d. When you're satisfied, click Next to continue the Discovery wizard.

Poll SNMP information with an agent

Only agents deployed on Linux/Unix-based computers can poll for SNMP information. You must install an SNMP package to poll for information. Agents support gathering information from SNMP v2 and v3.

SNMP polling provides the following types of information:

- Location or contact information
- Information used for Hardware Health
- Information used for Asset Inventory

Poll SNMP on AIX computers

AIX does not support polling SNMP v3 in encrypted mode.
To poll SNMP details correctly, you need to manually enable the SNMP daemon:

1. Log in to the AIX computer where you deploy the agent software.
2. Go to the configuration file and specify the SNMP configuration. You can use the following examples recorded in the /etc/snmpdv3.conf file as a reference:

```
# Two snmpv1 community strings: public commstr1
VACM_GROUP group1 SNMPv1 public -
VACM_GROUP group1 SNMPv1 commstr1 -
VACM_VIEW group1view internet - included -
VACM_ACCESS group1 - - noAuthNoPriv SNMPv1 group1view - -
COMMUNITY public public noAuthNoPriv 0.0.0.0 0.0.0.0 -
COMMUNITY commstr1 commstr1 noAuthNoPriv 0.0.0.0 0.0.0.0 -

# snmpv2c community string: swiagent
VACM_GROUP group2 SNMPv2c swiagent -
VACM_VIEW group2view internet - included -
VACM_ACCESS group2 - - noAuthNoPriv SNMPv2c group2view - -
COMMUNITY swiagent swiagent 0.0.0.0 0.0.0.0 -
COMMUNITY public public 0.0.0.0 0.0.0.0 -

# snmpv3 user with no authorization: user1
USM_USER user1 - none - - - -
VACM_GROUP group4 USM user1 -
VACM_VIEW group4view internet - included -
VACM_ACCESS group4 - - noAuthNoPriv USM group4view - -

DEFAULT_SECURITY no-access - -

logging file=/usr/tmp/snmpdv3.log enabled
logging size=100000 level=3
```
3. Test the configuration:
   - To test SNMPv1, use the `snmpdinfo` or `clsnmp`.
   - To test SNMPv3 and v3 requests, use `clsnmp` and make sure you have `clsnmp configured`. The following configuration file `/etc/clsnmp.conf` matches the `/etc/snmpv3.conf` example:

   ```
   v2cstring localhost snmpv2c
   v3user_noauth localhost snmpv3 user1 
   ```

   Agents deployed on your AIX computers can now successfully poll SNMP information.

**Specify the polling engine**

The poller selection is important when you click the Download MST button, the MST file created includes the poller IP address and other information. When you deploy the agent on the managed node, the agent will be installed and configured to communicate with the correct poller.

- If you selected Use Connection Details from Polling Engine, select a polling engine from the drop-down list.
- If you selected Enter Connection Details Manually, enter the host name and IP address.
View logs and events with the Orion Log Viewer

The Orion Log Viewer (OLV) provides a singular view into event messages received from nodes monitored by your Orion Platform products. You can access your syslog and trap messages, monitor VMware events, filter and search event logs, integrate Orion alerts, and more. To access the Orion Log Viewer in the Orion Web Console, navigate to Alerts & Activity > Syslogs (or Traps).*

- Upon installation, the Orion Log Viewer replaces the legacy Syslog and Trap Viewers, existing syslog and traps messages are only available in read-only format, and existing rules are not migrated.
- The Orion Log Viewer requires Microsoft SQL Server 2016 SP1 or higher (Azure SQL and Azure Managed Instance are also supported). Otherwise, the legacy Syslog and Trap Viewers will remain the primary log management tools.

Find additional information on Orion Log Viewer features below:

- Create custom rules
- Reorder custom rules
- Orion alert integration
- Log forwarding
- Search event logs
- Filter event logs
- Filter entry details
- Use an additional polling engine
- Centralized Upgrades

To take advantage of additional event analysis features such as live event streaming, consider upgrading to Log Analyzer. Review the feature comparison here.

*If you are a VMAN user, and have the VMware Events add-on, navigate to My Dashboards > VMware Events in the Orion Web Console to view VMware events.

OLV installation scenarios

The following table addresses a variety of Orion Log Viewer (OLV) add-on installation scenarios applicable to select Orion Platform products.
**Product** | **New installation** | **Upgrade**
--- | --- | ---
NPM, NCM, SAM, UDT, VMAN* | • **Standard Installation:** Confirm you have Microsoft SQL 2016 SP1 or newer, and then choose to install the OLV add-on or decline.
• **Lightweight Installation:** This option automatically installs OLV. | • If the SQL condition is not met (e.g., SQL 2014 is detected), the add-on screen is skipped and OLV is not installed.
• If the SQL condition is met, but legacy syslogs, traps, and custom rules are detected in the database, you can choose to install OLV or decline (legacy syslog, trap, and alert data are not migrated to the new database).
• If the SQL condition is met and no legacy syslogs, traps, and custom rules are detected in the database, you can choose to install OLV or decline.

Other Orion Platform products | • OLV is not an installation option | • Same as the new installation scenario, unless you select additional products (e.g., NPM) during upgrade.

Review additional items to consider [here](#).

*OLV is required for viewing VMware events with VMAN.

**OLV feature comparison**

The following table lists the features available with the legacy Syslog and Trap Viewers, Orion Log Viewer (Basic), and Log Analyzer.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Syslog/Trap Viewers</th>
<th>Orion Log Viewer (Basic)</th>
<th>Log Analyzer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog collection</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Trap collection</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Windows event collection</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>VMware event collection*</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Search event logs</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Filter event logs</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Create custom rules</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Log tagging</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Histogram</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Feature</td>
<td>Syslog/Trap Viewers</td>
<td>Orion Log Viewer (Basic)</td>
<td>Log Analyzer</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>---------------------</td>
<td>--------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Live Mode</td>
<td>x</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>Orion alert integration</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cross-stack correlation via Perfstack™</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Filter on log tags</td>
<td>x</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>Separate database for log collection</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Free Poller Engine</td>
<td>x</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>Centralized Upgrades</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Syslog\Trap forwarding</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Export logs to CSV</td>
<td>x</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>Reorder custom rules</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Log Viewer access from Node Details resource</td>
<td>x</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>Log Summary dashboard</td>
<td>x</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>LA instant eval</td>
<td>x</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Windows event filtering</td>
<td>x</td>
<td>x</td>
<td>✓</td>
</tr>
</tbody>
</table>

* Requires a SolarWinds Virtualization Manager license.

**Evaluate Log Analyzer**

Orion Log Viewer users can unlock the complete feature set of Log Analyzer to gain full access to live event streaming and real-time network analysis. Click the Log Analyzer Activation button on your Orion Log Viewer toolbar to begin a free 30-day evaluation. Features include colorful log tagging, Windows event collection, log exporting, and more. Review the feature comparison [here](#).

💡 The standard installation of LA requires Microsoft SQL Server 2016 SP1 or newer. The lightweight installation typically used by evaluation customers installs Microsoft SQL Server 2017.

1. On the Orion Log Viewer toolbar, click Log Analyzer Activation.
2. Review the Log Analyzer feature overview, and then click Evaluate Log Analyzer.

3. Complete the evaluation registration form, and then click Activate.
4. When the confirmation window appears, review the additional guidance, and then click Close to begin using Log Analyzer.

![Log Analyzer Activation](image)

**OLV licensing model**

Monitor any networked Orion Platform node in the Orion Log Viewer (OLV) with your product (NPM, NCM, SAM, UDT, VMAN) license plan.* In the Orion Web Console, check for available licenses by navigating to Settings > All Settings, and then clicking License Details in the Details pane. The License Details page lists all licensed Orion Platform products, and the number of nodes currently consuming a license.

If you choose to take advantage of the free 30-day Log Analyzer (LA) evaluation, you will have unlimited LA licenses for Orion Platform nodes during the evaluation period.

When your LA evaluation expires, you only have access to OLV features. This means OLV will continue to use Orion Platform nodes for licenses, so you will receive message data, but you will not have access to live event streaming, the event histogram, event tagging, and more. Review the feature comparison [here](#).

As part of the LA licensing framework, LA receives messages from all nodes the Orion Platform manages. If you choose to purchase an LA license after your evaluation, the LA licensing framework combines Orion Platform nodes with your LA licenses. For instance, if you have NPM SL100 and SAM AL100, and then register an LA100 license, you can monitor up to 300 nodes, but only receive messages from 100 nodes. Of the total (300) nodes, you can select which 100 nodes you would like to monitor in LA.

*The Orion Platform does not support using LA with one set of nodes, and OLV on remaining nodes. In other words, if you have an LA10 license and a SAM AL100 license, you can monitor 10 nodes with LA, but you cannot monitor the other 90 with OLV.*

*Orion Platform products must include the syslog and trap feature as part of the license plan.*
Messages received from an unknown network node are discarded until you add the device through Node Management. When log activity is observed from an unknown device, you receive a notification in the Orion Web Console linking you to the Events page, where you can add the node as a managed device.

Enable or disable log and event monitoring

To adjust your node settings, edit the node properties, and then select one of the Log and Event Monitoring options.

1. In the Orion Web Console, navigate to Settings > Manage Nodes.

2. Select one or more nodes, and then click Edit Properties.

3. Scroll down to the Log and Event Monitoring section.

Choose one of the following options from the Status drop-down list:

- Default: Monitoring will be enabled for this node on receipt of the first message.
- Enabled: Monitoring is enabled for this node.
- Disabled: Monitoring is disabled for this node. Log and event data will be discarded for this node.

4. Click Submit.

You can also enable a node by selecting one or more nodes and clicking More Actions > Enable Log Monitoring.
Disable log monitoring

1. In the Orion Web Console, navigate to Settings > Manage Nodes.
2. Select one or more nodes, and then click Edit Properties.
3. Scroll down to the Log and Event Monitoring section, select Disabled from the Status drop-down list, and then click Submit.

You can also disable a node by selecting one or more nodes and clicking More Actions > Disable Log Monitoring.

Before removing a node, determine if it is collecting events from additional networked nodes that you want to continue monitoring. This action can result in loss of data from multiple nodes.

Explore the Orion Log Viewer

The Orion Log Viewer allows you to monitor and review logs from nodes monitored by your Orion Platform products. In the Log Viewer, you can access your syslog and trap messages, monitor VMware events*, filter and search event logs, integrate Orion alerts, and more.

- To access syslogs in the Orion Web Console, navigate to Alerts & Activity > Syslogs.
- To access traps in the Orion Web Console, navigate to Alerts & Activity > Traps.
- To access VMware events in the Orion Web Console, navigate to My Dashboards > VMware Events.

*Requires VMAN.
<table>
<thead>
<tr>
<th>Number</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Filters</td>
<td>The Filters pane displays all filters you can apply to event messages. All filters are stored in groups. To apply a filter to the events table, click to expand a filter group, and then select a filter. The events table refreshes and displays events allowed by the filter conditions. Click the Hide Pane icon to collapse the pane, or the Show Pane icon to expand it.</td>
</tr>
<tr>
<td>2</td>
<td>Events</td>
<td>The Events table displays events that exist for your selected filter. The Filters pane displays the total number and names of applied filters. Enter keywords in tandem with the Filters pane to review specific activity. Select a specific event to view the associated details in the Entry Details pane. The color of the event (red, yellow, light blue) denotes the level of logged events (Error, Warning, Informational).</td>
</tr>
<tr>
<td>3</td>
<td>Orion Web Console menu bar</td>
<td>Use the Orion Web Console menu bar to access integrated Orion Platform products and functions, view your notifications, log out, and launch the Success Center.</td>
</tr>
<tr>
<td>4</td>
<td>Log Viewer toolbar</td>
<td>Use the Log Viewer toolbar to upgrade to Log Analyzer and access your log processing configuration rules.</td>
</tr>
<tr>
<td>5</td>
<td>Entry Details</td>
<td>The Entry Details pane displays specific information about the last event you selected in the Events table. When you click an event, the event is highlighted in the Entry Details pane along with supporting information. Click one or more entry details filter icons to apply additional conditions to your current filter set.</td>
</tr>
</tbody>
</table>

Create custom log-processing rules

On the Log Processing Configuration page, you can create custom rules to complement the standard, out-of-the-box rule sets. You can define rule conditions to identify a specific log entry, and then establish subsequent actions, such as executing commands and discarding log entries.

The pre-defined Rule Policy groups organize rule policies based on the message source and determine the rule policy evaluation order. The Processing Policies pane is organized into the following policy groups:

- Syslog
- Traps
- VMware Events
- Windows Events (Log Analyzer only)
- Global Pre-processing: Evaluated before log-specific and global post-processing rule policies
- Global Post-processing: Evaluated after all log-specific rule policies

<table>
<thead>
<tr>
<th>Group</th>
<th>Message Type</th>
<th>Evaluation Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Pre-processing</td>
<td>All messages</td>
<td>1</td>
</tr>
<tr>
<td>Syslog</td>
<td>Syslog messages</td>
<td>2</td>
</tr>
<tr>
<td>Group</td>
<td>Message Type</td>
<td>Evaluation Order</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Traps</td>
<td>Trap messages</td>
<td>3</td>
</tr>
<tr>
<td>VMware Events</td>
<td>VMware event messages</td>
<td>4</td>
</tr>
<tr>
<td>Windows Events (Log Analyzer only)</td>
<td>Windows event messages</td>
<td>5</td>
</tr>
<tr>
<td>Global Post-processing</td>
<td>All messages</td>
<td>6</td>
</tr>
</tbody>
</table>

1. On the Log Viewer toolbar, click Configure Rules.

![LOG ANALYZER ACTIVATION] [CONFIGURE RULES]

2. In the Processing Policies pane, click to expand a policy group, and then click My Custom Rules.

3. Click Create New Rule.

![PROCESSING POLICIES] [CREATE NEW RULE]

- IF BGP Neighbor Change - Syslog
  THEN Add tags: 'BGP Neighbor Change'

- IF BGP Peer Down
  THEN Trigger Orion Alert

- IF BGP Peer Established
  THEN Trigger Orion Alert
4. Enter a descriptive name for the rule, and then click Next.

5. Select your source computers.
   You can choose to trigger this alert from all sources, or specify conditions and values for one or more sources.
6. Define your log entry rule conditions and values, and then click Next.

7. Select one or more log entry actions.

8. Integrate an alert action, and then click Next.

9. Review your rule summary, and then click Save to create the rule. To edit your rule conditions and actions, click Back.

10. After you create one or more rules, you can then edit, enable, or disable each rule.

11. To return to the Log Viewer, navigate to My Dashboards > Logs > Log Viewer.

Add custom rule actions

You can add one or more of the following actions to any custom rule:

- **Forward the entry**: Send the entry to another system for further processing.
- **Run an external program**:
  1. In the Rule Actions pane, click Add an Action.
  2. Select Run an External Program, and then click Configure Action.
  3. Enter the program to run, command line arguments (optional), and then click Done.
- **Flag for discard**: The log entry is not saved to the database, but subsequent rule actions are still applied.
- **Stop processing rules**: Stops additional rule processing for the active log entry.
Reorder custom rules

On the Log Processing Configuration page, you can change the processing order for each of your custom rules.

1. On the Log Viewer toolbar, click Configure Rules.

2. In the Processing Policies pane, click to expand a policy group, and then click My Custom Rules.

3. Select one or more custom rule check boxes, and then click Move Rule.

4. In the custom rule list, select a rule, and then click Insert Above, or Insert Below.

Drop unwanted event logs

Streamline your Log Viewer table by selecting and dropping unwanted event logs that clutter your log feed and occupy valuable database space. You can establish rule parameters that will discard all undesired logs to ensure relevant content is displayed in a more efficient manner.
Integrate Orion alerts with Orion Log Viewer

On the Log Processing Configuration page, you can integrate alert actions into your custom rules, or create new rules and apply alert actions. You can configure your rule to send an event to the Orion Platform alerting engine when rule criteria are met, and also create a new alert that fires each time a rule is triggered.

For more information about Orion Platform alerting, see Use alerts to monitor your environment with the Orion Platform. To create a new rule, see Create custom log-processing rules.

Integrate an alert into an existing rule

1. On the Log Viewer toolbar, click Configure Rules.

2. In the Processing Policies pane, click to expand a policy group, and then click My Custom Rules.

3. Select an existing rule, and then click Edit Rule.
4. To integrate an alert, click Next, and then click Next again to view the rule actions.

5. To send a log rule fired event to Orion Platform alerting, select the associated check box. This action allows you to see the event on the Manage Alerts page and use it when defining a custom alert.

6. To create a new alert that fires when the rule is triggered, select the associated check box.

7. Enter a name for the alert.
8. From the drop-down list, select a severity level.

<table>
<thead>
<tr>
<th>Alert Name</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denied Traffic</td>
<td></td>
</tr>
</tbody>
</table>

9. Establish your reset conditions.

- **Reset this alert automatically after**
  Select to reset an alert after a set amount of time has passed. If this interval is less than the amount of time you wait for different escalation levels, the escalation levels that occur after this interval do not fire. This reset condition is especially useful to remove event-based alerts from Active Alerts.

  For example, if the trigger conditions still exists after 48 hours, you can use this to trigger your alert actions again. The alert is reset and triggers as soon as the trigger condition is detected, which is as soon as the objects are polled for this example.

- **No reset condition** - Trigger this alert each time the trigger condition is met
  The alert fires each time the trigger conditions are met.

  For example, when the alert for node 192.168.4.32 going down fires, a new alert for 192.168.4.32 fires every time the node is down when it is polled.

- **No reset action**
  The alert is active and is never reset. To re-trigger the alert, the alert must be manually cleared from the Active Alerts view.
10. Click Next. The rule summary displays the alert integration actions.

```
<table>
<thead>
<tr>
<th>Rule Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
</tr>
<tr>
<td>Enabled (On/Off)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SOURCE COMPUTERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>All source computers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LOG ENTRIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>IF Message</td>
</tr>
<tr>
<td>Contains power_error</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIRST</td>
</tr>
<tr>
<td>Add tags: 'Power Error'</td>
</tr>
<tr>
<td>Power Error</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ALERT INTEGRATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>When this rule fires, send a Log Rule Fired event to Orion Alerting.</td>
</tr>
</tbody>
</table>
```

11. Review the rule summary, and then click Save to apply the settings. To edit the rule conditions, click Back.

12. To view your alerts in the Orion Web Console, navigate to Settings > All Settings.

13. In Alerts and Reports, click Manage Alerts.
14. In the search field, enter Log Manager.

15. Select an existing alert to edit properties, enable or disable the alert, and assign actions.

You can also integrate alerts when creating a new custom rule and add multiple alert actions to one custom rule.

If you would like to modify the message and trigger actions of an out-of-the-box alert, duplicate the alert, and then edit as needed. If you do not change the trigger condition, disable the out-of-the-box alert to avoid duplicate alert notifications.

To add the log message that triggers the alert, copy the macro below to the alert message definition on the Trigger Actions page.

${N=OLM.AlertingMacros;M=OLMAgentMessage.EventMessage}

To view and access linked alerts, click Trigger Orion Alert in your custom rules list on the Log Processing Configuration page.

To view your active alerts in the Orion Web Console, navigate to Alerts and Activity > Alerts. When your alert triggers, it appears in the All Active Alerts page along with all with all your other OrionAlerts. From here, you can acknowledge alerts, view alert details and clear the triggered instance of an alert.

Set OLV storage and search retention period

On the Log and Event Settings page, you can set the number of days that syslog and trap messages are stored and searchable in the OLV database. The default setting is seven days, but you can adjust it to anywhere from one day to one year.
1. In the Orion Web Console, navigate to Settings > All Settings.
2. Scroll down to Product Specific Settings and click Log and Event Settings.
3. Enter the total number of days to keep syslog, traps, Windows events, and VMware events, and then click Save.*

The Log and Event Settings page also provides links to log processing rules, unmanaged log senders, managed but unlicensed log senders, and log monitoring options.

*The available options will vary based on the Orion Platform products you have installed.

Log forwarding

On the LA Log Processing Configuration page, create custom rules to forward your syslog and trap messages to a dedicated server. This feature allows you to forward log data to third-party systems and other SIEM tools.

1. On the Log Viewer toolbar, click Configure Rules.

2. In the Processing Policies pane, click to expand the Syslog or Traps policy group, and then click My Custom Rules.
3. Click Create New Rule.
4. Enter a descriptive name for the rule, and then click Next.

5. Select your source computers.
   You can choose to trigger this alert from all sources, or specify conditions and values for one or more sources.

6. Define your log entry rule conditions and values, and then click Next.

7. Select Forward the Entry, and then click Configure Action.
8. Enter the destination server IP and UDP port.

To forward secure syslogs, select TCP over TLS from the Via drop-down list, and then enter port 6514.

Select one of the following options for the source address:

- Use the Orion server's address as the source address
- Use the original sender's address as the source address
- Use a custom source address

9. Click Done, and then click Next.

10. Review your rule summary, and then click Save to create the rule. To edit your rule conditions and actions, click Back.
Search and filter historical event logs

The Filters pane displays all filters you can apply to event messages. All filters are stored in groups. To apply a filter to the events table, click to expand a filter group, and then select a filter. The events table refreshes and displays the incoming events allowed by the filter conditions. Click the Hide Pane icon to collapse the pane, or the Show Pane icon to expand it.

1. On the Orion Web Console menu bar, navigate to Alerts and Activity > Syslogs (or Traps).*
2. To apply a filter to the events table, click to expand a filter group, and then select one or more filters.
3. To set your time frame, open the custom time picker, select a quick pick option, or set a start and end date.

---

*Note: The Orion Web Console menu bar and interface may vary depending on the version of the Orion platform you are using. The steps provided are a general guideline and may not reflect the exact menu options available in your version.
4. To further refine your search results, enter a key word in the search box.

![Log Viewer](image)

*If you are a VMAN user, and have the VMware Events add-on, navigate to My Dashboards > VMware Events in the Orion Web Console to view VMware events.*

Filter entry details

1. In the Log Viewer table, click a log to view the associated event details.
2. In the Entry Details pane, click one or more filter icons.
3. To remove an Entry Details filter, click the associated Remove Item icon above the Filters pane.
Monitor Syslog messages

Syslog messages are received by the SolarWinds Syslog Service, which listens for incoming messages on UDP port 514. Received messages are decoded and stored in the SolarWinds Orion database. The SolarWinds Syslog Service can handle large numbers of simultaneously incoming Syslog messages from all your monitored devices.

A SolarWinds installation can process approximately 1 million Syslog messages per hour, which is about 300 Syslog messages per second. You can process more by increasing your hardware requirements over the minimum requirements.

You can view Syslog messages in the Orion Web Console or in the Syslog Viewer application.

Before you begin

- Confirm that your network devices are configured to send Syslog messages to the Orion server IP address. For proper configuration of network devices, refer to the documentation supplied by the device vendor.
- Ensure UDP port 514 is open for IPv4 and IPv6.
- The message must be formatted according to the Request for Comments (RFC) requirements.
- If a long message is split into smaller parts, these parts should be formatted to not be skipped.

SolarWinds recommends setting up Enable RFC Relay in the service to true to allow the service to restructure the message by adding the default facility, severity, or date.

View Syslog messages in the Orion Web Console

The Orion Web Console provides both syslog-specific resources and a syslog view with a table of syslog messages received by your Orion server.

The Syslog view displays a list of all the syslog messages generated by monitored network devices. The messages are listed by time of transmission, with the most recent at the top of the list.

1. Log in to the Orion Web Console, and click Alerts & Activity > Syslogs in the menu bar.

Starting with Orion Platform 2019.4, you can switch to displaying syslogs in the Log Viewer.
2. If you are using Orion Platform 2019.2 and earlier, or if you decided to keep the Syslogs view in Orion Platform 2019.4, you can use Syslogs as follows:
   
a. To filter syslog messages so that only messages relevant for specific devices are displayed:
      • To view messages for a specific syslog-enabled network object, select it in the Network Object list.
      
      Only objects that have sent a syslog message to the Orion server will be listed in this field.
      
      • To view messages for a specific device, provide the IP address in the IP Address field.
      • To view messages for a specific device type, select it in the Type of Device list.
      • To view messages for a specific vendor, select the vendor in the Vendors list.
   
b. To select which syslog messages should be displayed:
      • To view only messages with a severity, select the severity.
      • To view messages for a facility, select the facility.
      • To view messages of a type, type the string into the Message Type field.
      • To view only messages containing a pattern, provide the string in the Message Pattern field.

      You can use the following wildcards:
      
      Asterisk (*)
      
      Use * before or after the pattern string if the provided pattern is not the beginning, the end or the full message.
      
      Underscore (_)
      
      Use _ as a placeholder for one character.
      
      • To view syslog messages from a specific period of time, select either a period of time or enter custom Beginning and Ending Date/ Times.
      • Type the number of syslog messages you want to view into Number of Displayed Messages.
      • To view cleared and acknowledged syslog messages, select Show Cleared Messages.
   
c. Click Refresh to update the syslog messages list with your settings.

Syslog messages matching the selected criteria display in a list beneath the search area.

Click Hide or Show in the top-right corner of the view to remove or restore the Syslog messages search criteria area.

Click the Hostname or Message to open the Device Details view for the device.

Clear Syslog messages in the Orion Web Console

1. Log in to the Orion Web Console.
2. Click Alerts & Activity > Syslogs in the menu bar.
3. Define what you want to see in the Syslog messages table, and click Refresh.

4. Select the messages you want to acknowledge, and click Clear Selected Messages.

The messages are cleared. You can see cleared messages when you select the Show Cleared Messages box.

Syslog widgets in the Orion Web Console

- **Advanced Syslog Counts**: This widget groups by severity all Syslog messages received by the currently viewed node. For each severity, this resource provides the number of received Syslog messages.

- **Advanced Syslog Parser**: This widget provides a comprehensive view of the Syslog messages most recently received by the viewed node.

- **Advanced Syslog Summary**: This widget groups by message type all Syslog messages received by the currently viewed node, where the message type is encoded in the Syslog message packet. For each message type, this widget provides the severity, the hostname or IP address of the message originator, and the total number of Syslog messages received.

- **Last 25 Syslog Messages**: This widget provides a list of the last 25 Syslog messages sent by monitored network devices to the viewed node.

  Click the hostname, IP address, or message text to the Object Details page, which provides extensive diagnostic information about the monitored network.

  Click Edit to set the maximum number of displayed messages, select the time period for viewing messages, or establish filters to limit the displayed messages.

- **Syslog Summary**: This widget lists the Syslog messages received by the viewed node from monitored network devices over a specified period of time.

View syslog messages in the Syslog Viewer

SolarWinds Orion also provides the standalone Syslog Viewer application for viewing and acknowledging Syslog messages on your network. Syslog Viewer collects Syslog messages from your network and presents them in a readily reviewable and searchable list so that you can easily monitor your network.

You must be able to log in to the computer running your Orion server.

Open the Syslog Viewer by clicking Start > All Programs > SolarWinds Orion > Syslog Viewer.
View and clear Syslog messages in the Syslog Viewer

Syslog Viewer collects Syslog messages from your network and presents them in a readily reviewable and searchable list so that you can easily monitor your network. Clear messages you have already read and acted upon.

You must be able to log in to the computer running your Orion server.

1. Click Start > All Programs > SolarWinds Orion > Syslog Viewer.
2. Click View > Current Messages.
3. Clear read messages:
   - Right-click any message, and select Acknowledge Selected.
   - Add an Acknowledged column to the Syslog Viewer, and select the messages that you want to acknowledge.

Selected messages are acknowledged now.

Search for Syslog messages in the Syslog Viewer

In the Syslog Viewer, you can search through collected Syslog messages and format search results.

1. Click View > Search Messages.
2. Enter the search criteria.
3. Click Search Database.
4. To group messages for easier navigation, select the type of grouping from the Grouping list.

You can acknowledge messages both in the search results and in the Current Messages view. See Configure the Syslog Viewer.

5. To limit the number of displayed message, enter or select a number in the Maximum Number of Messages to Display field.
6. To view messages that meet your search criteria as they arrive, select a number for the Auto Refresh Every number of seconds field.

Auto Refresh is only available when you are viewing current messages. The Date/Time Range must be set to Today, Last 24 Hours, Last 2 Hours, or Last Hour.

Configure the Syslog Viewer

You must be able to log in to the computer running your Orion server.

1. Click Start > All Programs > SolarWinds Orion > Syslog Viewer.
2. Click File > Settings.
3. Click the General tab in the Syslog Server Settings window.
4. Adjust the Maximum Number of Messages to Display in Current Messages view slider to set the number of messages you want to display.

5. Automatically refresh the current messages view by selecting the option, and setting the refresh rate with the middle slider.

6. Adjust Retain Syslog Messages for How Many Days to set the length of time Syslog messages should stay in the database.

   - This setting significantly affects the database size and performance.

7. Click the Displayed Columns tab.

8. Use the arrow keys to select and order the fields of information you want to see in the Current Messages view.

   - Clearing Syslog messages is easier if you add the Acknowledged column to your view.


10. If you do not expect to use the Syslog Viewer as your primary viewer for Syslog messages, select the Message Parsing tab, and select what should be removed:

    - Remove embedded Date/Time from Syslog Messages
    - Remove Message Type from Syslog Messages
    - Remove Domain Name from DNS Lookups.

   - Removing the added data from each record helps you reduce the size of your SolarWinds Orion database.
Trigger alerts when receiving specific Syslog messages

You must be able to log in to the computer running your Orion server.

1. Click Start > All Programs > SolarWinds Orion > Syslog Viewer.
2. Click File > Settings.
3. Click Alerts/Filter Rules.
4. Click Add New Rule to create a rule, or edit a selected rule.
5. On the General tab, complete the following steps:
   a. Provide or edit the Rule Name.
   b. Select Enabled.
   c. Select the servers from the Apply this Rule To list.
   d. Enter the IP addresses or subnets to which this rule applies in the Source IP Addresses area.

Syslog rules may not be applied to nodes in an unmanaged state.

6. To limit the rule only to messages from specific hosts, domains, or host name patterns, click the DNS Hostname tab, and enter a DNS Hostname Pattern.

   The DNS Hostname Pattern rule is case-sensitive.

   To use regular expressions, select Use Regular Expressions in this Rule.

7. To limit the rule only to specific message types or texts within a Syslog message, go to the Message tab, and enter rules for Message Type Pattern and Syslog Message Pattern.

8. To apply specific severity or facility types, go to the Severity / Facility tab, and select the severity and facility types.
   By default, all message severities and facilities are selected.

9. To apply the rule only during a specific period of time, select the Time of Day tab, select Enable Time of Day Checking, enter the time period, and select the days of the week on which to apply the rule.
   Messages received outside the specified time frame will not trigger alerts.

   Enabling Time of Day checking creates more overhead for the CPU.

10. To suppress alert actions until a specified number of messages arrive that match the rule, complete the following procedure:
    a. Select the Trigger Threshold tab, and select Define a Trigger Threshold for this Rule.
    b. Enter option values.

   When Suspend Further Alert Actions For is selected, alert actions are not sent until the specified amount of time has expired. When the time period expires, only new alerts are sent. All alerts suppressed during the time period are discarded.
11. Configure Syslog alert actions on the Alert Actions tab:
   a. To create an action for the rule, click Add New Action.
   b. To edit an action for the rule, select the action, and click Edit Selected Action.
   c. Configure the action.
   d. To delete an action, select the action, and click Delete Action.
   e. Use the arrow buttons to set the order in which actions are performed. Actions are processed in the order listed, from top to bottom.
   f. Click OK to save all changes and return to Syslog Viewer Settings.

12. Use the arrow buttons to arrange the order in which the rules are applied. Rules are processed in the order they appear, from top to bottom.

Syslog alert actions

**Discard the Syslog Message**
Delete unwanted Syslog messages sent to the Syslog server.

**Tag the Syslog Message**
Add a custom tag to received Syslog messages. Ensure you include the Tag column in the viewer when assigning a tag.

**Modify the Syslog Message**
Modify the severity, facility, type, or contents of a Syslog message.

**Log the Message to a file**
Specify a file and a series of variables with which to tag Syslog messages sent to the file. Ensure you have already created the log file you want to use. The alert cannot create a file.

**Windows Event Log**
Write a message to local or remote Windows Event Logs.

**Forward the Syslog message**
Specify the IP address or hostname and the port to forward a Syslog event.

**Send a new Syslog message**
Trigger a new Syslog message, sent to a specific IP address or hostname, on a specific port, with a customizable severity, facility, and message.

**Send an SNMP Trap**
Send a trap to an IP address following a specific trap template and using a specific SNMP community string.
Play a sound

Play a sound when a matching Syslog message is received.

Text to Speech output

Define the speech engine, speed, pitch, volume, and message to read.

Execute an external program

Allows you to specify an external program to launch using a batch file. This action is used when creating real-time change notifications in Orion.

Execute an external VB Script

Launch a VB Script using the selected script interpreter engine and a saved script file.

Send a Windows Net Message

Send a net message either to a specific computer or to an entire domain or work group.

Send an E-mail / Page

Send an email from a specified account to a specified address, using a specific SMTP server, and containing a customizable subject and message.

Stop Processing Syslog Rules

Stops the processing of Syslog rules for the matching Syslog message.

Forward syslog messages

The Syslog message forwarding action allows you to forward received syslog messages. Additionally, if you have WinPCap version 3.0 or later installed on your Orion server, you can forward syslog messages as spoofed network packets.

The following procedure assumes you are editing a Forward the Syslog Message alert action. For more information, see Trigger alerts when receiving specific Syslog messages.

1. Provide the hostname or IP address of the destination to which you want to forward the received syslog message.
2. Provide the UDP Port you are using for Syslog messaging.
   - The default is UDP port 514.
3. Specify what IP address should be used for the source device in the syslog message. By default, the device IP is replaced by the Orion server IP address.
   - To designate a specific IP address or hostname as the Syslog source, select Retain the Original Source Address of the Message, select Use a Fixed Source IP Address, and provide the IP address or hostname.
   - To keep the original IP address of the syslog source device, select Retain the Original Source Address of the Message, select Spoof Network Packet, and select the Network Adapter.
4. Click OK to complete the configuration.

You have defined the destination, port for sending the syslog message, and the source IP of the device in the syslog message used in the alert action.

Syslog message priorities

At the beginning of each Syslog message, there is a priority value. The priority value is calculated using the following formula:

Priority = Facility * 8 + Severity

Syslog facilities

The facility value indicates which machine process created the message. The Syslog protocol was originally written on BSD Unix, so Facilities reflect the names of UNIX processes and daemons.

If you are receiving messages from a UNIX system, consider using the User Facility as your first choice. Local0 through Local7 are not used by UNIX and are traditionally used by networking equipment. Cisco routers, for example, use Local6 or Local7.

<table>
<thead>
<tr>
<th>Number</th>
<th>Source</th>
<th>Number</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>kernel messages</td>
<td>12</td>
<td>NTP subsystem</td>
</tr>
<tr>
<td>1</td>
<td>user-level messages</td>
<td>13</td>
<td>log audit</td>
</tr>
<tr>
<td>2</td>
<td>mail system</td>
<td>14</td>
<td>log alert</td>
</tr>
<tr>
<td>3</td>
<td>system daemons</td>
<td>15</td>
<td>clock daemon</td>
</tr>
<tr>
<td>4</td>
<td>security/authorization messages</td>
<td>16</td>
<td>local use 0 (local0)</td>
</tr>
<tr>
<td>5</td>
<td>messages generated internally by Syslog</td>
<td>17</td>
<td>local use 1 (local1)</td>
</tr>
<tr>
<td>6</td>
<td>line printer subsystem</td>
<td>18</td>
<td>local use 2 (local2)</td>
</tr>
<tr>
<td>7</td>
<td>network news subsystem</td>
<td>19</td>
<td>local use 2 (local3)</td>
</tr>
<tr>
<td>8</td>
<td>UUCP subsystem</td>
<td>20</td>
<td>local use 2 (local4)</td>
</tr>
<tr>
<td>9</td>
<td>clock daemon</td>
<td>21</td>
<td>local use 2 (local5)</td>
</tr>
<tr>
<td>10</td>
<td>security/authorization messages</td>
<td>22</td>
<td>local use 2 (local6)</td>
</tr>
<tr>
<td>11</td>
<td>FTP daemon</td>
<td>23</td>
<td>local use 2 (local7)</td>
</tr>
</tbody>
</table>
Syslog severities

The following table provides a list of Syslog severity levels with descriptions and suggested actions for each.

<table>
<thead>
<tr>
<th>Number</th>
<th>Severity</th>
<th>Suggested Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Emergency</td>
<td>A &quot;panic&quot; condition affecting multiple applications, servers, or sites. System is unusable. Notify all technical staff on call.</td>
</tr>
<tr>
<td>1</td>
<td>Alert</td>
<td>A condition requiring immediate correction, for example, the loss of a backup ISP connection. Notify staff who can fix the problem.</td>
</tr>
<tr>
<td>2</td>
<td>Critical</td>
<td>A condition requiring immediate correction or indicating a failure in a primary system, for example, a loss of a primary ISP connection. Fix CRITICAL issues before ALERT-level problems.</td>
</tr>
<tr>
<td>3</td>
<td>Error</td>
<td>Non-urgent failures. Notify developers or administrators as errors must be resolved within a given time.</td>
</tr>
<tr>
<td>4</td>
<td>Warning</td>
<td>Warning messages are not errors, but they indicate that an error will occur if required action is not taken. An example is a file system that is 85% full. Each item must be resolved within a given time.</td>
</tr>
<tr>
<td>5</td>
<td>Notice</td>
<td>Events that are unusual but are not error conditions. These items might be summarized in an email to developers or administrators to spot potential problems. No immediate action is required.</td>
</tr>
<tr>
<td>6</td>
<td>Informational</td>
<td>Normal operational messages. These may be harvested for network maintenance functions like reporting and throughput measurement. No action is required.</td>
</tr>
<tr>
<td>7</td>
<td>Debug</td>
<td>Information useful to developers for debugging an application. This information is not useful during operations.</td>
</tr>
</tbody>
</table>
Monitor SNMP traps

If you monitor a large number of devices, where each device may have many connected objects of its own, requesting information from each device is impractical. You can set up the SNMP Trap Server, and each managed device can notify it about any issues by sending a trap message.

SNMP traps are received by the SolarWinds Trap Service, which listens for incoming trap messages on UDP port 162, and then decodes, displays, and stores the messages in the SolarWinds Orion database.

By default, SNMP traps are stored in the Traps and TrapVarBinds tables in the Orion database.

The SolarWinds Trap Service can receive and process SNMP traps from any type of monitored network device, and can handle large numbers of simultaneously incoming traps.

A SolarWinds installation can process approximately 500 traps per second. Higher capacity can only be achieved with significant hardware improvements over minimum SolarWinds requirements.

You can view SNMP traps either in the Orion Web Console or in the Trap Viewer application. In the Trap Viewer, you can configure trap-specific alerts, to view, filter, and search for traps.

Before you begin

- Configure devices to send SNMP traps to the IP address assigned to the Orion server. For more information about proper configuration, refer to the documentation supplied by the vendor of your devices.
- Make sure the UDP port 162 is open for IPv4 and IPv6.
- When you use SNMPv3 for polling a device and receiving traps from it, confirm that the same authentication type (auth, noauth, or priv) is configured for both polling and traps.

View SNMP traps in the Orion Web Console

1. Log in the Orion Web Console.
2. Click Alerts & Activity > Traps in the menu bar.

Starting with Orion Platform 2019.4, you can switch to displaying traps in the Log Viewer.

3. If you are using Orion Platform 2019.2 and earlier, or if you decided to keep the Traps view in Orion Platform 2019.4, you can use Traps as follows:
   a. To display only traps relevant for a specific device, specify the device:
      - To display only traps for a device, select the device in the Network Object field.
      - To view traps for certain device type, select the device type in the Type of Device field.
b. Define what traps you want to view:
   - To view only traps of a designated type, select the type in the Trap Type field.
   - To view only traps originating from a specific IP address, type the IP Address in the Source IP Address field.
   - To view only traps with a designated community string, select the string in the Community String field.
   - To view only traps from a specific period of time, select the time period from the Time Period menu.

   c. Confirm the number of traps displayed in the Number of Displayed Traps field.
   d. Click Refresh to update the Traps view with your new settings.

View current traps in the Trap Viewer

The Trap Viewer is an application which allows you to view, search for traps, or configure filters and alerts.

You must be able to log in to the computer running your Orion server.

1. Click Start > All Programs > SolarWinds Orion > Trap Viewer.
2. Click View > Current Traps.
3. Click a column header to order listed traps by the selected trap characteristic.
4. Configure the Trap Viewer by clicking and dragging columns to order the presentation of trap characteristics.

The current traps are now displayed according to your settings.

Search for traps in the Trap Viewer

You can search collected trap messages and format the search results list in the Trap Viewer.

1. Click Start > All Programs > SolarWinds Orion > Trap Viewer.
2. Click View > Search Traps.
3. Enter search criteria, and click Search Database.
4. To group messages for easier navigation, select the type of grouping from the Grouping list.
5. To limit the number of displayed messages, enter or select a number in the Maximum number of messages to display field.
6. To view messages that meet your search criteria as they arrive, select a number for the Auto Refresh Every number seconds field.

Auto Refresh is only available when you are viewing current messages. The Date / Time Range must be set to Today, Last 24 Hours, Last 2 Hours, or Last Hour.

7. To hide the search criteria pane, toggle the pane open and closed by clicking the double up arrows in the top right of the page.
You can now see the traps according to your settings.

**Configure the Trap Viewer**

1. Click Start > All Programs > SolarWinds Orion > Trap Viewer.
2. Click File > Settings.
3. On the General tab, configure the Trap server settings:
   a. Position the top slider to set the Maximum Number of Traps to Display in Current Traps View.
   b. If you want to Automatically Refresh the Current Traps View, select the option, and position the middle slider to set the refresh rate.
   c. Position the Retain Trap Messages For How Many Days slider to set the length of time that traps remain in the database.
4. On the Displayed Columns tab, use the arrow keys to select and order the fields of information you want to see in the Current Traps view.
5. If you do not need the domain name in your trap messages, select Remove Domain Name from DNS Lookups on the Message Parsing tab.

   - Selecting this option can slightly reduce the size of your database.

**Configure Trap Viewer filters and alerts**

In the Trap Viewer, you can filter trap messages, and configure actions that trigger when received trap messages match defined rules.

- Click Start > All Programs > SolarWinds Orion > Trap Viewer.
- Click File > Settings, and click the Alerts / Filter Rules tab.
- Click Add Rule or click Edit Rule.
- Click the General tab, and select Enabled.
- Select the servers from the Apply This Rule To list.
- Apply the rule to specific messages.
  - Click DNS Hostname, and enter a DNS Hostname Pattern to apply the rule to messages from specific hosts, domains, or hostname patterns.
    - The DNS Hostname Pattern rule is case-sensitive.
  - Click Trap Details, and enter a Trap Details Pattern to apply the rule based on the Trap Details page 273
7. Click Conditions to define the what triggers the rule.
   - Select object identifiers and comparison functions from the linked context menus.
   - Click Browse (...) to insert conditions.

8. Click Time of Day > Enable Time of Day Checking to apply the rule during a specific period of time. Messages received outside the specified time frame will not trigger alerts.

   | Enabling Time of Day checking creates more overhead for the CPU. |

9. Click Trigger Threshold > Define a Trigger Threshold for this Rule to suppress alert actions until a specified number of traps arrive that match the rule.

   | When Suspend Further Alert Actions For is selected, alert actions are not sent until the specified amount of time has expired. When the time period expires, only new alerts are sent. All alerts that are suppressed during the time period will never be sent. |

10. Click Alert Actions.
    - Associate the rule with a new action by clicking Add New Action, and then selecting an action from the list to configure.
    - Edit an existing action for the rule.

11. Use the arrow buttons to set the order in which actions are performed.

    | Actions are processed in the order they appear, from top to bottom. |

12. Click OK to save all changes and return to Trap Viewer Settings.

13. Use the arrow buttons to arrange the order in which the rules are applied.

    | Rules are processed in the order they appear, from top to bottom. |

Trap messages are now filtered by the rules and alert actions are triggered when the rule conditions are met.

### Available trap alert actions

**Discard the Trap**

Delete unwanted traps sent to the SNMP Trap server.

**Tag the Trap**

Add a custom tag to received traps. Ensure you include the Tag column in the viewer when assigning a tag.
Flag the Trap with a specific color

Assign a specific color for display in the Orion Web Console and the Trap Viewer to flag traps matching the rule.

Log the Trap to a file

Specify a file and a series of variables with which to tag traps sent to the file. Ensure you have already created the log file you want to use. The alert cannot create a file.

Windows Event Log

Write a message to a local or a remote Windows Event Log.

Forward the Trap

Specify the IP address or hostname and the port on which to forward the trap. Specify the IP address or hostname of the trap destination and the port on which the trap should be sent. Check Include Source Address to include the IP address of the trap source.

Play a sound

Play a sound when a matching SNMP trap is received.

Text to Speech output

Define a specific speech engine, the speed, pitch, volume, and message to read.

Execute an external program

Specify an external program to launch using a batch file. This action is used when creating real-time change notifications in SolarWinds NPM.

Execute an external VB Script

Allows you to launch a VB Script using the selected script interpreter engine and a saved script file.

Send a Windows Net Message

Send a Windows Net message either to a specific computer or to an entire domain or workgroup.

Send an E-mail / Page

Send an email from a specified account to an address, using a specific SMTP server, and containing a customizable subject and message.

Stop Processing Trap Rules

Stops the processing of SNMP trap rules for the matching trap.

Change the status of an interface

SolarWinds NPM can change the status of an interface from which a trap is received. Designate the status to which the interface should change.
What is a Trap Template?

Trap templates are used to format your trap messages. You can use SolarWinds macros or variables in the OID Value and ValueName attributes or call values from your MIB.

The templates are placed in the following locations:

- /SolarWinds/Common/Orion-Detailed-Alert.trap
- /SolarWinds/Common/Orion-Generic-Alert.trap
- /SolarWinds/Orion/ForwardSyslog.trap

The following table describes the OIDs section of the Orion Generic Alert trap template. This is the section you modify to display the information you want in your trap messages.

<table>
<thead>
<tr>
<th>Template OID line</th>
<th>Information returned</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID OID=&quot;1.3.6.1.2.1.1.3.0&quot; MIB=&quot;RFC1213-MIB&quot; Name=&quot;sysUpTime.0&quot; Value=&quot;0&quot; DataType=&quot;67&quot; ValueName=&quot;0&quot; HexValue=&quot;&quot;</td>
<td>This line displays how long the device has been up.</td>
</tr>
<tr>
<td>OID OID=&quot;1.3.6.1.6.3.1.1.4.3.0&quot; MIB=&quot;SNMPv2-MIB&quot; Name=&quot;snmpTrapEnterprise.0&quot; Value=&quot;1.3.6.1.4.1.11307&quot; DataType=&quot;6&quot; ValueName=&quot;enterprises.11307&quot; HexValue=&quot;&quot;</td>
<td>This line displays the enterprise associated with the trap.</td>
</tr>
<tr>
<td>OID OID=&quot;1.3.6.1.4.1.11307.10.1&quot; MIB=&quot;SNMPv2-SMI&quot; Name=&quot;enterprises.11307.10.1&quot; Value=&quot;${AlertMessage}&quot; DataType=&quot;4&quot; ValueName=&quot;${AlertMessage}&quot; HexValue=&quot;&quot;</td>
<td>When the template is used in an alert, this line displays the alert message associated with the triggered alert.</td>
</tr>
</tbody>
</table>

Add more information by adding another OID element and incrementing the OID.
Alert Integrations in the Orion Platform

You can integrate Orion Platform products with the following IT Service Management solutions:

- ServiceNow® (Orion Platform 2016.1 or later)
- SolarWinds Service Desk (starting with Orion Platform 2019.4)

Integrating an alerting solution with the Orion Platform means that triggering an alert in the Orion Platform creates a new incident in the integrated alerting instance and vice versa.

Configure the integration

To make the integration of the Orion Platform and your alerting system work, complete the following steps.

Step 1: Set up the system to integrate with the Orion Platform.

- ServiceNow
- SolarWinds Service Desk

Step 2: Create an instance for the system in the Orion Platform.

Step 3: Configure Orion Platform alerts to create an incident (ServiceNow or SolarWinds Service Desk) as the alert action.

Configure the instance

1. Log in to the Orion Web Console using an account with administrator rights.
2. Click Settings > All Settings, and then click Manage Alert Integration Instances.
3. Click Add Instance and select your instance type.
   - To add a ServiceNow instance, select Service now, and complete the configuration.
   - To add a ServiceDesk instance, select Service Desk, and complete the configuration.

The new instance displays on the Manage Alert Integration Instances page. Check the operational state of the integration. You can now use Create ServiceNow Incident or Create SolarWinds Service Desk incident as an alert action.

Operational states

Once you configure the integration, you can go to Settings > Manage Alert Integrations and view a list of all integrated instances.
Operational states describe how the integration of your alerting system and the Orion Platform works:

- **Enabled**: new or updated alerts in the Orion Web Console create or update incidents in the integrated instance, and the other way around.
- **Restricted**: incidents in the integrated instances are updated and closed. Changes in Orion are reflected in the integrated instance (ServiceNow or SolarWinds Service Desk), and the other way around, but no new incidents are created.
- **Restricted by system**: applies only to ServiceNow. If the number of ServiceNow incidents created in a five-minute period reaches 100, the instance is automatically switched to Restricted state.
- **Disabled**: incidents cannot be created and updated in the integrated instance based on Orion Platform alerts.

**Configure SolarWinds Service Desk to be integrated to the Orion Platform**

1. In the Orion Web Console, click Settings > All Settings, and then click Manage Alert Integration Instances in the Alerts & Reports section.
2. On the Manage Alert Integration Instances page, click Add Instance > Service Desk.
3. Provide a name for your Service Desk instance.
4. Provide the token:
   a. Log in to your Service Desk Instance.
   b. Click the Settings icon in the top left and then click Setup.
   c. Click SolarWinds Interfaces > Orion.
   d. Click + to create a new integration instance, and then click Create in the top right corner. This creates the connection. The connection is in the Awaiting Connection stage because it waits to be registered in your Orion Platform.
e. Click Generate token and then click Copy Token.
f. Ensure that the Enable switch in the top right corner is selected. The green color indicates that the integration is enabled.

5. Go back to your Orion Platform and paste the token into the token field.
6. Ensure that HTTP proxy settings are configured correctly.
7. Click Test Connection to find out whether the SSD instance can be reached from the Orion Platform, and then click Save.

When you save the configuration, you are redirected back to the Manage Alert Integration Instances page. The new integration is displayed in the list. You can now configure alerts to create new Service Desk incidents.

When you check the integration in your Service Desk, you can see that the state of the instance changed to Connected because it has been registered with your Orion Platform.

### Integrate an Orion Platform product with ServiceNow

Integrate your Orion Platform product with ServiceNow® to automatically open new ServiceNow tickets based on critical events defined in your Orion Platform product.

The integration with ServiceNow allows for two-way communication between your Orion Platform product and ServiceNow. By integrating the two systems, you can:

- Automatically create incidents in ServiceNow and assign them to the correct tech or group
- Synchronize the acknowledgment of alerts and tickets in SolarWinds Orion and ServiceNow
Update, close, and reopen tickets
Suppress ticket storms

You can integrate one Orion Platform product with multiple ServiceNow instances.

The integration requires NPM 12.0, SAM 6.3, or any other Orion Platform product running Orion Platform 2016.1 or later.

Before you begin

Before you can configure the integration details in your SolarWinds Orion product, check the prerequisites and configure your ServiceNow instance.

- The communication between the SolarWinds server and the ServiceNow instance uses HTTPS port 443. Open this port for outbound communication.
- For minimum hardware and software requirements, see the administrator guide of your product.
- Download the ServiceNow integration application from the ServiceNow app store.
- Install the integration app and configure your ServiceNow instance for the integration.
- SolarWinds does not integrate with ServiceNow Express or on-prem offerings.

How does the ServiceNow integration with the Orion Platform work?

In ServiceNow®, incidents are created and as the staff are working on them, their status changes according to the stage they are in.

When you integrate ServiceNow with the Orion Platform, the actions that happen to the alert are reflected in ServiceNow. The same is true the other way round - if you work on an incident in ServiceNow, the changes must be reflected in the alert in the Orion Platform.

States in the Orion Platform vs ServiceNow states

In the Orion Platform, you specify the states when configuring the ServiceNow alert action.

The options for each state depend on the states defined for the state field on the incident table of your ServiceNow instance.

Closing states

Final states defined in ServiceNow. When a ServiceNow incident is in one of these states, the Orion Platform integration will not touch it anymore, the incident cannot be reopened again. When an alert is in a closing state and triggers again, a new ServiceNow incident is created.

New state

When a new ServiceNow incident is created, it is in the state you defined as State in the Incident Detail section when configuring the alert action. When you acknowledge an alert in the Orion Platform, only alerts that are in the new state change to acknowledge state.
Reset state

When an alert is reset in the Orion Platform, the corresponding ServiceNow incident changes into the Reset state.

To enable Orion alerts to reopen ServiceNow incidents when the trigger condition occurs again, specify a reset state.

To keep the ServiceNow incident closed forever and prevent the alert from reopening it, select one of the closing states here.

Reopen state

When an incident is not in a closing state, this is the state it is put in when the alert is re-triggered or when the incident is manually put in the reset state while the alert is still active.

Acknowledge state

When you acknowledge an alert, the ServiceNow incident will enter into this state.

What happens when...

- ... an alert is triggered in the Orion Platform?
- ... an alert is reset in the Orion Platform?
- ... an alert is re-triggered in the Orion Platform?
- ... an alert is acknowledged in the Orion Platform?
- ... an incident state is changed in ServiceNow?
... an alert is triggered in the Orion Platform?

When an alert is first triggered, the Orion Platform creates a new ServiceNow incident according to the settings in the alert action.

<table>
<thead>
<tr>
<th>Incident Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assigned to</strong></td>
</tr>
<tr>
<td><strong>Assignment group</strong></td>
</tr>
<tr>
<td><strong>Impact</strong></td>
</tr>
<tr>
<td><strong>State</strong></td>
</tr>
<tr>
<td><strong>Urgency</strong></td>
</tr>
<tr>
<td><strong>Short description</strong></td>
</tr>
</tbody>
</table>

... an alert is reset in the Orion Platform?

When an alert is reset in the Orion Platform, the ServiceNow incident changes into the reset state.

When the reset state is one of the closing states, the ServiceNow incident state changes, Close notes are added. This incident is closed and cannot be reopened any more.
When the reset state you configured is not a closing state, the Additional comments are added to the ServiceNow incident. When the alert re-triggers, the ServiceNow incident status will change to the reopen state.

When the alert is re-triggered in the Orion Platform?

When an alert is re-triggered, the Orion integration tries to find the corresponding ServiceNow incident. When it is closed, a new ServiceNow incident is created.

When it doesn't have a reset state defined, the incident won't be reopened.

When the ServiceNow incident status is not closed, the incident status changes to the reopen status.

⚠️ When the reopen state is not defined and the reset state is not a closing state or the incident is not closed manually, no more incidents will be created.

... an alert is acknowledged in the Orion Platform?

When the alert is acknowledged in Orion, the associated ServiceNow incident receives a work note. If the incident is untouched (in the new state), it will transition to the defined acknowledge state.
... an incident state is changed in ServiceNow?

For example, when a technician takes the ticket in ServiceNow and starts working on it, the alert is acknowledged in Orion.

When the user changes the incident's state to a reset state in ServiceNow and the alert that created this incident is still active in Orion, it will transition to the reopen state.

Install and configure the Orion Platform Alert Integration application in ServiceNow

The SolarWinds Alert Integration application enables the communication between your SolarWinds server and the ServiceNow® instance.

After downloading the SolarWinds Alert Integration application from the ServiceNow store, deploy the application in ServiceNow.

1. Navigate to your downloaded system applications.
2. Locate the SolarWinds Alert Integration application, and click Install.

When the installation is complete, the caption of the Install button will change to Installed.

After the installation is complete, SolarWinds recommends that you create a ServiceNow integration user with Web service access only.

Create a ServiceNow integration user with Web service access only

1. Navigate to the user administration section in ServiceNow, and create a new user.
2. Provide a user ID, a password, and other required information.
3. Specify that the new user should have Web service access only.
4. Edit the newly created user, and add the `x_sow_intapp.integration_user` role to the role list.

After installing the integration application and creating an integration user, you can now configure the integration with ServiceNow in your SolarWinds Orion server.

Configure an Orion Platform product with ServiceNow

After completing the configuration of the integration in ServiceNow®, you can configure the integration to be able to automatically create, update, and resolve alerts that were raised in your Orion Platform product in your ServiceNow instance.

1. In the Orion Web Console, click Settings > All Settings.
2. In the Alerts & Reports group, click ServiceNow Instances.
3. Click Add Instance.
4. Enter a name and the URL for the ServiceNow instance.
5. Enter the ServiceNow credentials:
   - Username
     The user name of the account that is configured for the SolarWinds integration role.
   - Password

6. Test the connection to your ServiceNow instance. If the connection is not working, you receive descriptive messages to help you solve the issue.

7. If you are accessing your ServiceNow instance through a HTTP proxy, select Use a HTTP proxy server, and click the Configure your HTTP proxy settings link to edit the details. For more information, see Configure web proxy settings in the Orion Platform.

8. Click Save.

Enable/disable or restrict your ServiceNow instance

You can influence the behavior of the integration using the Operational State of your ServiceNow instance in the Orion Platform.

1. Click Settings > All Settings, and then click Manage ServiceNow instances.

2. Select the instance to change, click Set the Operational State, and select a status:
   - To make the integration between ServiceNow and the Orion Platform work (to make sure triggering the alert creates a ServiceNow incident and that the instance status in ServiceNow corresponds with the alert in the Orion Platform, select Enabled.
   - To turn off the integration, select Disabled.
   - To prevent the Orion Platform from creating new incidents, but to update and close existing ServiceNow incidents both in ServiceNow and the Orion Platform, select Restricted.

   **Restricted by system**
   To prevent flooding your ServiceNow with new incidents, the Orion Platform automatically restricts creating new incidents when the integration creates more than 100 new incidents within five minutes. In this case, the status of your ServiceNow instance is Restricted by system.

Troubleshoot ServiceNow

This topic provides frequently asked questions about the ServiceNow® integration.

**Why are my incidents reopening right after I resolve them?**

When you change an incident's state to the reset state manually and the alert that created this incident is still active, the incident transitions to the reopen state.

To forcefully close the incident, put it in one of the closing states.

**Why are closed incidents reopening instead of creating a new incident?**

Make sure the final closed state is one of the closing states.

If you never want to reopen an incident, set the reset state to a closing state.
Why are my incidents reopening after I changed the closing states?

This is a known issue. When you add a state to the group of closing states, the change is not reflected on incidents already closed according to the original definition of closing states.

If an incident was closed and the state it was in was not originally among the closed states, the incident gets reopened when the alert triggers again. After that (when its state is among closed states), the incident will not reopen any more.

You can also resolve this by updating the mapping in the database. Contact support for the script to run.

Why are my incidents not being reopened and only receive work notes?

Make sure you define the reset state, which is used to show that an incident is resolved. Only incidents in the reset state get reopened. This is to stop the incident from transitioning to the reopen state on any incident update.

Why does my incident not change state when I acknowledge its associated alert?

When you acknowledge the alert, the incident only changes to the defined acknowledge state when the incident has not been touched yet. This means that the incident is in the state defined in incident detail of the alert action.

Why is an object still reopening my tickets when it is no longer monitored (deleted on SolarWinds side)?

When you delete a monitored object, its related objects (triggered alerts, interfaces...) are deleted. If an alert is in the triggered state at the time of deletion, the incident stays in the triggered state with no way to reset.

The incident will be cleaned up during nightly database maintenance.

To resolve the issue immediately, run the maintenance.

I want the integration to only create incidents and leave them alone afterwards. How do I do this?

If you do not define any states in the Create ServiceNow Incident alert action, the incident will be created and receive notes when actions happen in the Orion Platform, but its state will not be changed.

However, there will only be one incident at a time. Only when it is closed would a triggered alert create a new one.

Configure web proxy settings in the Orion Platform

If your SolarWinds Orion server does not have Internet access, you can use a proxy server to allow the Orion server to connect to certain pages and websites. Use a proxy server to:

- Access the THWACK community
- Access the product blog
- Check for maintenance updates
• Access an alerting instance you integrated with your SolarWinds Orion server. See Alert Integrations in the Orion Platform.

To configure web proxy settings:

1. In the Orion Web Console, click Settings > All Settings > Product specific settings > Proxy Settings.
2. Select Use the following settings, and specify the IP address and port number of the proxy server.
3. If the proxy server requires authentication, select the check box, and specify the user name and password.
4. Enter a URL, and click Test connection to verify that you can reach the destination address through the proxy.
5. Click Save.
Troubleshooting environmental issues with Performance Analysis dashboards

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

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

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

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

Compatible SolarWinds products

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

Correlate data from the following SolarWinds products:

- NPM 12.1 or later
- SAM 6.4 or later
If you have at least one of these products installed together on the same server, you can access Performance Analysis dashboards. However, you may not be able to use all collected metrics if you pull data from older product versions.

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

- NetPath™

For a more complete list, see SolarWinds KB MT85165.

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

Create analysis projects

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

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

1. Click My Dashboards > Home > Performance Analysis.

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

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

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

Create analysis projects from the entity details page

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

1. Open the details page to an entity.

2. Click Performance Analyzer on the Management widget.

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

- Average CPU Load
- Average Percent Memory Used
- Average Response Time
- Alerts
- Events
- Status
Update charts in real-time (Real-Time Polling)

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

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

Click Start Real-Time Polling in the toolbar.

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

During an analysis, you can apply a transformation algorithm to any currently charted metric. Transformation algorithms can make it easier to correlate data and to find trends, anomalous values, or other patterns. Using transformation algorithms can help you understand your data more quickly and efficiently.

Enable a Display Transform algorithm:

1. Hover your mouse over a currently charted metric, displayed on the right side of the screen.

2. Click the revealed menu button to see the available transformation algorithms.

3. Click an algorithm to enable it.

When you enable an algorithm, the metric's chart immediately updates and reflects the transformed data. If needed, the chart's scale automatically adjusts to fit the transformed data.

In the dropdown menu, the active transformation algorithm is highlighted. Click an active algorithm to disable it, select a different algorithm to use it instead, or select None to disable Display Transform for the current metric. You can have one algorithm active for each charted metric.
**Display Transform algorithms**

You can apply any one of the following algorithms to a charted metric:

**Change Point** - useful for finding significant changes in the numerical average of a set of data over time. When the numerical average for a time series changes significantly, the charted line will move up or down to the new numerical average, indicating that there has been a notable statistical change in the numerical average of the data.

**Difference** - Shows the relative positive or negative difference between a data point and the point immediately following it. The largest differences indicate significant changes in data during the scope of the charted timeframe. If the metric being transformed is a percentage, then the absolute difference (which is always positive) is shown.

**Linear Regression** - Shows the overall linear trend of the charted data. The slope of the linear trend indicates the overall trend of the data in the charted timeframe. Linear Regression is useful for showing if a noisy set of data is trending up, trending down, or remaining constant.

**Normalized** - Compresses a charted timeframe by representing each data point as a value between 0 and 100, relative to each other data point in the set. 100 represents the highest data point, and 0 represents the lowest data point. Normalized data is useful for comparing metrics of different scales: since each normalized metric shows all data in a common scale of 0 to 100, the data becomes easier to compare.

**Percentile Standardized** - takes the data and calculates the median value and the median absolute deviation of the data set and calculates where each data point is relative to the median and median absolute deviation. The resulting range of data is indicative of anomalies from a percentile stand point. This can be useful because a mean value is often skewed by extreme outliers whereas percentiles are resilient to outliers in a large enough data set. If the metric being standardized is already a percentage, then the data will also be normalized in addition to being standardized.

**Smoothing** - Takes a moving average of the data so that odd spikes in the data are averaged out, leaving only the overall pattern of data. Smoothing is useful for finding patterns in data that has a lot of spikes.

**Smoothing and Standardized** - Combines the smoothing and standardized algorithms. Useful for finding cause and effect patterns. If the metric being standardized is a percentage, then the data will also be normalized in addition to being standardized.
**Standardized** - Useful for quantifying how anomalous a value is relative to the rest of the data in the charted timeframe. Viewing multiple timeframes of data in standardized format can help you see patterns where anomalous values or trends happen. Values between -3 and 3 are expected whereas values less than -3 or greater than 3 can be considered anomalous. If the metric being standardized is a percentage, then the data will also be normalized in addition to being standardized.

**View the polled data for a plotted metric**

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

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

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

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

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

View more information for an entity

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

Share analysis projects

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

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

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

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

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

Add saved analysis projects to views as a widget

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

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

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

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

Cannot find your project in Available Widgets?

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

Delete analysis projects

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

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

Add a Performance Analysis Project to the menu

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

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

The menu has a link to the Performance Analysis project.

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

Troubleshooting Analysis Projects

I do not see all the data I expect

- The collected data depends on the products you install and how they are configured. For example, you cannot display storage I/O data without installing and configuring SRM.
- You may not have access to the data. The data displayed depends on your account limitations.
- The entities may not have data during the time period you view. For example, a node under maintenance does not have data during that time frame because the node is not polled.
- You may be examining a time before the node was added.
- The data may not exist in the database.

I do not see key entities

The Performance Analysis dashboard respects account limitations. If your account is restricted from viewing certain entities or nodes, you cannot view the data in the Performance Analysis dashboard.

Not all metrics I add are charted or data does not display correctly after I add more metrics

This is usually due to browser limitations. Changes to the Performance Analysis dashboards are reflected in the URL. If you have a large amount of data, the URL may exceed the character limit for URLs in your particular browser.

Save the troubleshooting project to compress the URL and continue to edit it.

Some entities do not have metrics

Metrics without data do not display in the metric palette.

Some metrics do not line up or change when I expand or contract the time frame

We use up to 240 data points to create the charts. On larger time frames, the data can be slightly distorted due to how many data points are used to create the chart. Additionally, data points are averaged and become more granular as you contract the time frame.
The charts include different information when I share them

The person looking at the shared chart may have account limitations applied or have different account limitations.

Real-Time Polling does not work

The node may be down, or the underlying polling method, such as SNMP, may be unresponsive.
Use alerts to monitor your environment with the Orion Platform

An alert is an automated notification that a network event has occurred, such as a server becoming unresponsive. The network event that triggers an alert is determined by conditions you set up when you configure your alert. You can schedule alerts to monitor your network during a specific time period, and create alerts that notify different people based on how long the alert has been triggered.

The types of events for which you can create alerts vary, depending on the Orion Platform products you have installed. For example, you can create an alert to notify you if a node in a specific location goes down or if the network response time is too slow when you have NPM. If you have installed SAM, you can receive alerts about application response times or when your Exchange mailbox database is almost full.

You can create alerts for any monitored object. You can alert against volumes and nodes with most Orion Platform products.

Use the following topics to get started if you have never used Orion Platform products:

- Alert preconfiguration tasks in the Orion Platform
- Best practices and tips for alerting in the Orion Platform
- Navigate to the Alert Manager in the Orion Platform
- Create new alerts to monitor your environment with the Orion Platform
- Alert me when a server goes down in the Orion Platform

You can also view our Alert Lab on THWACK for community-based alert information.

Alert preconfiguration tasks in the Orion Platform

Some alerts require extra configuration, separate software installations, or information that you may need to request from other departments.

Alert actions that require set up before creating or configuring alerts include:

- Send an email or page in the Orion Platform
- Dial a paging or SMS service in the Orion Platform
- Play a sound when an alert is triggered in the Orion Platform
- Send an SNMP trap in the Orion Platform
- Use the speech synthesizer to read alerts in the Orion Platform

Monitored objects in the SolarWinds Orion database must exist before creating or configuring alerts. Monitored objects can include items such as nodes, databases, and applications.
Configure the default information in the email action for Orion Platform alerts

The information you provide in the default email action is used to populate the Send an Email/Page action. You can still customize individual email actions if you configure the default email action.

- Separate email addresses with a semicolon.
- All email actions require a designated SMTP server.

1. Click Settings > All Settings in the menu bar.
2. Click Configure Default Send Email Action.
3. Under the Default Recipients heading, provide the email addresses of all default recipients for any email alert action, like the following:
   email@company.com; email2@company.com; distrolist@company.com
4. Provide the default sender and reply address.
5. Enter the default SMTP server information.

   Selecting SSL encryption automatically changes the SMTP port number to 465.

Best practices and tips for alerting in the Orion Platform

Use these best practices and tips to help you configure and test your alerts.

Use the out-of-the-box alerts as templates

SolarWinds recommends using the alerts that are included when you install the product as templates for your new alerts.

Find an alert that is similar to one you want to create and then click Duplicate & Edit in the menu bar. Fields are pre-populated so you can skip to specific parts of the Alert Wizard where there is data you want to change.

Enable out-of-the-box alerts

If there are out-of-the-box alerts that match your monitoring needs, enable them in your environment. You can customize the alert actions for those alerts. If you want to modify the conditions, use the alert as a template.

Restrict who receives alerts

During your initial evaluation and testing, send alerts to a few people instead of to a large distribution list. This can prevent overloading your email server while you fine-tune your alerts.

Plan which devices to monitor

To reduce the number of alerts sent out, consider which devices are most important. For example, you may want to receive alerts only for mission-critical interfaces instead of every interface on a device.
Establish dependencies

Establish dependencies to prevent you from receiving duplicate alerts that stem from a single network event. For example, you may want to be emailed if servers in your server farm go down, but if the router goes down and the servers can no longer be polled, you do not want to receive notifications for all of your servers.

Navigate to the Alert Manager in the Orion Platform

Use the Alert Manager to create, edit, delete, enable, or disable alerts. You can access the Alert Manager in one of three ways:

- Settings Page (Recommended)
  - Click Settings > All Settings in the menu bar. Under Alerts & Reports, click Manage Alerts.
- Active Alerts Details
  - From the Active Alerts Details page, click Manage Alerts in the Management resource.
- Node Details
  - On the Node Details page, navigate to the All Alerts this Object can trigger resource, and then click Manage Alerts.

Add an SMTP server in the Orion Platform

You must add and configure a designated SMTP server if you want to complete an email action with any SolarWinds Orion Platform product.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Alerts & Reports grouping, click Manage SMTP Servers.
4. Click Add SMTP Server.
5. Provide the Hostname or IP Address of your SMTP Server and the designated SMTP Port Number.

   The SMTP server hostname or IP address field is required. You cannot send an email without identifying the SMTP server.

6. If you want to use SSL encryption for your alert email, select Use SSL.

   Opting to use SSL automatically changes the SMTP port number to 465.

7. If your SMTP server requires authentication, select This SMTP Server requires Authentication, and provide requested credentials.
8. Click Save.
Create new alerts to monitor your environment with the Orion Platform

Navigate to the Alert Manager in the Orion Platform to create a completely new alert definition, or duplicate an alert that is similar to the alert you want to create.

1. Enter the alert properties, which includes who can view the alert, severity, and how frequently the alert conditions are evaluated.
2. Define the conditions must exist to trigger the alert.
3. Define what event occurs to reset the alert.
4. Schedule when you want the alert to monitor your environment.
5. Define what happens when an alert is triggered.
6. Define what happens when the alert is reset.
7. Review your alert, including the number of alerts that will be triggered based on the conditions you defined.

You can skip to different steps if you clicked Duplicate & Edit or if you are editing a saved alert.

Once you have created an alert, it is added to the list of available alerts in the Alert Manager. When the alert is enabled, it immediately monitors your environment for the conditions necessary to trigger it.

Set alert properties in the Orion Platform

After creating a new alert, use the Alert Properties to describe the alert, including which users can view the alert.

Name of alert definition

This is a required field. The name is displayed in the Alert Manager and can be used to sort your alerts. If you intend to create a large number of alerts, consider a naming convention that allows you to quickly scan through them.

SolarWinds recommends a name that describes the condition and most visible alert action. For example, you can use "Email NetAdmins when router goes down" as the name of an alert.

Description of alert definition

Describe the alert. This is displayed on the Manage Alerts page, so important information should be near the front.

Enabled (On/Off)

Choose to evaluate the alert immediately after it is created and saved. The alert is enabled. If you are in the process of refining your alert, you may want to disable this alert until it is ready for use.
Evaluation Frequency

Set how frequently you want to evaluate the conditions. If you choose to alert on an event, such as a changed IP address, the condition is not evaluated by frequency, but by when the change is reported based on the polling interval.

SolarWinds recommends using intervals longer than one minute to evaluate alert conditions. Shorter frequencies can negatively impact your network performance or computing resources.

Severity of Alert

Control how the alert in the Active Alerts resource looks, and use the severity to group or filter alerts more easily.

Alert Custom Properties

Use custom properties to organize your alerts. For example, you can create a "Responsible Team" custom property and use it to help audit who receives specific alerts.

You must create a custom property for alerts before you can use it in an alert.

Alert Limitation Category

Restrict who can view the alerts. For example, managed service providers can restrict alerts to their specific customers. Create a new alert limitation by editing or creating a user account.

Define the conditions that must exist to trigger an alert in the Orion Platform

The trigger condition is the most complex step in creating an alert. Before you begin, you may want to revisit the Best practices and tips for alerting in the Orion Platform. To see an example of completed trigger conditions, see the Alert me when a server goes down in the Orion Platform topic.
Trigger conditions are built using child conditions that are evaluated in order. Child conditions are represented as a line item under the Actual Trigger Condition. You can have multiple trigger condition blocks with multiple child conditions.

Filter your environment to only display the objects you want to monitor in The scope of alert. Use the Show List link to view all of the objects that the alert monitors.

1. Choose what objects you want to monitor in the I want to alert on field.
2. Establish how much of your environment you want to monitor in The scope of alert.

You can monitor all objects in your environment or filter your environment to a specific set of objects.

3. Create your trigger condition.

a. Choose if the child conditions must be true or false to trigger the alert.
   - All child conditions must be satisfied (AND) - Every child condition must be met
   - At least one child condition must be satisfied (OR) - At least one child condition must be true
   - All child conditions must NOT be satisfied - Every child condition must be false
   - At least one child condition must NOT be satisfied - At least one child condition must be false

b. Click the + sign to add child conditions.
   - Add Single Value Comparison (Recommended) - The child condition evaluates a single field, like Status
   - Add Double Value Comparison - The child condition evaluates two conditions, such as Status and OS
   - Add And/Or block - Adds a sub condition block

Use the X at the end of each child condition to delete it, or use the drop-down menu at the top of the block to delete the entire condition.

c. Select the object you want the child condition to evaluate, and then select which field you want to evaluate. In the example screenshot, the object is "Node" and the field is "Status".

You can evaluate objects based on variables or macros.
d. Select how you want to compare the polled value of the field to the value entered here, and then enter the value. In the example screenshot, the comparison is "is equal to" and the value is "Down".

e. To use more complex conditions, such as evaluating when an application on a specific server is down and a different application on another server is down, enable complex conditions under Advanced options. See Building Complex Conditions for more information, or visit THWACK, SolarWinds' community website, for support from other users.

f. Choose how long the condition must exist before an alert is triggered. This prevents receiving alerts when the alert condition, such as high CPU utilization, occurs briefly or only once during a certain time period.

- Send an alert immediately when the condition is met by clearing any selection for Condition must exist for more than.
- Wait before sending an alert by selecting Condition must exist for more than, and entering how long the condition must exist. This option prevents multiple alerts firing if the condition is temporary.

If you have successfully created an alert condition, you can move to the next step in the alert wizard. The Summary step evaluates the conditions against your environment and returns how many objects will trigger the alert.

Define the conditions that must exist to reset an alert in the Orion Platform

Use the reset condition to define what must occur to remove an alert instance from the active alerts list. For example, the "Email me when a Node goes down" alert automatically resets when the node comes back up. You can use the built-in reset conditions or create your own.

When reset conditions are met, the alert is removed from Active Alerts. You can also add actions that occur when the reset conditions are met.

For example, you can create an alert that triggers when nodes in your lab go down. If node 192.168.4.32 goes down, the alert fires for that specific instance of the trigger condition and any escalation levels you create continue until you reset the alert. After the alert is reset, all trigger actions stop and a new alert fires the next time node 192.168.4.32 goes down. If you have created reset actions, the reset actions fire.

When the alert is reset, escalation actions are halted.

Select one of the following reset conditions:

- **Reset this alert when trigger condition is no longer true (Recommended)**

SolarWinds recommends using this reset condition. If the trigger condition is no longer true when the objects are next polled, this selection automatically resets the alert.
You can use the Condition must exist for more than option in the trigger conditions in conjunction with this reset condition. Trigger conditions that involve volatile components, such as high CPU utilization, can trigger excessively with this reset condition.

- **Reset this alert automatically after**
  Select to reset an alert after a set amount of time has passed. If this interval is less than the amount of time you wait for different escalation levels, the escalation levels that occur after this interval do not fire. This reset condition is especially useful to remove event-based alerts from Active Alerts.

  For example, if the trigger conditions still exists after 48 hours, you can use this to trigger your alert actions again. The alert is reset and triggers as soon as the trigger condition is detected, which is as soon as the objects are polled for this example.

- **No reset condition - Trigger this alert each time the trigger condition is met**
  The alert fires each time the trigger conditions are met.

  For example, when the alert for node 192.168.4.32 going down fires, a new alert for 192.168.4.32 fires every time the node is down when it is polled.

- **No reset action**
  The alert is active and is never reset. To re-trigger the alert, the alert must be manually cleared from the Active Alerts view.

- **Create a special reset condition for this alert**
  Select to build a specific reset condition. For example, you can choose to reset the condition when the node has been up for more than 10 minutes.

  The alert wizard evaluates the reset condition for errors. If there are no errors, you can proceed to the next step, or go back to previous steps.

  See Define the conditions that must exist to trigger an alert in the Orion Platform or Build complex conditions in the Orion Platform for more information on creating conditions.

### Schedule when an alert monitors your environment

You can configure when an alert monitors your environment. By default, alerts monitor your network for changes all the time. Schedule when you want to monitor your network for the trigger conditions you created for the alert.

You can create multiple schedules that control when an alert is enabled or disabled. For example, you can schedule the alert to monitor your network during off hours, and disable the alert during your maintenance windows.

> Alerts must be enabled to allow schedules to run.

1. **Select Specify time of day schedule for this alert.**
2. **Click Add Schedule.**
3. Enter the following information:

- **Schedule Name**
  This is not required, but may help you organize or troubleshoot your schedules. If you do not enter a name, a name is automatically generated from the time period.

- **Enable or Disable alert during following time period**
  If you choose to disable the alert, it is enabled all other times unless otherwise scheduled.

- **Frequency**
  Choose when to monitor on a high level, such as daily, weekly, or monthly.

- **Enable or Disable every**
  These options change based on the frequency.
  - If you selected Daily:
    You can choose to enable or disable the alert every few days, up to every 31 days. You can also select business days. For example, you may want to disable network or disk activity alerts if you run daily, off-site backups of your critical data.
  - If you selected Weekly:
    Choose which days the alert is enabled or disabled. You may want to disable alerts during a weekly maintenance window.
  - If you selected Monthly:
    Choose which months the alert is enabled or disabled. This option is useful when you have quarterly or monthly maintenance windows.
    Choose either a specific date, such as June 22nd, or a day, such as Thursday.

- **Starting on**
  Choose when to begin the schedule.
  - Right now - Start the schedule immediately.
  - Specific Date - Select a time and day to begin the schedule.

- **Ending on**
  Choose an end date for the schedule, if necessary.

4. Click Add Schedule to create the schedule.

When you add a schedule to an alert, the alert only monitors during the time period you have scheduled, or does not monitor during that time. Alert actions can also have schedules, so not all alert actions may occur during the scheduled period.

**Define what happens when an alert is triggered in the Orion Platform**

Choose actions that occur whenever the trigger conditions are met. You can also set up escalations levels so that different actions occur if the alert has not been acknowledged quickly enough.
Add actions to alerts

By default, what you enter into the Message displayed when this alert field is displayed in the All Active Alerts resource.

You can create a new action or use an action that you have already created. When you reuse an action, you are also reusing all of its configurations, including its schedule and execution settings.

If you are alerting others through email, SolarWinds recommends that you notify a small number of users while you fine tune your alerts.

1. Click Add Action.
2. Select an action from the list.
   
   See Alert Actions for a complete list of available actions.
3. Click Configure Action.
4. Enter the necessary information for the action.
   
   Each action requires different information. Select from the list of Alert Trigger Actions for more information per action.

   Some actions require extra configuration steps, specific information, or special software. See Alert preconfiguration tasks in the Orion Platform.

   Each action has the following sections:

   - Name of action - This is not required, but makes it easier to organize and find your actions in the Action Manager.
   - Time of Day - You can choose different actions to occur at different times of the day or month. For example, if you want to send a page, you might send it to a different person on weekends or holidays rather than during the week.
   - Execution settings - You can select both options, neither option, or a single option.
     - Do not execute this action if the alert has been acknowledged already (Recommended)
     - Repeat this action every X minutes until the alert is acknowledged

5. Click Add Action to save it to the list of actions in the alert.

Add a preexisting action to the alert

You can add actions that have already been configured to an alert. For example, if you configured an action to reboot a VM, you can add that action to a separate alert.

If you use a preexisting action, any configuration change you make to the action, including schedules, is used in every alert the action is assigned.

1. Click Assign Action(s).
2. Select one or more actions from the list.
3. Click Assign.
Add what happens when an alert is not acknowledged

Escalation levels in Orion Platform products refer to user-defined time intervals between when an alert is activated and when a user acknowledges that alert. You can configure the alert to perform different actions per escalation level.

Escalation Level 1 contains all initial actions that you want to occur when the trigger conditions are met and the alert activates.

Escalation Levels 2 and above include all actions you want to occur if no one acknowledged the alert during the previous escalation levels.

For example, if an alert for a critical server activates and all of the recipient or first-level responders are out for training and do not acknowledge the alert, then the actions fire in the second escalation level. These actions may include emailing managers or other backup staff.

1. In an existing alert, click Trigger Actions.
2. Below the action, click Add Escalation Level.
3. Choose how long you want to wait after the previous escalation level before performing the actions in the new escalation level.
4. Enter new actions in this escalation level.

You can copy all of the actions as Reset Actions. This lets you quickly craft actions to indicate that the issue has been acknowledged or resolved. Click Copy Actions to Reset Actions Tab.

When an alert is triggered, the actions will be performed in the order that they are displayed on the list. You can test each action to ensure the action does what you expect it to do.

Define what happens when the alert is reset in the Orion Platform

Use reset actions to perform specific tasks when an alert is no longer active, such as writing to the log that the issue has been acknowledged. Reset actions are usually used to notify others that the situation has been resolved or to write the resolution to a log file.

1. Click Add Action.
2. Select an action from the list.
   
   See Alert Actions for a complete list of available actions.
3. Click Configure Action.
4. Enter the necessary information for the action.
   
   Each action requires different information. Select from the list of Alert Actions for more information per action.
   
   Some actions require extra configuration steps, specific information, or special software. See Preconfiguration Tasks.
Each action has the following sections:

- **Name of action** - This is not required, but can make it easier to organize and find your actions in the Action Manager.
- **Time of Day** - You can choose different actions to occur at different times of the day or month. For example, if you want to send a page, you might send it to a different person on weekends or holidays than during the week.

5. Click Add Action to save it to the list of reset actions in the alert.

To perform the same actions as when the alert was triggered, click Copy Actions From Trigger Actions Tab. Use the copied trigger actions as a base and modify them to reflect that the alert is no longer active.

When an alert is reset, the actions will be performed in the order that they are listed. You can **test** each action to ensure the action does what you expect it to do.

**Review the alert's configuration in the Orion Platform**

The Summary tab allows you to check your alert definition before you save any changes.

Before you click Submit, review the information box above it. This box lists the number of objects that will trigger the alert immediately based on your current trigger condition.

Modify any section by clicking **Edit** next to that section.

You can **integrate your alerts** with other SolarWinds' products, such as AlertCentral or Web Help Desk, by expanding Alert Integration.

Once you have created an alert, it is added to the list of available alerts in the Alert Manager. When the alert is enabled, it immediately monitors your environment for the conditions necessary to trigger it.

**Reduce alerting noise in the Orion Platform**

This section includes techniques for reducing alert noise.
Complex trigger conditions in the Orion Platform

Use the Advanced options in the trigger conditions to create complex conditions, such as alerting when an application is down and when your failover server is active for more than an hour.

Complex conditions are generally enabled by users who are comfortable with building normal trigger conditions, or who have trialed alerts using the normal trigger conditions and require more control over the trigger conditions to better refine the environmental conditions that trigger an alert.

Do not use complex conditions until you have tested the trigger conditions individually. Creating an alert with complex conditions without testing it may prevent you from receiving important alerts.

How condition blocks are evaluated

The condition blocks are evaluated at the same time. If they are all true based on the conditions, the alert triggers. For example, condition A, B, and C must be true in order for the alert to trigger.

(Condition A) & (Condition B) & (Condition C)

Condition blocks are evaluated using variations of AND, so the trigger condition in each section must be met.

A condition block can be evaluated at a different time than other condition blocks. For example, if you want to be alerted if the backup system is active for more than an hour, you can choose to wait an hour after the primary condition block, where the application going down is the trigger condition, before evaluating whether the backup system is still active.

Aggregate alerts

With complex conditions enabled, you can choose to trigger alerts only when multiple objects meet the trigger condition.

After you have enabled complex conditions, the following option is available in your trigger condition:

- Condition must exist for more than [ ] minutes
- Alert can be triggered if [ ] objects (at the same time) have met the specified condition

This setting then combines all alerts that would be sent for each object into a single alert.

Do not use this setting until you are confident that the trigger condition is correct. This setting can prevent important alerts from triggering.
Alerts with multi-element triggers in the Orion Platform

You can use complex conditions to trigger alerts when objects meet separate trigger conditions at the same time. For example, if you have two applications on two separate servers, you can still manage if you lose one application. However, if you lose both applications, you need the system to send a critical alert.

⚠️ Complex conditions should be used with caution. SolarWinds recommends testing each trigger condition individually before combining them.

On the Trigger Conditions panel, expand Advanced options, and select Enable complex conditions.

With a standard alert, you can create an alert for each of the two applications. With a complex condition, you can create a single alert where the application would have to fail on both Server A and Server B in order to generate an alert.

In this example, the primary trigger condition is written for Server A.

![Complex trigger condition diagram](image-url)
Click Add Section and write a trigger condition for Server B.

In this example, both conditions must resolve to TRUE in order for the alert to fire, but do not have to relate to each. The condition blocks are evaluated at the same time. If they are all TRUE based on the conditions, the alert triggers. You can add additional conditions to configure granular and complex alerts.

Using condition blocks is a great way to reduce alerts. Instead of receiving an alert for each element, you can receive a single alert.
Use instance names

In the example above, a specific node name is selected in the condition. This works well if the alert has a very limited scope. Another approach is to use instance names in the condition.

Use duration in the trigger for Orion Platform alerts

Using durations for alerts is a great way to reduce the total number of alerts you receive. There are times when you want an alert to trigger as soon as the condition is detected. Other times, you may only want the alert to trigger when a condition exists for more than a certain amount of time.

For example, the WAN link out of your corporate headquarters might occasionally spike over 80% utilization. However, you only want to be alerted if the link is more than 80% for longer than 10 minutes. Set conditions to receive an alert when the utilization on the WAN link is over 80% for 10 minutes, and you will only receive an alert when there is a sustained spike.
The following example illustrates an alert that includes duration. Ensure that you select the Condition must exist check box and enter a duration.

![Alert Configuration Example]

The 'Do Not Alert' alert in the Orion Platform

You can use custom properties to suppress alerts from being triggered when an object goes down. In this case, include a custom property in the alert condition that stops the alert from being fired.

1. Click Settings > All Settings.
2. In the Node & Group Management group, click Manage Custom Properties.
3. Click Add Custom Property.
4. Create a Boolean (Yes/No) custom property called AlertOnThis.
5. Click Select Nodes.
6. Select all of the nodes on the system.
7. Click the green arrow to move all selected nodes to the right.
8. Set the AlertOnThis property to Yes.

9. For devices for which you do not want to receive an alert, set the custom property to False.
10. Define the alert to trigger when the AlertOnThis custom property is equal to Yes and the Node Status is equal to Down.

If you use the AlertOnThis custom property, every alert must include the AlertOnThis check. Otherwise, all nodes will trigger alerts regardless of how this custom property is set.

Send Orion Platform alerts to specific contacts

When you have people or groups that are responsible for different monitored objects, you might only want them to receive alerts for objects for which they are responsible.

1. Create a custom property called ContactEmail.
2. Enter the email address for each monitored object.
3. Create an alert that sends an email when an object goes down.
4. On the Trigger Action page in the Alert builder wizard, add an Email action. Because you want the recipient of the email to be variable depending on who the ContactEmail is, you need to add a variable to the Recipients section.

The variable ensures that your alert email is only delivered to people who are listed in the ContactEmail custom property.

The To: field does not have an Insert Variable button, so if you have labeled your custom property something other than ContactEmail, open the Message section, click Insert Variable to find the custom property, and cut and paste the variable into the To field.
Alerts with device-specific thresholds in the Orion Platform

You can set different alert thresholds per device, interface, or other monitored element. For example, it is acceptable to you if most of your nodes reach a 90% threshold for CPU load, but you want a few nodes to alert when they reach a 70% threshold. You can set CPU thresholds locally on a node, and then create a generic alert that notifies you when a threshold has been reached.

1. Begin by creating the actual trigger condition with a double value comparison.
   a. Click the plus sign.
   b. Select Add Double Value Comparison.

   The trigger condition fields expand, and you can enter a double value comparison trigger.

2. Include the threshold in the trigger condition.
   An alert will be triggered when the threshold value is reached.

Single alert when multiple devices go down in the Orion Platform

There are situations when multiple devices go down, and instead of getting an alert for each device, you only want to receive one alert that notifies you that something is wrong. A multiple device alert is closely related to a dependency alert, where Orion detects a down status for a network element because an object in front of the network element is down. For example, if a router goes down, Orion detects that all servers behind the router are also down because Orion cannot communicate with the servers. But, the servers behind the router are still physically up, they are just reported as down. In this case, the alerts triggered can be numerous and inaccurate. You can create a dependency between the router and servers so that when the router goes down, only a single alert is triggered.
With a multiple devices go down alert, the devices reported as down are actually down. For example, you monitor the network connections to multiple remote sites. You need an alert that notifies a group that addresses network issues, like when the carrier loses connectivity to several sites simultaneously. Unless you configure the alert to trigger when multiple devices go down, you will receive one alert for each site. The following alert only triggers when more than 10 sites go down at the same time.

Use groups

You can also use groups to alert you when multiple devices go down. In this approach, create a group and assign related devices to it. In this scenario, an alert is only triggered when all devices in the group are down, and not just a subset of devices. Using groups saves you time when configuring alerts, and is also useful when you have load balanced devices and you only care when all the devices are down, not just when some are down.

Event correlation alerts (Y after X) in the Orion Platform

You may have some conditions you want to alert on if Y happens after X. For example, you might want to receive an alert if there is a problem with your failover. In this example, if node A goes down, the alert waits 5 minutes, and then checks that node B is up. If node B is not up, the alert is triggered.

Make sure to select a And then after value, which is located between the alert sections.
Then, in the secondary section, configure the actual trigger condition so that Node Name is equal to Node B and Node Status is equal to Down.

**Commonly created alerts in the Orion Platform**

The following sections walk you through the easiest method to create common alerts and include tips on how to build more complex alerts.

**Alert me when a server goes down in the Orion Platform**

Use the following procedure to create an alert that writes to a log and sends an email when a Windows server goes down.

1. Search for "Email me when a Node goes down" in the Alert Manager.
2. Select the check box next to the alert, and then click Duplicate & Edit.
3. Enter a name for the alert, such as "Notify me when Windows 2008 servers go down".

4. Enable the alert, and then click Trigger Condition or Next.

5. In the scope of alert, select Only following set of objects.

6. Select Node Machine Type is equal to Windows 2008 Server as the child condition.

   You can further refine your scope by entering another AND condition. For example, you can enter Node IP Address starts with 10.10.45 to restrict the scope of the alert to a specific subnet.

7. The actual trigger condition should be Node Status is equal to Down.

   You can further suppress alerts by enabling complex conditions in the Advanced options. This allows you to choose to wait until multiple nodes are down before triggering a single alert.

8. Click Reset Condition. The default action should be to reset the alert when the node is up.

9. Click Trigger Actions, and then click Add Action.

10. Select Log the Alert to a file, and then click Configure Action.

    a. Enter the location of the log. For example, enter C:\ExampleAlertLog.txt in the Alert Log Filename Field.

    b. In the Message text box, type Node \(\text{\$\{N=SwisEntity;M=Caption\}}\) is currently down.

    c. Click Add Action.

11. Click Add Escalation Level, and enter 5 minutes to wait for 5 minutes before escalating to the next level.

12. Click Add Action in Escalation Level 2, and select Send an Email/Page. Click Configure Action.

    a. Enter your email as the recipient.

    b. Add a message.

    You can use variables to customize your message. You can also use a variable that allows you to acknowledge an alert from email \(\text{\$\{N=Alerting;M= AcknowledgeUrl\}}\).

    c. Enter your SMTP server information if you have not already done so.

    You can enter a default SMTP server that is used for all your email in the Configure Default Send Email Action setting.

    d. Go to Execution settings to click Add Action.

13. Click Copy Actions to Reset Actions Tab, and then click Next.
14. Click Edit next to your logging action, and modify your message to Node
   \( \text{\$\{N=SwisEntity;M=Caption\} is back up.} \)

15. Click Edit next to your email action, and modify your message. You can also delete the email if you do
    not want to know if the situation has been resolved.

16. Click Summary to see if any object will trigger the alert, and then click Submit.

Once you have created the alert, it is added to the list of available alerts in the Alert Manager. You can test
and view the results of each of your alert actions. See Testing Alerts for more information.

**Alert on custom properties in the Orion Platform**

The following example creates multiple alerts using the NodeLocation custom property. An alert triggers
when a node goes down. Upon triggering, the alert will write to a local log file, send a syslog message, and
send an SNMP trap.

The \( \{\text{variable}\} \) syntax is required for variables.

1. Click Alerts & Activity > Alerts in the menu bar, and then click Manage Alerts.

2. Select the check box next to Node is down, and then click the Duplicate & Edit button.

3. Click Trigger Condition, and add a child condition. A child condition should already exist for a node
   being down.

4. Select the node object, and choose NodeLocation in the field drop-down menu. Enter a comparison
   and value.

5. Click the Trigger Actions, and then click Add Action.

6. Select Log the Alert to a file, and then click Configure Action.
   a. Enter the log filename in the Alert Log Filename field.
   b. In the Message text box, type the following:
      \( \text{Node \$\{N=SwisEntity;M=Caption\} is currently down.} \)
   c. Click Add Action.

7. Click Add Action, and select Send a Syslog Message. Click Configure Action.
   a. Type 127.0.0.1 as the Hostname or IP Address of the Syslog Server, and then type the
      following in the Message field:
      \( \text{Node \$\{N=SwisEntity;M=Caption\} is currently down.} \)
   b. Click Add Action.

8. Click Add Action, and select Send SNMP Trap. Click Configure Action.
   a. Type 127.0.0.1 as the SNMP Trap Destination, and then type the following in the Alert
      Message field:
      \( \text{Node \$\{N=SwisEntity;M=Caption\} is currently down.} \)
   b. Click Next.
   c. Click Add Action.

9. Click Summary to see if any objects will trigger the alert, and click Submit.
After you have created the alert, it is added to the list of available alerts in the Alert Manager. You can test and view the results of each of your alert actions.

- You can view results of your Syslog message action in the Web Console or through the Syslog Viewer on your Orion server.
- To view the results of your SNMP Trap action, click Start > All Programs > SolarWinds Orion > Trap Viewer.

**View triggered Orion Platform alerts in the Orion Web Console**

View active triggered alerts through Alerts & Activity > Alerts in the menu bar. Click each alert to view the details, which includes a historic count of how frequently the object triggers the alert and other objects that are experiencing the same set of conditions that triggered the alert you are viewing.

You can also add the All Active Alerts widget to any view.

**Remove alerts from the Active Alerts list in the Orion Platform**

When an alert has triggered and becomes active, you can then acknowledge it. After an alert is acknowledged, alert actions in higher escalation levels are halted and the time it was acknowledged and the account that acknowledged it is recorded. You can also add notes that other users can read.

Depending on your organization, acknowledging an alert can have different purposes outside of halting further notifications. The most common purposes are to provide an audit trail or to prevent multiple people from working on the same issue.

> You must enable the Allow Account to Clear Events privilege to acknowledge alerts. For more information about access privileges for Orion Web Console users, see Define what users can access and do in the Orion Platform.

1. Click Alerts & Activity > Alerts in the menu bar.
2. Click Acknowledge next to the alerts you want to acknowledge.

> Depending on how you configure the email, you can acknowledge an alert directly from an email notification.

You can hide acknowledged alerts by clicking More, and then selecting Hide Acknowledged Alerts.

**Test alert triggers and actions in the Orion Platform**

You do not have to actually experience a device failure to confirm that your alerts are working. The trigger condition is automatically evaluated and trigger and reset actions can be tested individually.
Test trigger conditions

Alert conditions are automatically evaluated on the Summary tab. Scroll to the bottom of the page and view the information box above the Submit button.

Test alert actions while creating or editing an alert

When you simulate actions, the action will be performed regardless of whether the trigger condition is true. If the action sends a message to a recipient, you should reduce the recipient list to yourself and a small number of team members until you are confident the alert is ready to be enabled in your production environment.

1. Click Trigger Actions or Reset Actions.
2. Click Simulate next to the alert action you want to test.
3. Select an object to resolve any variables you have used in your alert action.
4. Click Execute. Test email, play a sound, and text to speech actions without sending an email by clicking Simulate.

Test alert actions in the Action Manager

You can also test actions independent of the trigger or reset conditions by using the Action Manager.

1. Select the action you want to test.
2. Click Test.
3. Select an object to resolve any variables you have used in your alert action.
4. Click Execute. Test email actions without sending an email by clicking Simulate.

After the alert test completes, you can view the results of your alert actions.

- To view the results of your email alert action, open EvaluationAlertLog in your Orion folder, typically <Volume:\ProgramData\Solarwinds \Logs\Orion\ActionsExecution.log.
- To view results of your Syslog message action, click Start > All Programs > SolarWinds Orion > Syslog Viewer.
- To view the results of your Syslog message action, click Start > All Programs > SolarWinds Orion > Trap Viewer.

Modify multiple alerts or share alerts in the Orion Platform

Use the Alert Manager to bulk edit multiple alerts. You can enable or disable multiple alerts or add pre-configured actions.
Alerts must be enabled to be executed. For example, if an alert is scheduled to run for a short period of time each year, it must be enabled so the schedule runs. A disabled alert will **not** be executed, even if it is scheduled to run.

- **Create alerts**
- **Edit alerts**
- Duplicate and edit alerts: Select an alert, click Duplicate & Edit, and **edit the copy of the alert** you have created.
- Enable/disable alerts: Select an alert, and click Enable/disable.
- **Assign actions to alerts**
- **Export/Import alerts**
- Delete alerts: Select the alert and click Delete.

**Edit alerts**

Select an alert and click Edit. You can edit the alert definition:

- **Alert properties**
- **Trigger conditions**
- **Trigger actions**
- **Alert schedule**
- **Reset conditions**
- **Reset actions**

**Add actions to alerts without opening the Alert Wizard**

Assign actions that you have already configured to alerts. You can assign multiple actions to multiple alerts. Actions are categorized into trigger and reset actions based on how the action was created in the Alert Wizard.

SolarWinds does not provide generic actions due to the differences in intent behind trigger and reset actions. For example, a trigger action to send an email is usually a notification that an event happened, while the associated reset action is usually a notification that the event has been resolved.

**Share alerts with others (export and import alerts)**

SolarWinds customers share their customized alerts in the SolarWinds THWACK community. Visit [THWACK.solarwinds.com](http://THWACK.solarwinds.com) to download and import alerts created by others.

Export an alert to save the alert definition as an XML file on your local computer. Alerts are exported to XML and can only be imported from XML. You can send this file to other coworkers or share it in the SolarWinds THWACK community.

⚠️ **Before you share an alert, check the exported file for confidential information, such as SMTP server credentials. Delete this information or password-protect the sensitive information** in the alert before making it public. Also review your company policy on sharing this type of file.
Password-protect sensitive data when exporting and importing alerts

Starting with Orion Platform 2019.2, you can secure sensitive data in alerts with a password or remove the sensitive data when exporting the alert.

Sensitive data might include:

- SMTP credentials used when sending emails
- SNMP Community strings used in the Send a SNMP trap action

To protect sensitive data in an alert to be exported:

1. On Alert Manager, select the alert to export.
2. Click Export/Import > Export.
3. Decide whether to strip the sensitive data or protect it with a password.
4. If you decide to password-protect the data, provide a password and complete the export.

The alert is downloaded to your default download location.

When importing the alert, you can either import the alert without the sensitive data, or provide the password to include the sensitive data.

1. On Alert Manager, click Export/Import > Import.
2. Navigate to the location of the alert.
3. Provide the password or select not to import sensitive data.
4. Complete the import.

Build complex conditions in the Orion Platform

Complex conditions are generally enabled by users who are comfortable with building normal trigger conditions, or who have trialed alerts using the normal trigger conditions and require more control over the trigger conditions to better refine the environmental conditions that trigger an alert.

Do not use complex conditions until you have tested the trigger conditions individually. Creating an alert with complex conditions without testing it may prevent you from receiving important alerts.

1. Navigate to the Trigger Condition page.
2. Expand Advanced options.
3. Select Enable complex conditions.

You can use complex conditions to do the following:

- Wait for multiple objects to meet the trigger condition before alerting
- Evaluate multiple condition blocks
- Evaluate multiple object types
How conditions are evaluated in the Orion Platform

Conditions are a set of user-defined rules governing alert triggers and resets.

**All child conditions must be satisfied (AND)**

Every child condition in the group must be true before the alert is triggered.

In the following example, there are three child conditions.

- Node Status is equal to Up
- Percent Loss is greater than or equal to 75
- CPU Load is greater than or equal to 85

This alert will not trigger unless the Node is Up, packet loss is greater than or equal to 75%, and CPU load is greater than or equal to 85%.

You can also think of the condition as:

Alert when: (Node Status = Up) AND (Percent Loss >= 75) AND (CPU Load >= 85)

**At least one child condition must be satisfied (OR)**

At least one child condition must be true before the alert is triggered.

In this example the alert trigger reads:

Alert when: (Node Status = Up) OR (Percent Loss >= 75) OR (CPU Load >= 85)

In this situation, if any of the three conditions become true, the alert will trigger.

**All child conditions must NOT be satisfied**

Every child condition must be false before the alert is triggered.

In this example the alert trigger reads:

Do not alert when: (Node Status = Down) AND (Percent Loss <= 75) AND (CPU Load <= 85)

Alternatively, you can think of the trigger as:

Alert when: (Node Status != Down) AND (Percent Loss > 75) AND (CPU Load > 85)

The conditions have been inverted (Node Status = Down instead of Node Status = Up).

**At least one child condition must NOT be satisfied**

Any child condition must be false before the alert is triggered.

In this example the alert trigger reads:

Do not alert when: (Node Status = Down) OR (Percent Loss <= 75) OR (CPU Load <= 85)

Alternatively, you can think of the trigger as:
Alert when: (Node Status != Down) OR (Percent Loss > 75) OR (CPU Load > 85)

The conditions have been inverted (Node Status = Down instead of Node Status = Up).

Wait for multiple objects to meet the trigger condition in the Orion Platform

With complex conditions enabled, you can choose to trigger alerts only when multiple objects meet the trigger condition.

After you have enabled complex conditions, the following option is available in your trigger condition:

- Condition must exist for more than [ ] minutes

- Alert can be triggered if [ ] objects (at the same time) have met the specified condition

This setting combines all alerts that would be sent for each object into a single alert.

Do not use this setting until you are confident that the trigger condition is correct. This setting can prevent important alerts from triggering.

For example, if you were monitoring computers used in a high availability cluster, you may only want to be alerted if more than half the cluster is down at the same time.

1. Enable complex conditions.
2. In the trigger condition, select Alert can be triggered if.
3. Enter how many objects must meet the trigger condition before sending an alert.

Evaluate multiple condition blocks in the Orion Platform

You can use complex conditions to evaluate multiple condition blocks, or sections, independently. For example, you may want to create an alert when an application is down and when your fail-over server is active for more than an hour.

1. Enable complex conditions.
2. Click Add Section.
3. Select And then after from the drop-down menu between the two condition sections.

4. Choose how long to wait before evaluating the next section.
5. Create the next condition block.
How condition blocks are evaluated

The condition blocks are evaluated at the same time. If they are all true based on the conditions, the alert triggers. For example, condition A, B, and C must be true in order for the alert to trigger.

(Condition A) & (Condition B) & (Condition C)

Condition blocks are evaluated using variations of AND, so the trigger condition in each section must be met.

A condition block can be evaluated at a different time than other condition blocks. For example, if you want to be alerted if the backup system is active for more than an hour, you can choose to wait an hour after the primary condition block, where the application going down is the trigger condition, before evaluating whether the backup system is still active.

Evaluate multiple object types in the Orion Platform

To evaluate multiple object types, you should use complex conditions. Complex conditions can be used to alert on different object types within the same alert. For example, you can create an alert to notify you when IIS is down and the free space on the volume is less than 30 GB.

1. Enable complex conditions.
2. Click Add Section.
3. Choose a different value in I want to alert on.

Manage alert actions in the Orion Platform

You can edit, test, enable, disable, and delete alert actions from the Action Manager.

Mostly for bulk actions and assigning previously created actions to alerts. View meta data about the action to help troubleshoot alert actions from a single area instead of trying to find the action in an alert.

Edit actions

Edit options depend on the action. See the action in question in the list of available alert actions.

Test actions

1. Select the action, and click Test.
2. Select a node to test it on, and click Execute.

See Test alert actions for more details.
Assign an action to an alert

You can use actions that you have already configured in multiple alerts. For example, if you have configured an action to email emergency response teams, you can assign this action to multiple alerts. When you assign an alert, it is added to the highest escalation level.

Enable and Disable Alerts

Use the On/Off toggle or select an alert and click Enable/Disable to enable or disable alerts.

Alerts must be enabled to be evaluated. For example, if an alert is scheduled to run for a short period of time each year, it must be enabled so the schedule runs. A disabled alert will not be evaluated, even if it is scheduled to run.

Alert actions available in the Orion Platform

Orion Platform products provide a variety of actions to signal an alert condition on your network.

Change a custom property alert action in the Orion Platform

Custom properties are additional fields, such as country, building, asset tag, or serial number, that you can define and store in your SolarWinds Orion database. After properties are added, you can view or filter using them.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Change Custom Property option, and then click Configure Action.
3. Under Custom Property Settings, select the custom property and enter the value you want to change it to.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   - This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the value of the custom property you selected changes.

Create a ServiceNow incident in the Orion Platform

This alert action is only available if the integration with ServiceNow® is enabled.
For information about configuring ServiceNow integration, see [Configure an Orion Platform product with ServiceNow](https://example.com).

⚠️ To use this action, make sure the integration with ServiceNow is enabled on the Alert Summary page. If the Integrate alert with other SolarWinds box is not selected, the incident is created but the integration is not two-sided, so you cannot reset or clear the incidents in ServiceNow®.

**Configure a ServiceNow incident**

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Create ServiceNow Incident, and click Configure Action.
3. Under Select ServiceNow Instance, specify the ServiceNow instance where you want to create the incident.
4. Under Incident Detail, define the properties of an incident template that will be used for new incidents. For example, here you can define the urgency, impact, and other properties of incidents. Text areas can hold macro variables to add information about alerts and alert objects.
   
   If the property you want is not displayed in the Incident Detail section, click Select Properties at the bottom of the section, and select the property from the list. Some properties are reference fields in ServiceNow. See [Use reference fields](https://example.com) and [Filter expression examples](https://example.com) for more details.

5. Under State Management, define how the status of the incident in ServiceNow changes when the alert is reset, reopened, acknowledged, and closed.

   Options in the drop-downs provide states defined in your ServiceNow.
You can also specify notes to be added to the incident.

6. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   ![This is often used to prevent an action from occurring during specific windows.]

7. Select how frequently this action occurs for each triggered alert in Execution Settings.
8. Click Add Action.
The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, an incident will be created or updated in the specified ServiceNow instance.

When you use this alert action, we recommend that you only use it on the trigger tab. It is also recommended that you only use one ServiceNow action per alert.

To deactivate the integrated behavior, remove the alert action from the alert definition.

You can specify one alert action for one ServiceNow instance. To create an incident in another ServiceNow instance, specify another alert action and use a different ServiceNow instance.

Use reference fields

When you configure ServiceNow incidents, you can use reference fields to refer to different database tables in ServiceNow.

The reference value you provide in the Orion Web Console is used in ServiceNow to locate a referenced record. This enables you to use advanced ServiceNow filter expressions.

The reference field’s value is usually the Sys ID of the referenced record, and the application by default tries to locate the referenced record by Sys ID.

You can also specify which fields should be used for specific referenced tables when trying to locate a referenced record. Some definitions are defined by default. For example, setting a field user_name for the sys_user table allows you to use the user name in reference fields such as Caller or Assigned to.

Some default fields are not mapped automatically when you install versions 1.0.2 or 1.0.5 of the SolarWinds Alert Integration application and must be mapped manually. Upgrades from version 1.0.1 and earlier are not affected. This issue is resolved in SolarWinds Alert Integration 1.0.10.

You can specify your own reference fields in the SolarWinds Alert Integration application, under Configuration > Incident Reference Fields Definitions, and you can control the order of different fields on the same table by setting different priorities.

Filter expression examples

Reference fields can also be used as filter expressions. The following examples show the configuration of reference fields.

<table>
<thead>
<tr>
<th>Reference field</th>
<th>Value</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment group</td>
<td>name=Hardware</td>
<td>Assigns the incident to the group called Hardware.</td>
</tr>
<tr>
<td>Location</td>
<td>state=TX^city=Austin^streetLIKESouthwest Parkway</td>
<td>Sets the location to Southwest Parkway, Austin, TX.</td>
</tr>
<tr>
<td>Reference field</td>
<td>Value</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>Configuration item</td>
<td>mac_address=${N=SwisEntity;M=MAC}</td>
<td>Locates the configuration item based on the MAC address of the interface, by using a macro.</td>
</tr>
</tbody>
</table>

For more information, see the [ServiceNow Wiki](https://servicenow.com) about reference fields.

### Create a SolarWinds Service Desk incident in the Orion Platform

This alert management action is only available if the integration with [SolarWinds Service Desk](https://www.solarwinds.com) is enabled. For information about configuring Service Desk integration, see [Configure SolarWinds Service Desk to be integrated to the Orion Platform](https://www.solarwinds.com).

#### Configure a Service Desk incident

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Create SolarWinds Service Desk Incident, and click Configure Action.
3. Under Name of action, provide a name for the alert action.
4. Under Select Service Desk Instance, select a Service Desk instance.

![Configure Action: Create SolarWinds Service Desk Incident](image-url)
5. Add Entity attributes to show in the incident.

6. Review Custom attributes. By default, "Title" and "Description" are used. These attributes correspond with the title and description of incident. The rest of attributes is used by the SSD automation. SSD automation handles incident creation and provides rules for processing the incidents.

7. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

8. Select how frequently this action occurs for each triggered alert in Execution Settings.

9. Click Add Action.

The action is added to the trigger action list, and you can test the action using the Simulate button. When the trigger conditions of the alert are met, an incident will be created or updated in the specified Service Desk instance.

**Recommendations**

- Use the Creating Service Desk Incident action only as a trigger action. If you add this action as a reset action, it will not be executed.

- Use one Service Desk action per alert.
Always specify one alert action for one Service Desk instance. To create an incident in another Service Desk instance, specify another alert action and use a different Service Desk instance.

You can specify one alert action for one Service Desk instance.

**Stop creating Service Desk Incidents for an alert**

To deactivate the integrated behavior, remove the alert action from the alert definition.

When you remove the integration from integration instances, the alert action will be unassigned.

**Dial a paging or SMS service in the Orion Platform**

This action forwards alerts to a paging or SMS service.

To use an email gateway via a wireless provider, select **Send and Email/Page**. When adding email addresses, use the format specified by your provider, such as 9055556543@txt.att.net.

This action requires that you purchase and download PageGate from [Notepage.net](http://Notepage.net). You need to install it on your Orion server and integrate it with the Orion Platform.

For instructions on configuring this action, see the following links, hosted by NotePage, Inc., © 2018, available at www.notepage.net, obtained on July 9, 2018:

- [How to Integrate SolarWinds Orion with PageGate](http://How to Integrate SolarWinds Orion with PageGate)
- [Orion Integration Video Tutorial](http://Orion Integration Video Tutorial)
- [SolarWinds Orion Platform Integration](http://SolarWinds Orion Platform Integration)
- [Text Messaging Video Tutorials](http://Text Messaging Video Tutorials)

**Email a web page to users in the Orion Platform**

Send a web page as a PDF, including content of resources available in the Orion Web Console, to others.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Email a Web Page option, then click Configure Action.
3. Enter the Recipients.
4. Enter the Subject and Message of your alert trigger email/page.
   - For the Optional Web Server Authentication section, select User currently logged in, Another user, or No user defined.
   - You can create a dynamic URL to send information about the object that triggered the alert.
   - Use variables to make the message dynamic.

Multiple addresses must be separated with commas.
5. Enter your SMTP server information.

6. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   This is often used to prevent an action from occurring during specific windows.

7. Select how frequently this action occurs for each triggered alert in Execution Settings.

8. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, an email is sent to the recipients with a PDF generated from the web page.

Create a dynamic URL

Use variables to create a URL that changes based on the object that triggers the alert. Click Insert Variable and search for URL to find the all of the variables you can use to create the dynamic URL.

For example, enter ${N=SwisEntity;M=DetailsUrl} in the URL field to email a link to the Details view of the object that triggered the alert. When the email is sent, the variable resolves to a valid URL such as http://myserver/Orion/View.aspx?NetObject=N:3 and the email contains the content of the Details view in the body.

Execute an external batch file in the Orion Platform

There are several circumstances where you may want to execute a program when a specific network event occurs. For example, you may want to run a custom script to reboot your SQL servers.

External programs selected for this action must be executable using a batch file called from the command line. Programs executed this way run in the background. However, you can set the SolarWinds Alerting Engine Service to Interact with Desktop.

   SolarWinds recommends that scripts and batch files be placed on the root of c:\ to simplify the path for the batch file.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.

2. Select the Execute an External Program option, then click Configure Action.

3. Under Execute an External Program settings:
   a. Enter the Network path to external program in the field provided. For example: Use c:\test.bat, where c:\ is the disk on your main poller and test.bat is your external program to be executed.

   b. Select either Define User or No User Defined for Optional Windows Authentication.

   Enter users as domain\user.

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This
schedule only applies to the alert action you are editing.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the external program runs.

Execute an external Visual Basic script in the Orion Platform

In some situations, you may want to execute a Visual Basic (VB) script when a network event occurs to perform a specific action.

- SolarWinds recommends that scripts and batch files be placed on the root of c:\ to simplify the path for the batch file.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Execute an External VB Script option, then click Configure Action.
3. Under Execute an External VB Script settings:
   a. Select a VB Script Interpreter from the drop down list.
   b. Enter the Network path to the external VB Script in the field provided. For example: Use c:\test.vbs, where c:\ is the disk on your main Orion poller and test.vbs is your external VB Script to be executed.
   c. Select either Define User or No User Defined for Optional Windows Authentication.

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the VB script runs.

How to use scripts with arguments

To use scripts with arguments, your VBScript must be able to read parameters.
Script example

```wscript
If (Wscript.Arguments.Count < 2) Then
Wscript.Quit
End If
parameter1 = Wscript.Arguments(0)
parameter2 = Wscript.Arguments(1)
```

Then, you can enter script with parameters (such as alert variables) into the path to script.

```wscript
C:\vbscript.vbs
"{N=Alerting;M=AlertName}"
"{N=Alerting;M=AlertTriggerTime;F=DateTime}"
```

Path example:

```wscript
C:\vbscript.vbs "{N=Alerting;M=AlertName}"
"{N=Alerting;M=AlertTriggerTime;F=DateTime}"
```

See the thwack post on how to [remanage nodes using a VB script when an alert is triggered](https://www.thwack.com/social/thread/5437913?thread_id=9432853).

**Failover to a standby server in the Orion Platform**

Use this alert action in conjunction with SolarWinds High Availability. You can use alerts to refine your monitoring and force a failover when specific conditions exist.

For example, if you want to force a failover to your secondary server when the primary server's CPU load is more than 85% for more than 20 minutes, create an alert that monitors the primary server and choose the Failover Action in the trigger action. You can then use the Failover Action as the reset action to set the primary server as active server.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.

An HA pool must be set up to configure this action.
2. Select the Failover Action, and then click Configure Action.
3. Select the pool you want to use to failover to the backup server.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   
   ![This is often used to prevent an action from occurring during specific windows.]

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the HA pool you selected fails over to the secondary server.

Log the alert message to a file in the Orion Platform

SolarWinds can be configured to log alerts to a designated file which can be viewed at a later time.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Log the Alert to a File option, then click Configure Action.
3. Under Log to File Settings:
   a. Enter the log filename in the Alert Log Filename field.
   b. Enter a maximum log file size in MB (0 = unlimited).
   c. Enter the Message of your alert trigger in the field provided.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   
   ![This is often used to prevent an action from occurring during specific windows.]

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the alert is logged to the file with the message you created.

Log the alert to the NPM event log

Record when an alert is triggered to the NetPerfMon (NPM) event log on your Orion server or on a remote server for later investigation.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Log the Alert to the NetPerfMon Event Log from the options, and then click Configure Action
3. Under Log the Alert to the NetPerfMon Event Log settings, enter the text you want written to the file. Use variables to make the message dynamic.

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing. This is often used to prevent an action from occurring during specific windows.

5. Expand Execution Settings to select when the action occurs.

6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the alert is logged to the NPM event log with the message you created.

Change the resource allocation of a virtual machine in the Orion Platform

If a virtual machine is experiencing performance issues, you can have an alert trigger a specified allocation of resources. This alert management action is available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.

2. Select Manage VM - Change CPU/Memory Resources, and click Configure Action.

3. Enter a name for the action.

4. Under Select Virtual Machine, specify the virtual machine on which you want to adjust the number of CPUs, the memory capacity, or both.
   a. To change the resource allocation of the virtual machine that triggered the alert, click Execute this action. This option is only available if the alert is built to trigger for virtual machines.

   b. To change the resource allocation of a different virtual machine, click Select specific VM, and search for a virtual machine.

5. To power off the virtual machine before changing the resource allocation, and then power it on again after the resource allocation has been changed, select the relevant option. If the option is not selected, the action will be performed live on the virtual machine.

6. Under Specify New Resources, specify whether you want to add more resources to the virtual machine, or replace the existing resources with new resources, and then specify the parameters of the new resource or resources.
   a. Select Number of processors, and specify the number of processors to allocate.

   b. Select Memory, and specify the memory capacity to allocate.

7. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This
schedule only applies to the alert action you are editing.

8. Select how frequently this action occurs for each triggered alert in Execution Settings.
9. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified CPU and memory resources will be allocated to the virtual machine.

Delete a snapshot of a virtual machine in the Orion Platform

If a virtual machine is experiencing resource issues, you can have an alert trigger a virtual machine snapshot to be deleted. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Delete Snapshot, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine from which you want to delete a snapshot.
   a. To delete a snapshot of the virtual machine that triggered the alert, click Execute this action.
   This option is only available if the alert is built to trigger for virtual machines.
   b. To delete a snapshot of a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the snapshot of the specified virtual machine will be deleted.

Move a virtual machine to a different host in the Orion Platform

If a virtual machine is experiencing issues, you can have an alert trigger the virtual machine to be moved to a different host. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Move to a Different Host, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to move.
   a. To move the virtual machine that triggered the alert, click Execute this action.

   This option is only available if the alert is built to trigger for virtual machines.

   To apply the action only to virtual machines of a specific vendor, select the relevant option, and specify whether you want to perform to action on Hyper-V or VMware virtual machines.

   b. To move a different virtual machine, click Select specific VM, and search for a virtual machine.

4. To power off the virtual machine before moving it to a different host, and then power it on again after the action has been completed, select the relevant option.

   If the option is not selected, the action will be performed live on the virtual machine.

5. Under Select Target Host, search for the host where you want to move the selected virtual machine.

6. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing. This is often used to prevent an action from occurring during specific windows.

7. Select how frequently this action occurs for each triggered alert in Execution Settings.

8. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be moved to a different host.

### Move a virtual machine to a different storage in the Orion Platform

If a virtual machine is experiencing storage issues, you can have an alert trigger the moving of the virtual machine to a different storage location. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.

2. Select Manage VM - Move to a Different Storage, and click Configure Action.

3. Under Select Virtual Machine, specify the virtual machine that you want to move.
   a. To move the virtual machine that triggered the alert, click Execute this action.

   This option is only available if the alert is built to trigger for virtual machines.

   To apply the action only to virtual machines of a specific vendor, select the relevant option, and specify whether you want to perform to action on Hyper-V or VMware virtual machines.

   b. To move a different virtual machine, click Select specific VM, and search for a virtual machine.
4. To power off the virtual machine before moving it to a different storage, and then power it on again after the action has been completed, select the relevant option.

   ![Info icon] If the option is not selected, the action will be performed live on the virtual machine.

5. Under Select Target Datastore, search for the datastore where you want to move the selected virtual machine.
   
   a. In a VMware environment, select one of the available datastores.
   
   b. In a Hyper-V environment, select one of the available datastores, and click either Use the default location to move the virtual machine to the default location of the datastore, or click Specify custom path, and enter a custom location.

6. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   ![Note icon] This is often used to prevent an action from occurring during specific windows.

7. Select how frequently this action occurs for each triggered alert in Execution Settings.

8. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be moved to a different datastore.

### Pause a virtual machine in the Orion Platform

If a virtual machine is experiencing issues, you can have an alert trigger a pause for the virtual machine. This alert management action is only available if the integration with Virtualization Manager is enabled.

This action can only be configured for Hyper-V virtual machines.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.

2. Select Manage VM - Pause, and click Configure Action.

3. Under Select Virtual Machine, specify the virtual machine that you want to pause.

   a. To pause the virtual machine that triggered the alert, click Execute this action.

      ![Info icon] This option is only available if the alert is built to trigger for virtual machines.

   b. To pause a different virtual machine, click Select specific VM, and search for a virtual machine.

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

      ![Note icon] This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.

6. Click Add Action.
The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be paused.

Power off a virtual machine in the Orion Platform

If a virtual machine is experiencing issues, you can have an alert trigger the virtual machine to be powered off. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Power Off, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to power off.
   a. To power off the virtual machine that triggered the alert, click Execute this action.
      • This option is only available if the alert is built to trigger for virtual machines.
   b. To power off a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   • This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be powered off.

Power on a virtual machine in the Orion Platform

If a virtual machine is powered off, you can have an alert trigger the virtual machine to be powered on. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Power On, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to power on.
   a. To power on the virtual machine that triggered the alert, click Execute this action.

   ![This option is only available if the alert is built to trigger for virtual machines.]

   b. To power on a different virtual machine, click Select specific VM, and search for a virtual machine.

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   ![This is often used to prevent an action from occurring during specific windows.]

5. Select how frequently this action occurs for each triggered alert in Execution Settings.

6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be powered on.

**Restart a virtual machine in the Orion Platform**

If a virtual machine is experiencing issues, you can have an alert trigger the virtual machine to be restarted. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.

2. Select Manage VM - Reboot, and click Configure Action.

3. Under Select Virtual Machine, specify the virtual machine that you want to reboot.
   a. To reboot the virtual machine that triggered the alert, click Execute this action.

   ![This option is only available if the alert is built to trigger for virtual machines.]

   b. To reboot a different virtual machine, click Select specific VM, and search for a virtual machine.

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   ![This is often used to prevent an action from occurring during specific windows.]

5. Select how frequently this action occurs for each triggered alert in Execution Settings.

6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine restarts.
Suspend a virtual machine in the Orion Platform

If a virtual machine is experiencing performance issues, you can have an alert trigger the virtual machine to be suspended. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Suspend, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to suspend.
   a. To suspend the virtual machine that triggered the alert, click Execute this action.
      
      This option is only available if the alert is built to trigger for virtual machines.
   b. To suspend a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   
   This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine is suspended.

Take a snapshot of a virtual machine in the Orion Platform

If a virtual machine is experiencing issues, you can have an alert trigger a snapshot of the virtual machine to be taken. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Take Snapshot, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine of which you want to take a snapshot.
   a. To take a snapshot of the virtual machine that triggered the alert, click Execute this action.
      
      This option is only available if the alert is built to trigger for virtual machines.
   b. To take a snapshot a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This
schedule only applies to the alert action you are editing.

This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.

6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, a snapshot is taken of the specified virtual machine.

Play a sound when an alert is triggered in the Orion Platform

The Play a Sound action uses the SolarWinds desktop notification client to play the sound on your computer when an alert arrives.

You must download and install the client on every computer that you want to play a sound when an alert arrives. After installing the desktop notification client, configure which sound you want to play when an alert is received.

Computers that do not have the desktop notification client installed on them do not play a sound when an alert arrives. If you want an alert notification sound to play on your desktop or laptop, you must install and configure the desktop notification client on that computer.

Download the desktop notification client from <Your SolarWinds Orion server>/DesktopNotificationTool/SolarWinds.DesktopNotificationTool.msi. Run the installer and follow the on-screen instructions to install the client.

The desktop notification client requires the following information to connect to your Orion server and receive alerts:

- Orion Server Name or IP Address
- Orion User Name
- Password

You can use the server name and credentials that you use to logon to your SolarWinds product.

SolarWinds can be configured to play a sound upon alert trigger or reset. This alert action is frequently used in NOC environments. The SolarWinds Desktop Notification client must be installed on each computer that you want to play a sound. The following procedure configures a sound to play for an alert.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.

2. Select the Play a Sound option, and then click Configure Action.

3. Under Play a sound settings:
   - If not installed, click Download our desktop notification client to download and install the notification client. From the notification client, select an alert sound.

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This
schedule only applies to the alert action you are editing.

This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, a sound plays through the client.

**Restart IIS sites or application pools in the Orion Platform**

If IIS or application pools are experiencing performance or resource issues, you can use an alert to restart them.

You must know the IIS Server name and the Site or Application Pool to restart a remote instance of IIS.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Restart IIS Site/Application Pool from the options, and then click Configure Action.
3. Expand Restart IIS Site/Application Pool Settings.
   a. Select the IIS Action to Perform from the drop down list.
   b. Choose the Site or Application Pool.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the selected site or pool restarts.

**Send an SNMP trap in the Orion Platform**

SNMP traps signal the occurrence of significant events by sending SNMP messages to a monitoring device. You can have an alert trigger this action to inform you of these events.
This action requires the following information:

- UDP port number
- SNMP version number
- SNMP credentials

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Send SNMP Trap option, then click Configure Action.
3. Under Send SNMP Trap Message:
   a. Enter SNMP Trap Destinations in the field provided.
   b. Select a Trap Template from the drop down lists.
4. Enter the Message of your alert trigger in the field provided.
   a. Optionally click Insert Variable to add variables using the following procedure:
5. Expand SNMP Properties.
   a. Enter a UDP Port number in the field provided.
   b. Select an SNMP Version from the drop down list.
   c. Enter the SNMP Community String in the field provided.
6. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   ! This is often used to prevent an action from occurring during specific windows.
7. Select how frequently this action occurs for each triggered alert in Execution Settings.
8. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the SNMP trap message is sent.

Send a GET or POST request through HTTP or HTTPS in the Orion Platform

SolarWinds can be configured to communicate alerts using GET or POST functions through HTTP or HTTPS. As an example, a URL may be used as an interface into a trouble ticket system, and, by correctly formatting the GET function, new trouble tickets may be created automatically.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert wizard.
2. Select the Send a GET or POST Request to a Web Server option, then click Configure Action.
3. Under HTTP request settings:
   a. Enter a URL in the field provided.
   b. Select either Use HTTP GET or Use HTTP POST.

   Enter HTTPS instead of HTTP in the URL to send the information using HTTPS.

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.

6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the GET or POST request is sent to the server. You can view the server logs to confirm that the action occurred.

Send a syslog message in the Orion Platform

SolarWinds can log received alerts to the syslog of a designated machine for later investigation. The following procedure configures an alert to send a message to a designated syslog server.

Starting with Orion Platform 2019.2, you can encrypt syslog messages using TCP or TCP/TLS protocols.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Send a Syslog Message option, then click Configure Action.
3. Under Send a Syslog message settings:
   a. Enter the Hostname or IP Address of the syslog server in the field provided.

   Multiple syslog servers should be separated by commas.

   b. Select a protocol. By default, UDP is selected. Ensure that appropriate ports are open:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port to open</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>514</td>
</tr>
<tr>
<td>TCP</td>
<td>1468</td>
</tr>
<tr>
<td>TCP/TLS</td>
<td>6514</td>
</tr>
</tbody>
</table>

   To specify a different port, provide it directly in the Hostname/IP Address field above. For example: 1.23.4.10:500 sends a syslog message to 1.23.4.10, port 500.
c. If you selected TCP/TLS, further specify certificate validation rules:
   - Ignore Certificate Chain Errors: Select the box to ignore any chain errors of the certificate, such as a missing root certificate.
   - Disable Certificate Revocation Check: Select the box to skip CRL check of a certificate. Useful to bypass 'revoked certificate' errors.
   - Ignore Certificate Name Mismatch: Select to ignore errors where the Common Name or Subject Alternative Name of the certificate does not match the client's (Orion server) host name.

d. Select a Severity and a Facility from the drop down lists.

4. Enter the Message of your alert trigger in the field provided.

5. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   This is often used to prevent an action from occurring during specific windows.

6. Select how frequently this action occurs for each triggered alert in Execution Settings.

7. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the syslog message is sent.

Send an email or page in the Orion Platform

This action sends an email from the product to selected recipients for the investigation into the cause of the alert.

Before configuring this alert you must first configure the default SMTP server the product uses to send an email. You can change the default SMTP server later or use different SMTP servers for specific alerts.

You need the following information:
   - The SMTP host name or IP address
   - The SMTP port number
   - Whether the SMTP server uses SSL
   - The SMTP credentials, if necessary
   - Default sender email address

Configure the SMTP server in the alert action or from the Settings page.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Send an Email/Page option, then click Configure Action.
3. Enter recipients and the message.
4. Enter the SMTP information.

5. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   This is often used to prevent an action from occurring during specific windows.

6. Select how frequently this action occurs for each triggered alert in Execution Settings.

7. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the email or page is sent.

Manually set a custom status in the Orion Platform

Setting a custom status can be useful if you want to change the status of a familiar node, but does not affect actual, polled values. For example, if the custom status is set to Up, but the server is down or unresponsive, packet loss continues to be 100%. Alerts based on the status do not trigger in this instance, but alerts based on a polled value, such as packet loss, do trigger.

When the status is set with an alert, the status does not update to the actual, polled status. The status must be switched manually to a different status or configured to use the polled status. Change the status to use the polled status from the node details page or create a reset action to set the status to use the polled status.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.

2. Select the Set Custom Status option, then click Configure Action.

3. Under Change Object Status Manually:
   a. Select Change to a specific status if you are creating a trigger action, and choose a status.
   b. Select Use polled status if you are creating a reset action.
   c. Choose the nodes you want to set the status.

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.

6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the status for the object changes.
Use the speech synthesizer to read alerts in the Orion Platform

The Text to Speech Output action uses the SolarWinds desktop notification client and your computer's speech synthesizer to convert text messages-to-speech messages. The action notifies users of new alerts by reading the alert out loud. This capability is especially helpful for users who are visually impaired or who are not always at their desks to read alerts onscreen.

Download and install the client on each computer that you want to play a sound. Then configure which synthesizer you want to play.

SolarWinds uses Microsoft® Speech Synthesis Engine version 5.0. If you are under active SolarWinds maintenance, you may also install and use other text-to-speech engines by visiting the SolarWinds website. The following procedure configures text-to-speech output for an alert trigger or reset.

**Due to restrictions on Windows service applications, the Text to Speech action is not available to SolarWinds installations on Windows 7 or Windows Server 2008 and higher.**

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Text to Speech Output option, then click Configure Action.
3. Under Text to Speech Output settings click Download our desktop notification client to download, install, and configure the notification client.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   - This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the message is read.

Log an alert to the Windows Event Log on a specific server in the Orion Platform

Add an entry to the Windows Event Log either on the SolarWinds Orion server or on a monitored remote server later investigation.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Windows Event Log option, then click Configure Action.
3. Under Event Log Settings, enter the message you want logged.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the alert message is added to the Windows Event log.

Defunct alert variables in the Orion Platform

The following variables are no longer valid:

- `${Property}` - The property the alert is monitoring. You can select a new variable with the specific property you want to view.
- `${TriggeredValue}` - The value that triggered the alert. You can select a new variable with the specific property you want to view.
- `${AlertStartTime}` - When the alert is active. You can use the Time of Day scheduler to control when the alert is active.
- `${AlertEndTime}` - When the alert is no longer active. You can use the Time of Day scheduler to control when the alert is not active.
- `${ObjectSubType}` - Determines if the node supports SNMP or is ICMP only. You can use Node.ObjectSubType as the macro name.

Share Orion Platform alerts with other SolarWinds products

Alerts may be shared with selected other SolarWinds products that are not part of the SolarWinds Orion Platform, such as AlertCentral, Web Help Desk, or ServiceNow.

1. On the Alert Summary page, expand Alert Integration.
2. Select the Integrate alert with other SolarWinds check box.
3. Provide an Alert Subject. You can choose to use this name as the subject field for the alert.
4. Choose the alert Severity.

Same information may be used to determine how a shared alert is handled by the other product.

5. Include additional alert properties in the alert by clicking Insert Variable and choosing the ones you want to include. This ensures that the variables you used in the alert message are translated correctly to the other product.
Manage Orion Web Console user accounts in the Orion Platform

Users need an Orion Web Console account to perform actions in your SolarWinds product, such as acknowledging alerts. Default account views and privileges are assigned in the account manager.

You may not need to grant all privileges to all users if they only need to review reports or access views. See Share Orion Platform views with non-Orion Web Console users for more information.

Add users individually, add group accounts, or use Active Directory accounts. If a user is in multiple group accounts, the permissions of the group highest on the Groups tab of the Account Manager are applied to the user. By default SolarWinds uses MSAPI to authenticate Active Directory users, but you can authenticate users with LDAP.

To prevent issues with accounts, make sure that your SQL Server disables the no count connection option.

Default accounts

In the Orion Web Console, there are two default accounts: admin and guest.

When you log in to the Orion Web Console for the first time, specify a password for the default Admin user.

The guest password only has view permissions for all entities. By default, it is disabled and is configured with a blank password.

To use the guest password, you need to enable it. SolarWinds recommends that you change the password for this account before you start using it.

Create users in the Orion Platform

Before you begin, consider what tasks the user must perform, what views and menu bars are most suitable, and what type of account to use.

Supported account types:

- Orion individual account
- Windows individual or group account (you can use Active Directory or local domain accounts)
- SAML individual or group account
Users created using default settings can log in to the Orion Web Console and see information available in views, resources, and reports. For administration and customization tasks, users need extra rights.

Create Orion individual accounts

1. Log in to the Orion Web Console, and click Settings > All Settings.
2. Click Manage Accounts in the User Accounts grouping, and click Add New Account on the Individual Accounts tab.

![Manage Accounts](image)

3. Select Orion individual account, and click Next.

![I would like to create:](image)

4. Type a user name and the account credentials, and click Next.

   When creating an Orion individual account, you cannot use the symbols @, \ (backslash), or / (forward slash) in the name.

5. On Define Settings, provide rights so that the user can perform assigned tasks, select default views and menu bars, and then click Submit.

The user account is listed in the Individual Accounts tab.
Create users based on existing Active Directory or local domain accounts

Users can use their existing Active Directory credentials to log in to the Orion Web Console, so you do not need to manage an extra user account.

- You must enable Windows Account Login in the Orion Web Console.
  1. Click Settings > All Settings, and in Product Specific Settings, click Web Console Settings.
  2. In Windows Account Login, select Enable automatic login, and click Submit.
- To maintain administrative privileges, individual and group Windows user accounts must be defined in the same domain as the SolarWinds server they can access.
- Only Security AD groups are supported. Distribution Groups are not supported.

1. Log in to Orion Web Console, and click Settings > All Settings.
2. Click Manage Accounts in the User Accounts grouping, and click Add New Account.
3. Select Windows individual account or Windows group account, and click Next.

4. Provide the credentials for an account with administrative access to the Active Directory or local domain, and click Next.
5. If a system account is available, you can use it. Select Use [Account Name] account to access Active Directory or Local Domain, and click Test Active Directory.

- You may need to specify the credentials manually.
- This option is not available when LDAP is enabled. You must specify credentials manually.

6. To specify the credentials manually, select Specify credentials to access the Active Directory or Local Domain, and provide the credentials.

7. Search for the Active Directory or local domain account.

To search for all users or groups in the domain, enter domain name\* and click Search.

8. Select the appropriate users in the Add Users area, and click Next.

9. On Define Settings, provide rights so that the user can perform assigned tasks, select default views and menu bars, and then click Submit.

Users can now log in to the Orion Web Console using their local domain or Active Directory credentials. If you use Active Directory, users can also automatically login with their Windows credentials.

Change account passwords in the Orion Platform

When you log in to the Orion Web Console for the first time after you have deployed your Orion Platform products, you are prompted to create a password for the Admin account. This password cannot be blank.

To change passwords for user accounts, complete the following steps:

1. Log in to the Orion Web Console using an account with Administrator rights, and click Settings > All Settings.
2. Click Manage Accounts in the User Accounts grouping.
3. Select a user, and click Change Password.

![Manage Accounts](image)

4. Enter and confirm the new password, and click Change Password.

Enable Orion Platform users to authenticate through LDAP

You can choose to have all of your AD users authenticate through LDAP. The Orion server does not need to be added to the Windows domain with this authentication method. All authentication requests will use the domain you save, even if the Orion server is part of a different domain.

We do not support Anonymous authentication through LDAP.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. Click Advanced AD Settings in the User Accounts grouping.
4. Toggle Authenticate Active Directory Users via LDAP.
5. Enter your LDAP server information and select the authentication method that matches what is used in LDAP.

Click Discover DN to fill in the distinguished name (DN) of the AD domain automatically. If the DN field does not populate, verify that the Directory Server Address is correct.

Windows individual accounts now use LDAP. If you created Orion Web Console accounts that use Active Directory or local accounts and those accounts cannot authenticate through LDAP, those accounts cannot login.

If you disable this selection, Windows users or group members created while it was enabled cannot login.

Authenticate Orion Platform users with SAML v2

Starting with Orion Platform 2018.4, you can log in to the Orion Web Console using the Security Assertion Markup Language (SAML) v2 single sign-on protocol. SAML v2 is the protocol used for exchanging authentication and authorization data between the security domain (Identity Provider) and the service provider.
How to configure SAML v2 authentication in the Orion Platform

1. Configure the single sign-on login provider (such as AD FS or Okta) to be able to communicate with the Orion Platform.

SAML 2.0 is an open standard. The following sections provide step-by-step instructions for configuring Active Directory Federation Services and Okta, but you can use the Orion Platform SAML authentication together with a wide variety of different SAML 2.0 providers.

3. Configure the Identity Provider in the Orion Web Console.

4. Create SAML single users or SAML group user accounts for users who log in to the Orion Web Console using SAML v2 authentication.

Configure Active Directory Federation Services for single sign-on login to the Orion Web Console

Mapping AD FS to the Orion Platform requires that:

- AD FS is configured on the server.
- A token encryption certificate is available.
- Service endpoint URL for the relying party trust is configured.

Step 1: Configure the Relying Party Trust

1. In the Windows Server Manager, click Tools, and then select AD FS Management.
2. Under Actions, click Add Relying Party Trust.
3. On the Welcome page, choose Claims aware and click Start.
4. On the Select Data Source page, click Enter data about the relying party manually, and click Next.
5. On the Specify Display Name page, type a name in Display name. Under Notes, type a description for this party trust, and click Next.
6. Ensure that the encryption certificate for the relying party trust is empty, and then click Next.

Orion Platform 2018.4 does not support this certificate. Providing the certificate might cause issues.
7. On the Configure URL page, do the following:
   a. Select the Enable support for the SAML 2.0 WebSSO protocol box.
   b. Under Relying party SAML 2.0 SSO service URL, type the Security Assertion Markup Language (SAML) service endpoint URL for this relying party trust, such as https://hostname.domain/Orion/SamlLogin.aspx, and then click Next.

   ![Screenshot of a table showing options for configuring a relying party trust.](Screenshots property of © 2019 Microsoft.)

   The Orion Web Console must be configured to support https.

8. On the Configure Identifiers page, specify one or more identifiers for this relying party, such as http://hostname, click Add to add them to the list, and then click Next.


10. Complete the wizard.

Step 2: Configure Claim Rules for the Relying Party Trust

When you have created the Relying Party Trust, configure Claim Rules:

1. Right-click the created Relying Party Trust and select Edit Claim Issuance Policy.
2. Click Add Rule.
3. From the drop-down, select Send LDAP Attributes as Claims, and click Next.
4. Fill in the Claim rule name and pick Active Directory as an Attribute store.
5. Next fill the Mapping of LDAP attributes as follows:

<table>
<thead>
<tr>
<th>LDAP Attribute</th>
<th>Outgoing Claim Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-Principal-Name</td>
<td>Name ID</td>
</tr>
<tr>
<td>Given-Name</td>
<td>FirstName</td>
</tr>
<tr>
<td>Surname</td>
<td>LastName</td>
</tr>
</tbody>
</table>
### LDAP Attribute | Outgoing Claim Type
---|---
E-Mail-Addresses | Email
Token-Groups - Qualified by Long Domain Name | OrionGroups

You have configured your AD FS to match the Orion Platform requirements. [Specify the Identity Provider in the Orion Web Console](https://example.com).

**Step 3: Configure Additional Website**

*This step applies only if you have deployed additional web servers.*

1. In AD FS Management, right-click Relying Party Trusts, and select Properties.
2. Select the Endpoints tab and click the Add SAML button.
3. Set the following values and click OK.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint type</td>
<td>SAML Assertion Consumer</td>
</tr>
<tr>
<td>Binding</td>
<td>POST</td>
</tr>
<tr>
<td>Index</td>
<td>Select a value higher than existing indexes.</td>
</tr>
<tr>
<td>Trusted URL</td>
<td>Your SAML login URL, such as <code>https://hostname.domain/Orion/SAMLLogin.aspx</code></td>
</tr>
</tbody>
</table>

4. Click Apply and then click OK.

The additional website is configured for SAML configuration in the Orion Platform.

**Step 4: Export the token-signing certificate from the AD FS server**

1. Open AD FS and navigate to Service > Certificates.
2. Click the Token-signing certificate.
3. In the Actions section, click View Certificate.
4. Click the Details tab, click Copy to File, and then click Next.
5. Select Base-64 encoded X.509 (.CER), and click Next.
6. Click Browse, select a location, enter a file name, and then click Save.
7. Click Next, and then click Finish.

**Configure Okta for single sign-on login to the Orion Web Console**

*If prompted to switch to the Classic UI, switch to the Classic UI.*

1. Log in to your Okta organization with administrative privileges.
2. Click on the blue Admin button.

4. Select the SAML 2.0 option and click Create.

5. In General Settings, type the SAML Application Name in the App name field, and click Next.

6. In the Configure SAML Setting section, make the following changes:
   a. In the General section, paste the SAMLLoging URL of your Orion Web Console into the Single sign on URL.
      Example: https://hostname.domain/Orion/SAMLLogin.aspx
   b. Enter the address of your Orion Web Console to Audience URI (SP Entity ID)
      Example: http://hostname
   c. In the Attribute Statements section, add following attribute statements:

<table>
<thead>
<tr>
<th>Name</th>
<th>Name format</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Unspecified</td>
<td>user.email</td>
</tr>
<tr>
<td>FirstName</td>
<td>Unspecified</td>
<td>user.firstName</td>
</tr>
<tr>
<td>LastName</td>
<td>Unspecified</td>
<td>user.lastName</td>
</tr>
</tbody>
</table>

   d. Add following to the Group Attributes Statements:

<table>
<thead>
<tr>
<th>Name</th>
<th>Name format</th>
<th>Filter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OrionGroups</td>
<td>Unspecified</td>
<td>Regex</td>
<td>.*</td>
</tr>
</tbody>
</table>

7. If you have deployed an additional web server, configure the additional website:
   a. Select the Allow this app to request other SSO URLs box.
   b. In the Requestable SSO URLs, click Add Another, and provide the additional web server URL into the URL field. For example: https://hostname.domain/Orion/SAMLLogin.aspx
   c. In the Index box, provide appropriate index value.

8. Click Next, and then click Finish.

9. Specify users to access the Orion Web Console through SAML login:
   a. In Okta, click Assignments > Assign, and select Assign to People.
   b. Select users and click Assign.
   c. When you have selected all users, click Done.

Now configure the identity provider in the Orion Web Console.

Click the View Setup Instruction button in the section with Sign on methods and leave the tab open. You will need this information to configure the Identity Provider in the Orion Web Console.
Configure your Identity Provider in the Orion Web Console

1. Log in to the Orion Web Console using an administrator account.
2. Click Settings > All Settings.
3. In the User Accounts section, click SAML Configuration.
4. Click Add Identity Provider.
5. In the Enter Orion URL step, make sure that the hostname of the Orion Web Console server is correct, and click Next.
   Verify that the hostname of the server hosting your main website and/or additional website:
   a. Log in to the Orion Web Console hosted on your main Orion Platform server using an administrator account.
   b. Click Settings > All Settings, and then click Web Console Settings.
   c. Make sure that the Orion Web Server Address field is empty or that the hostname is the same as you can see on the Prepare Identity Provider page.
   d. If you have deployed additional web servers, review the additional web server hostname. Repeat steps b-c for the Orion Web Console hosted on the additional web server.
6. In Prepare IdP step, copy to clipboard the Single Sign-on URL you need to use when configuring Okta or AD FS, and use the URL accordingly.
7. In the Configure step, fill in the information according to the Identity Provider:
   - **Identity Provider Name - Name**: specify how the identity provider will be displayed on the login page.
   - **SSO Target URL (Endpoint)**
     Okta format: https://dev-140035.oktapreview.com/app/solarwindsdev140035_appName_1/xyz/sso/saml
     AD FS format: https://hostname.domain/adfs/ls
   - **Issuer (Entity ID)**
     Okta format: http://www.okta.com/exkpjshx3ZUPjCfB0h7
AD FS format: http://hostname.local/adfs/services/trust

- **Public Certificate** - Certificate in Base64 form
  [Where do I get the certificate for AD FS?]

8. Click Next and save the configuration.

When logging to the Orion Web Console, users now see an additional button Log In with Okta or Log In with AD FS, based on the Identity Provider you have defined. To enable users to log in using single sign-on, create SAML users or SAML user groups for the users.

**Create a SAML user in the Orion Platform**

1. Log in to the Orion Web Console using an account with Administrator privileges.
2. Click Settings > All Settings > Manage Accounts.
3. Click Add New Account, and select SAML individual account or SAML group account.

4. For Name ID, provide the same user name you **specified in the Identity Provider (AD FS or Okta)**. The Name ID and Identity Provider Name must match.

5. **Specify what the user can access, do and the default menu bars** and complete the wizard.

Users now can log in to the Orion Web Console by clicking the Login with Okta/AD FS button on the login page and providing their Okta or AD FS credentials.

**Create SAML user groups in the Orion Platform**

1. Log in to the Orion Web Console using an account with Administrator privileges.
2. Click Settings > All Settings > Manage Accounts.
3. Click the SAML Groups tab and click Add New Group Account.
4. Provide the name for the group. Use the following format for the name: hostname.domain\Group Name.

   * The SAML Group and the Identity Provider Group Name must match.

5. **Specify what the user can access, do and the default menu bars** and complete the wizard.

   Members of the SAML group can now log in to the Orion Web Console by clicking the Login with Okta/AD FS button on the login page and providing their Okta or AD FS credentials.

### Troubleshoot SAML Login

If users cannot log in using SAML login, review the SAML log to find out more details. By default, the log is located at

```
C:\ProgramData\SolarWinds\Logs\Orion\SAML.log
```

### Test your SAML configuration

1. Click Settings > All Settings > SAML Configuration, and then click Test Configuration.

2. To test SAML configuration on the computer you have the Orion Web Console open, click Test Configuration.

3. To test whether SAML login works correctly for other users on other computers, click Copy and send the link to the user who is attempting to log in using the SAML protocol from another computer. If the output is unsuccessful, instruct the user to copy it and send it to the administrator.

4. The Test SAML configuration page opens with the results of the test. You can see the test sent to your Identity Provider and its response. Use the response to troubleshoot the issue or send it to your administrator.

### Define what users can access and do in the Orion Platform

Each user or group account can have different privileges applied to it, such as the ability to modify alert definitions or delete nodes.

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

2. Click Settings > All Settings in the menu bar.

3. Click Manage Accounts in the User Accounts grouping.

4. Select an account, and click Edit.
5. Specify the login options.

<table>
<thead>
<tr>
<th>Login option</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Should the user be able to log in immediately?</td>
<td>Set Account Enabled to Yes.</td>
</tr>
<tr>
<td></td>
<td>• Disabling an account does not delete it. Account definitions and</td>
</tr>
<tr>
<td></td>
<td>details are stored in the SolarWinds Orion database and can be</td>
</tr>
<tr>
<td></td>
<td>enabled later.</td>
</tr>
<tr>
<td></td>
<td>• When you disable an account that was used to create alerts, the</td>
</tr>
<tr>
<td></td>
<td>alerts' Owner field is permanently cleared, but the alerts operate</td>
</tr>
<tr>
<td></td>
<td>as normal.</td>
</tr>
<tr>
<td>Should the user be able to log in only temporarily?</td>
<td>Specify the expiration date.</td>
</tr>
<tr>
<td>Should the user be logged in indefinitely even if the browser is closed?</td>
<td>Select Yes for the Disable Session Timeout option. Session timeouts</td>
</tr>
<tr>
<td></td>
<td>are global and set in Web Console Settings. By default, new user</td>
</tr>
<tr>
<td></td>
<td>accounts are configured to timeout automatically.</td>
</tr>
</tbody>
</table>

6. Specify what tasks the user should be able to do.

<table>
<thead>
<tr>
<th>Task</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add and edit user accounts and reset passwords.</td>
<td>Allow Administrator Rights</td>
</tr>
<tr>
<td></td>
<td>Granting administrator rights does not assign the Admin menu bar to a user.</td>
</tr>
<tr>
<td>SolarWinds recommends that you do not allow users to change their own Orion Web Console account passwords.</td>
<td></td>
</tr>
<tr>
<td>Add, edit, and delete nodes.</td>
<td>Allow Node Management Rights</td>
</tr>
<tr>
<td>Create, edit, and delete maps in the Network Atlas.</td>
<td>Allow Map Management Rights</td>
</tr>
<tr>
<td>Add, edit, schedule, and delete reports.</td>
<td>Allow Report Management Rights</td>
</tr>
<tr>
<td></td>
<td>To only allow access to some reports, select the report category the user can access.</td>
</tr>
<tr>
<td>Task</td>
<td>Access (Select Yes for this option or do as instructed)</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Add, edit, and delete alerts. | Allow Alert Management Rights  
To only allow some actions, keep No in Allow Alert Management rights and Allow items in the Alerts section as appropriate.  
To only access some alerts, select the category the user can access, or No Limitation. |
| Customize views. | Allow Account to Customize Views  
By default, customized view creation is not allowed. Changes made to a view are seen by all other users that have been assigned the same view. |
| Enable/disable monitoring, or stop triggering alerts for monitored entities. | Allow Account to Unmanage Objects & Mute Alerts |
| Acknowledge and clear events, advanced alerts, and Syslogs. | Allow Account to Clear Events, Acknowledge Alerts and Syslogs |

7. If you want the user to use additional browser functions, such as right-click menu options, set Allow Browser Integration to Yes.

   Right-click menu options also depend on installing the SolarWinds Desktop Toolset and running the Toolset Integration Tray application on each client computer.

8. Provide the maximum Number of Items in the Breadcrumb List.

   To show all available items in breadcrumb drop-downs, set this option to 0.

9. Click Submit.

New account settings are applied when a user next logs in.

The user account also controls the default menu bars and views, and how much of your network they can access through the Orion Web Console.
Restrict user access to network areas by applying limitations in the Orion Platform

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

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

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

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

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

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

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

Create limitations based on custom properties in the Orion Platform

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

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

1. Click Start > All Programs > SolarWinds Orion > Grouping and Access Control > Account Limitation Builder.
2. Click Start on the splash screen.
3. Click Add Limitation.

4. Select a Custom Property. The fields are populated automatically based on your selection.

5. Choose a Selection Method.

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

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

6. Click OK.

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

Delete account limitations in the Orion Platform

Deleting a limitation makes it unavailable for future use in the Orion Web Console. If the limitation is applied to user accounts, the accounts will remain limited.

   - This procedure requires access to the computer that hosts the Orion server.

1. Start the Account Limitation Builder in the SolarWinds Orion > Grouping and Access Control program folder.

2. Click Start on the splash screen.

3. Click the row of the limitation that you want to delete.

   - Use <Shift+Click> to highlight multiple consecutive rows or <Ctrl+Click> to highlight multiple non-consecutive rows.

4. Click Edit > Delete Selected Limitations.

The limitation is now unavailable for limiting user accounts in the Orion Web Console.

Patterns for limitations in the Orion Platform

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

   - Patterns are not case sensitive.

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

(*foo* EXCEPT *b*) AND (*all* OR *sea*) matches seafood and footfall, but not football or Bigfoot.
Set default menu bars and views for users in the Orion Platform

The items users see in My Dashboards and in Alerts & Activity are specified in their user accounts.

**💡 Improve performance by setting the Home Page View to a view with a limited number of resources on it.**

1. Click Settings > All Settings in the menu bar.
2. In the User Accounts grouping, click Manage Accounts.
3. Select a user, and click Edit.
4. Scroll down to Default Menu Bars and Views, and select top menu bars from the lists.

![DEFAULT MENU BAR AND VIEWS](image)

5. Select Yes for the items the user can see in the Alerts & Activity menu bar.

![Show Alerts Menu](image)

6. Select an item and use the arrows to change the order of menu bars. Select an item from the list to specify the default Home page view.

![Tabs ordering](image)

7. Click Submit.

The user can now use the specified links in My Dashboards and Alerts & Activity menu bars.

New account settings are applied when a user next logs in.
You can set default view for feature-specific views, such as hardware health or F5, or for product-specific view, such as VSAN or Application Details.

**Limit users to specific network areas in the Orion Platform**

Account limitations ensure that Orion Web Console users only view the network objects that are relevant to their job duties.

You can use account limitations in the following ways:

- Limit customer views to specific network nodes
- Limit views by department or functional area
- Limit views by device type or device role
- Limit views based on the geographic location of devices

Predefined account limitations use built-in SolarWinds Orion properties to limit user access. For greater flexibility, you can create your own account limitations in the Account Limitation Builder, based on custom properties.

**Configure automatic login in the Orion Platform**

You can log in automatically to the Orion Web Console using any of the following methods.

**Use a Windows Active Directory Account**

Create users based on active directory or local domain accounts, and enable automatic login for users logged in to the server. See Create users based on existing Active Directory or local domain accounts.

(i) Windows authentication must be enabled in the Configuration Wizard and the Web Console Settings. See Enable Windows Authentication with Active Directory in the Orion Platform.

**Automatically log in with Windows Pass-through Security**

Users can be authenticated through Windows Security, with no need to log in with separate credentials. For more information, see Log in to the Orion Platform with Windows pass-through security.

**Share content to non-SolarWinds users with the DirectLink account**

If the DirectLink account is active, any URL referring directly to an Orion Web Console page will bypass the login page by logging the user into the DirectLink account. See Share Orion Platform views with non-Orion Web Console users.

**Pass-through user credentials in a URL**

See Automatically log in to the Orion Platform by passing your credentials through the URL.
SAML v2 Single Sign-on login: Active Directory Federated Services (AD FS) or Okta

Starting with Orion Platform 2018.4, you can use existing Okta or AD FS credentials to log in to the Orion Web Console. See Authenticate Orion Platform users with SAML v2.

Users are authenticated in the following priority:

1. Windows Active Directory Authentication when enabled
2. The Account or User ID and Password passed on the URL
3. The Account or User ID and Password entered on the login.aspx page
4. The Windows User if Pass-through Security is enabled
5. The Windows Domain to which the User belongs, for example, Development\Everyone
6. A DirectLink Account

Enable Windows Authentication with Active Directory in the Orion Platform

The Orion Web Console can authenticate Active Directory users and users who are members of Active Directory security groups by using MSAPI or LDAP. By default, Windows individual or group accounts use MSAPI to authenticate accounts.

You can only use one authentication protocol at a time. All Windows accounts are authenticated through MSAPI or LDAP, depending on which one is enabled.

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

Authenticate users through MSAPI

1. Create a user account based on existing Active Directory or local domain account.
2. Enable the Orion Web Console to use automatic Windows Authentication.
   a. Start the Configuration Wizard in the SolarWinds Orion > Configuration and Auto-Discovery program folder.
   b. Select Website, and click Next.
   c. Provide the appropriate IP Address, Port, and Website Root Directory, and select Yes - Enable Automatic Login Using Windows Authentication.
   d. Click Next, and complete the Configuration Wizard.
3. Log in to the Orion Web Console using the appropriate domain and user, providing Domain\User name or Username@Domain as the User Name.
4. Run the Configuration Wizard and enable Windows authentication.
5. Login to the Orion Web Console, and navigate to Settings > All Settings. In Web Console Settings, select Enable automatic login in the Windows Account Login drop-down.

Supported Active Directory scenarios in the Orion Platform

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

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

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Web Console Login Supported?</th>
<th>Local Login Required?</th>
<th>Network Atlas and Unmanage Utility Login Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login with &quot;Orion Server&quot; domain AD account</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Login with &quot;Orion Server&quot; domain Group AD account</td>
<td>Yes</td>
<td>Yes</td>
<td>LogonFallback must be enabled.</td>
</tr>
</tbody>
</table>
## Scenario

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Web Console Login Supported?</th>
<th>Local Login Required?</th>
<th>Network Atlas and Unmanage Utility Login Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login with trusted domain AD user</td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Login with trusted domain AD Group User</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login with &quot;Orion Server&quot; domain Group AD account (group user belongs to trusted domain)</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login with trusted domain Group AD account (group user belongs to &quot;Orion Server&quot; domain)</td>
<td>No</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Login with AD user or Group user from a foreign AD forest</td>
<td>Yes, when LDAP is enabled</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Login with AD Federation Services (Orion Platform 2018.4)</td>
<td>Yes, when LDAP is enabled</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Login with AD Federation Services (Orion Platform 2018.4)</td>
<td>Yes, when LDAP is enabled</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Enable LogonFallback

LogonFallback must be enabled when the Active Directory user of the Orion Web Console does not have local login rights to the web server.

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

To authenticate users through Windows pass-through security, IIS NT Security must be enabled on your server.

Pass-through security can be configured to employ Domain security, Local computer security, or both Domain and Local computer security at the same time.

The Orion Platform account credentials must match the credentials used for the Domain or Local computer security.

- This procedure requires access to the computer that hosts the Orion server.
- When authenticating users with Windows Security, ensure your Orion server uses the NetBIOS domain name, instead of the fully qualified domain name.

1. If you are using NT Domain Authentication Format for pass-through accounts, create these pass-through accounts in the Orion Web Console Account Manager using Domain\UserID as the User Name. For example:
   - Washington\Edward
   - StLouis\Bill

2. If you are using Local Computer Authentication Format for pass-through accounts, create these accounts in the Orion Web Console Account Manager using Computer\UserID as the User Name. For example:
   - SolarWindsS2\Edward
   - Server3\JonesR


Log in to the Orion Web Console using the Windows account credentials you have already established.

Share Orion Platform views with non-Orion Web Console users

Any URL referring directly to a Orion Web Console page bypasses the login screen, logging the user into the DirectLink account. If the DirectLink account does not exist, users are directed to the login page.

- The DirectLink account is created like any other account, and it can include custom views and account limitations.
- If you embed a view in another website, you may need to either disable cross-frame (X-Frame) protection in your IIS configuration, or add the website to the X-Frame-Options header in IIS. SolarWinds enables cross-frame protection by default to decrease security risks. Consult microsoft.com for more information.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the User Accounts grouping, click Manage Accounts.
4. Click Add New Account.
5. Type DirectLink as the User Name.
6. Type a Password, confirm it, and click Next.
7. Edit DirectLink account options. See Define what users can access and do in the Orion Platform.
8. Click Submit.

Users can now look at views without an account on the Orion Web Console.

Automatically log in to the Orion Platform by passing your credentials through the URL

Create a favorite or bookmark that includes your Orion individual account user name and password as parameters within the URL.

HTTP requests are not encrypted, so account information sent in HTTP requests are not secure. For more information about enabling HTTPS on your Orion Platform product server, consult www.microsoft.com.

Create a favorite with a link in the following form to pass the login information:


Provide the hostname or IP address of your Orion server as the DOMAIN. Provide your Orion user name as the USER, and then provide your Orion user account password as the PASSWORD.
Manage Orion Polling Engines in the Orion Platform

To optimize your polling engines for best performance, SolarWinds recommends tuning them regularly. If you use more than one polling engine, you must balance the load so each engine performs best.

View information about the performance of all polling engines in your Orion Platform product installation in the Polling Engine view by clicking Settings > All Settings, and then Polling Engines in the Details group.

Modify polling engine settings by clicking Settings > All Settings, and then Polling Settings in the Thresholds & Polling group.

Use additional polling engines to balance polling in the Orion Platform

SolarWinds Orion Scalability Engines, including Additional Polling Engines and Additional Web Servers, extend the monitoring capacity of your SolarWinds installation.

Requirements and recommendations will vary from product to product. Go to your product's documentation page in the SolarWinds Success Center for more information.

See Requirements in the Scalability Engine Guidelines.

Pre-flight checklist

Before you install an Additional Polling Engine in your environment, be sure you complete the following actions:

- Be sure your product uses Orion Platform 2016.2 and later.

  To find out the Orion Platform version, log in to the Orion Web Console and see the Orion Platform version in the footer. If the version is 2016.1 and earlier, see Orion Bundle for additional servers.

- Install or upgrade the Main Polling Engine.

- Ensure product versions match between the Primary Polling Engine, all Additional Polling Engines, and Additional Web Servers. This includes the version of .NET. Find a version number listed in the footer of the Web Console. If your product versions do not match, you must upgrade before you can install Additional Polling Engines.

- Verify port requirements for your SolarWinds product.
Acquire a user name and password with administrative privileges to the Orion Web Console on your Main Polling Engine.

Be sure the Additional Polling Engine uses the same SQL database as the Main Polling Engine.

If you configured an alert with a Send Email action to trigger on a node monitored by an Additional Polling Engine, confirm that the Additional Polling Engine can access your SMTP server.

Add the IP address of your Additional Polling Engine to Windows Servers on the Security tab.

Make sure that the following options are set:

- Ensure that a case-sensitive community name has been specified.
- Ensure that Accept SNMP packets from any host is selected OR ensure that the ipMonitor system is listed within the Accept SNMP packets from these hosts list.
- Ensure that your network devices allow SNMP access from the new polling engine. On Cisco devices, you can for example modify the Access Control List.

Port requirements for Additional Polling Engines

Additional Polling Engines have the same port requirements as Main Polling Engine. The following ports are the minimum required for an Additional Polling Engine to ensure them most basic functions.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Service/Process</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>161</td>
<td>UDP</td>
<td>SolarWinds Job Engine</td>
<td>Outbound</td>
<td>The port used for sending and receiving SNMP information.</td>
</tr>
<tr>
<td>162</td>
<td>UDP</td>
<td>SolarWinds Trap Service</td>
<td>Inbound</td>
<td>The port used for receiving trap messages.</td>
</tr>
<tr>
<td>1433</td>
<td>TCP</td>
<td>SolarWinds Collector Service</td>
<td>Outbound</td>
<td>The port used for communication between the APE and the Orion database.</td>
</tr>
<tr>
<td>1434</td>
<td>UDP</td>
<td>SQL Browse Service</td>
<td>Outbound</td>
<td>The port used for communication with the SQL Server Browser Service to determine how to communicate with certain non-standard SQL Server installations. Required only if your SQL Server is configured to use dynamic ports.</td>
</tr>
<tr>
<td>1801</td>
<td>TCP</td>
<td>Message Queuing WCF</td>
<td>Inbound</td>
<td>The port used for MSMQ messaging from the Orion Web Console to the Additional Polling Engine.</td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Service/Process</td>
<td>Direction</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>-------------------------------------</td>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>5671</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>Bidirectional</td>
<td>The port used for SSL-encrypted RabbitMQ messaging from the Orion Web Console to the Additional Polling Engine.</td>
</tr>
<tr>
<td>17777</td>
<td>TCP</td>
<td>SolarWinds Information Service</td>
<td>Bidirectional</td>
<td>The port used for communication between the Additional Polling Engine and the Orion Web Console.</td>
</tr>
</tbody>
</table>

**Install an Additional Polling Engine**

1. Click Settings > All Settings > Polling Engines.
2. Click Download Installer Now.
3. Run the installer on the computer you want to use as your additional polling engine or website.
4. Enter the main Orion server credentials.
5. Choose either Additional Polling Engine or Additional Website. If you want to install a backup server for High Availability, view [SolarWinds High Availability requirements](#) first. The packages are downloaded from the main Orion server.
6. Follow the onscreen instructions to complete your installation and configuration.

The Additional Polling Engine or Additional Web Server is installed, together with all hotfixes for products released later than September 2016.

> For example, when installing or upgrading to SAM 6.3 and IPAM 4.3.2, any hotfixes for SAM 6.3 are installed. You must install the hotfix for IPAM manually.

Repeat installing on all Additional Polling Engines and then on all Additional Web Servers in your environment.

Activate the Additional Polling Engine licenses.

**Activate Additional Polling Engine licenses**

1. In the Orion Web Console, click Settings > All Settings > License Manager.
2. Locate the license in the License Manager, click Activate, and complete the activation.

   The Additional Polling Engine license is activated. Review the polling engine it is assigned to, and re-assign the license if necessary.

When finished, specify nodes to be polled by the Additional Polling Engine.
Use an Additional Web Server

With an Additional Web Server, you can access the Orion Web Console remotely, from a location other than your primary Orion server.

Requirements

- A matching version of Additional Web Server and your product installed on the main polling engine
- 64-bit operating system:
  - Windows Server 2019
  - Windows Server 2016
- Minimum hardware requirements
  - CPU speed: Quad-core processor, 2.5 GHz or better
  - Hard drive space: 10 GB minimum
  - Memory: 6 GB minimum, 12 GB recommended

A higher number of concurrent users may change the requirements.

- Enabled TLS 1.2 for the RabbitMQ messaging

Port requirements

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Service/Process</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>World Wide Web Publishing Service</td>
<td>Inbound</td>
<td>Default additional web server port. Open the port to enable communication from your computers to the Orion Web Console. If you specify any port other than 80, you must include that port in the URL used to access the web console. For example, if you specify an IP address of 192.168.0.3 and port 8080, the URL used to access the web console is <a href="http://192.168.0.3:8080">http://192.168.0.3:8080</a>.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>IIS</td>
<td>Inbound</td>
<td>The default port for https binding.</td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Service/Process</td>
<td>Direction</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>----------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>1433</td>
<td>TCP</td>
<td>SolarWinds Information Service</td>
<td>Outbound</td>
<td>The port used for communication between the SolarWinds server and the SQL Server. Open the port from your Orion Web Console to the SQL Server.</td>
</tr>
<tr>
<td>1801</td>
<td>TCP</td>
<td>Message queuing</td>
<td>Outbound</td>
<td>The port used for MSMQ messaging from the Additional Web Server to the Main Polling Engine.</td>
</tr>
<tr>
<td>5671</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>Outbound</td>
<td>The port used for SSL-encrypted RabbitMQ messaging from the Additional Web Server to the Main Polling Engine.</td>
</tr>
<tr>
<td>17777</td>
<td>TCP</td>
<td>SolarWinds Information Service</td>
<td>Outbound</td>
<td>Orion module traffic. Open the port to enable communication from your polling engine to the web server, and from the web server to your polling engine.</td>
</tr>
</tbody>
</table>

Before you begin, prepare:

- Hostname or IP address of your main polling engine
- Orion Web Console user name and password with administrative rights
- To use SQL authentication, prepare the SQL server credentials
- SQL database name

Download and install an Additional Web Server

1. In the main Orion Web Console, click Settings > All Settings > Web Console Settings.
2. Click Download Installer Now.
3. Run the installer on the computer you want to use as your Additional Web Server.
4. Enter the main Orion server Orion server credentials.
5. Choose Additional Website.
   The packages are downloaded from the main Orion server.
6. Follow the onscreen instructions to complete your installation.
Configure the Additional Web Server

1. If the Configuration Wizard does not start automatically, click Start > All Programs > SolarWinds Orion > Configuration and Auto-Discovery > Configuration Wizard.
2. Click Next on the Welcome tab of the Configuration Wizard.
3. Select or type the SQL Server used by your primary Orion server.
4. If you are using Windows NT Integrated Security, select Use Windows Authentication, and click Next.
5. If you are using a SQL Server login and password, complete the following steps:
   a. Select Use SQL Server Authentication.
   b. Provide your Login and Password, and click Next.
6. Select or type the Database Name that is connected to your Orion server, and click Next.
7. If a dialog appears that says that multiple polling engines have been detected, click OK to continue database upgrade/verification.
8. When the database structure validation completes, click Next.
9. Specify a SQL account User Name and Password for the polling engine and web site to use to access the database, and click Continue.
   
   i If you already have a SQL account, you can specify the credentials for that account.

10. To set up the web console, click Next on the Create Website tab, and then complete the following procedure:
   a. Specify the IP Address of the local server on which you are installing the new web-only interface.
   b. Specify the TCP Port through which you want to access the web console.
   
   i If you specify any port other than 80, you must specify that port in the URL that is used to access the web console. For example, if you specify an IP address of 192.168.0.3 and port 8080, your URL is http://192.168.0.3:8080.
   c. Specify the volume and folder in which you want to install the web console files, and then click Continue.
11. If you are asked to overwrite an existing website, click Yes.
12. When the new web console has been created, click Continue.

You can now use the additional Orion Web Console to access your Orion Platform product.

Activate your license

- To evaluate an Additional Web Server, just install it.
- To activate a production license for an Additional Web Server, log in to the Orion Web Console on your main polling engine, and activate the license.
Calculate node availability in the Orion Platform

Determine the availability under Orion Polling Settings > Calculations & Thresholds > Availability Calculation by using one of the following methods.

- To disregard node availability during maintenance, suspend collecting data or triggering alerts for the node.

Node Status

The default method is based on the historical up or down status of the selected node. The selected node is polled for status on the Default Node Poll Interval defined on the Orion Polling Settings view.

If the selected node responds to a ping within the default interval, the node is considered up, and a value of 100 is recorded in the Response Time view. If the node does not respond to a ping within the default interval, the node is considered down and a value of 0 is recorded in the Response Time view.

To calculate node availability over a selected time period, the sum of all Response Time table records for the selected node over the selected time period is divided by the selected time period. This provides an average availability over the selected time period.

Percent Packet Loss

This method is a more complicated calculation that bases the availability of a selected node on its packet loss percentage. The selected node is polled for status. If it responds within the Default Node Poll Interval defined on the Orion Polling Settings view, a value of 100 is averaged with the previous 10 availability records.

The result of the Percent Packet Loss calculation is a sliding-window average. To calculate node availability over a selected time period, the sum of all results in the Response Time table for the selected node over the selected time period is divided by the selected time period. This provides an average availability over time.

Assign credentials to virtual servers in the Orion Platform

If you did not provide the credentials within the Network Sonar Discovery, or when adding the node to the database, assign credentials based on the server vendor.

- VMware ESX or vCenter accounts used as credentials must have read-only permissions as a minimum.
Assign credentials to Hyper-V servers
1. Click Settings > All Settings > Manage Virtual Devices.
2. On the Virtualization Polling Settings page, select Hyper-V.
3. Select a Hyper-V server from the list, and click Edit Properties.
5. Click Test to verify the credential set, and click Submit.

Assign credentials to VMware servers
1. Click Settings > All Settings > Manage Virtual Devices.
2. On the Virtualization Polling Settings page, select VMware.
3. Select a VMware server from the list, and click Assign ESX Credential.
4. Choose an existing credential, or specify a new credential set.
5. Click Test to verify the credential set, and click Assign Credential to assign it to the VMware server.

Set the node warning level in the Orion Platform
A device may drop packets or fail to respond to a poll for many reasons. When the device fails to respond, the device status is changed from Up to Warning. You can specify how long a node can remain in the Warning status before it is marked as Down. During the interval specified, the service continually checks the node status.

Set the Node Warning Interval to a higher value to avoid false notifications.
1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Thresholds & Polling grouping, select Polling Settings.
4. Scroll down to Calculations & Thresholds, and enter a higher value for Node Warning Level.
5. Click Submit.

Delete polling engines in the Orion Platform
If there are polling engines in your SolarWinds environment that have no assigned monitored objects, you can delete them from the Polling Engine details view.
This method for deleting polling engines from your SolarWinds environment is only available for polling engines that no longer have objects assigned for monitoring.

- If you want to delete an existing polling engine to which monitored objects are currently assigned, use Node Management to reassign monitored objects to other polling engines, and delete the polling engine as indicated in this procedure.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. Click Polling Engines in the Details group.
4. Verify that the Elements listing for the polling engine you want to delete reports "0 elements assigned," and click Delete unused polling engine.
5. Click Yes, delete to confirm the deletion.
Administrative functions of the Orion Web Console in the Orion Platform

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

Orion Web Console administration in the Orion Platform

Users with Administrator rights can click Settings > All Settings to access the Main Settings and Administration page. The page presents a variety of tools to control the appearance and delivery of information to Orion Web Console users.

As more Orion Platform products are added, additional options will be displayed.

Getting Started

Before you can start monitoring your network, you must designate the network objects you want to monitor. This grouping provides direct links to discovery-related views so you can quickly and easily start monitoring your network:

- Discovery Central provides a centralized overview of the types and number of network objects you are monitoring with your Orion installation.
- Network Sonar Discovery starts the Network Sonar Discovery Wizard that automatically discovers devices across your entire network for monitoring.
- Add a Node opens the Add Node Wizard. See Add a single node for monitoring to the Orion Platform.

Node & Group Management

- Manage Nodes displays the Node Management page, where an Orion Web Console administrator can immediately add, view, and manage all network objects currently managed or monitored by your Orion Platform products.
- Manage Virtual Devices opens the Virtualization Polling Settings view where you can view both a list of currently monitored Hyper-V or VMware ESX Servers and a library of the VMware credentials used to monitor your ESX Servers. For more information, see Monitor virtual infrastructure.
- Manage Dependencies opens the Manage Dependencies view. Dependencies allow you to formalize dependent relationships between monitored objects based on network topology or priority to eliminate the potential for duplicated or redundant polling and alerting.
- Manage Agents allows you to create and manage your alerts. For more information, see View agent connections and status, update agents, or manage agents.
Manage Groups opens the Manage Groups view. To a greater degree than previously available with custom properties, groups enable you to logically organize your monitored network objects. For more information, see [Group monitored objects](#).

Manage Custom Properties allows you to create and manage custom properties that you can use within your Orion Platform products. For more information, see [Custom properties in the Orion Platform](#).

Manage World Map allows you to manage the nodes you want to display in the Worldwide Map resource.

Manage Pollers allows you to create new pollers or edit existing pollers to fit the needs of your unique devices. You can also import pollers created by your peers from THWACK.

Manage Hardware Sensors allows you to enable or disable monitoring hardware health sensors in the Orion Web Console. For more information, see [Monitor hardware health](#).

### Alerts & Reports

- Manage Alerts - create and manage web-based alerts. For more information, see [Use alerts to monitor your environment with the Orion Platform](#).
- Manage Reports - create and manage web-based reports. For more information, see [Create a web-based report in the Orion Platform](#).
- Manage SMTP Servers - add and manage SMTP servers used to send email notifications.
- Configure Default Send Email Action - configure the default SMTP server and email information used with the Send Email alert action.
- ServiceNow® Instances - integrate your Orion Platform product with a ServiceNow instance. For more information, see [Configure an Orion Platform product with ServiceNow](#).

### Product Specific Settings

- Virtualization Settings allow an Orion Web Console administrator to set up Virtualization Manager integration, configure virtualization, and view your License Summary.
- Web Console Settings allow an Orion Web Console administrator to customize the function and appearance of both the Orion Web Console and the charts that are displayed as resources in Orion Web Console views. For more information about configuring Orion Web Console and Chart Settings, see [Orion Web Console and chart settings for the Orion Platform](#).
- Agent Settings allow an Orion Web Console administrator to configure settings relevant for your agents. For more information, see [Modify global agent deployment and update settings](#).
- Proxy Settings allow an Orion Web Console administrator to configure a proxy server through which Orion can connect to THWACK and check for maintenance updates if Orion does not have internet access. For more information, see [Configure web proxy settings in the Orion Platform](#).

### Thresholds & Polling

- Polling Settings define the configuration of polling intervals, timeouts, statistics calculations, and database retention settings for your Orion polling engine. For more information about configuring Orion Polling Settings, see [Update polling settings in the Orion Platform](#).
Virtualization Thresholds allows you to set warning and critical thresholds specific for the Virtualization module.

Custom Poller Thresholds allow you to set warning and critical threshold levels for your custom pollers.

NPM Thresholds allow you to set warning and critical thresholds specific for the Network Performance Monitor.

Orion Thresholds allow you to configure warning and critical thresholds for nodes and volumes. These thresholds are used in all Orion modules.

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

Windows Credentials

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

User Accounts

- Manage Accounts allows you to manage user accounts, and specify management rights and limitations.
- Accounts List provides a table of existing accounts and appropriate details, such as assigned rights or the last login.

Views

- The Manage Views page enables administrators to add, edit, copy, or remove Orion Web Console views. See How custom views work in the Orion Platform.
- The Add New View page enables you to define new Orion Web Console views.
- The Created NOC Views provides the list of current Network Operations Center page, and enables you to add new NOC views.
- The Views by Device Type page allows administrators to designate default views for network devices. See Specify views for device types in the Orion Platform.

Customize Navigation & Look

- Customize Menu Bars allows Orion Web Console administrators to configure the menu bars seen by individual users. See My Dashboards in the Orion Platform.
- Color Scheme allows administrators to select a default color scheme for resource title bars. The color scheme selection takes effect immediately throughout the web console. See Change the Orion Web Console color scheme in the Orion Platform.
- External Websites allows Orion Web Console administrators to designate any external website as an Orion Web Console view, appearing in the Views toolbar. See Add external websites to the Orion Platform.
Details

Database Details
This is an information-only page that displays details about the SQL Server database currently used by your SolarWinds Orion installation, such as the version and configuration settings for both your Orion server and your database server, and the total number of monitored objects in the SolarWinds Orion database.

Polling Engines
This page shows the status and selected configuration information for each currently operational polling engine.

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

License Details
This is an information-only page that displays details about all Orion products that you currently have installed. This page also shows the version numbers of the Orion products you are running and the versions of associated DLLs.

License Manager
This link opens the web-based License Manager. Click the link to manage your Orion Platform licenses directly from the Orion Web Console.

View secure data in the Orion Platform
Sensitive network information, such as community strings, logins, and passwords, is not viewable in the Orion Web Console by default.

If you have secured your network, you can display secure data in the Orion Web Console.

1. Click Settings > All Settings in the menu bar.
2. In the Thresholds & Polling grouping, click Polling Settings.
3. Scroll down to the Calculations & Thresholds area, and select Allow Secure Data On Web (Advanced).

This setting does not affect the display of custom reports that you export to the web.

Handle counter rollovers in the Orion Platform
Specify a method that decides what happens if a polled value is less than the previous polled value.

Orion Platform products are capable of handling either 32-bit or 64-bit counters.
By default, counters are assumed to be 32-bit.

32-bit counters have a maximum value of $2^{32}$, or 4,294,967,296.
64-bit counters have a maximum value of $2^{64}$, or 18,446,744,073,709,551,616.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Thresholds & Polling grouping, click Polling Settings.
4. Scroll down to the Calculations & Thresholds area, and select the Counter Rollover method.
   - If you use 32-bit counters, select Method 1.
     This method detects a rollover, and calculates based on it.
     First, the method checks whether the device rebooted and reset its counters to 0. In this case, the last value is 0.
     When it is a real rollover, we take the maximum value of the 32 or 64 bit number, take the difference between the maximum and the last polled value, and add it to the current polled value: $(\text{MaxValue} - \text{LastPolledValue}) + \text{CurrentPolledValue}$
   - If you use 64-bit counters, select Method 2.
     When a rollover is detected, Orion drops the poll and takes a new sample within 20 seconds.
     The new data point is stored, throwing the first data point away.
     In memory, we have the value from the previous poll (A) and the LastPolledValue (B). Because $B < A$, we detect counter rollover. Orion drops the last poll and does a fast poll within 20 seconds. The value stored in the database is calculated as $C - B$.

Orion fully supports the use of 64-bit counters, but these counters can exhibit erratic behavior in some implementations. If you notice peculiar results, disable the use of 64-bit counters for the problem device, and contact the device manufacturer.

The rollover method is changed for your polled nodes.

**Configure web proxy settings in the Orion Platform**

If your SolarWinds Orion server does not have Internet access, you can use a proxy server to allow the Orion server to connect to certain pages and websites. Use a proxy server to:

- Access the THWACK community
- Access the product blog
- Check for maintenance updates
- Access an alerting instance you integrated with your SolarWinds Orion server. See Alert Integrations in the Orion Platform.
To configure web proxy settings:

1. In the Orion Web Console, click Settings > All Settings > Product specific settings > Proxy Settings.
2. Select Use the following settings, and specify the IP address and port number of the proxy server.
3. If the proxy server requires authentication, select the check box, and specify the user name and password.
4. Enter a URL, and click Test connection to verify that you can reach the destination address through the proxy.
5. Click Save.

Maintain the SolarWinds Orion database in the Orion Platform

All Orion Platform products use a Microsoft SQL Server database to store Orion Web Console settings and collected network performance and configuration data.

There are two utilities that allow you to perform the most commonly required database tasks without having to access either the Microsoft SQL Server or its associated tools.

**Database Manager**

Add SQL servers to your Orion configuration, view database information, perform queries or edit database values. See [View database details and data in the Database Manager](#).

**Database Maintenance**

Summarize, clean, and compact your SolarWinds Orion database. See [Database maintenance in the Orion Platform](#).

Additional resources

Visit [SolarWinds Success Center](#) for more details and tips for maintaining a healthy SolarWinds Orion database, such as:

- [Best practices for managing your Orion database](#)
- [Migrate the Orion database](#)

View database details and data in the Database Manager

The Database Manager is used to add additional servers to your Orion configuration, perform queries, view database and table details, export data, and edit database values.

For more advanced database maintenance, SolarWinds recommends that you use the Server Management Studio provided with Microsoft SQL Server to back up, clear historical maintenance records, and perform other maintenance.

ℹ️ If you need to backup or restore a database, you should use the SQL Server Management Studio.
Database maintenance in the Orion Platform

Database maintenance is an automatic process that optimizes the size of your SolarWinds Orion database. During maintenance, the data collected for a certain period are aggregated and new statistical values, based on the aggregated data, are calculated. The data are discarded, and only the aggregated statistics are retained.

Database maintenance runs every day at a specified time. Depending on the data granularity and retention period, you may need to configure your database differently. Keep in mind that the more granularity and the longer the retention period, the larger the database.

Check the database size

1. Start the Database Manager in the SolarWinds Orion > Advanced Features program folder.
2. Add your database server and expand it.
3. Right-click your SolarWinds Orion database, and select Database Details.
The database size is displayed in the Properties tab.

Specify the time to run database maintenance

Make sure database maintenance runs after business hours.

1. Log in to the Orion Web Console using an administrator account.
2. Click Settings > All Settings.
3. Click Polling Settings in the Thresholds & Polling grouping.
4. Scroll down to Database Settings, and enter an Archive Time.

5. Click Submit.

Adjust retention periods

Data for collected statistics are retained for a specified time. Shorten the retention periods to save storage space in your database.

1. Log in to the Orion Web Console using an administrator account.
2. Click Settings > All Settings.
3. Click Polling Settings in the Thresholds & Polling grouping.
4. Scroll down to Database Settings, and adjust the retention periods.

The detailed data are retained for the specified period and summarized into hourly data. Hourly data are then summarized into daily statistics, and daily statistics are discarded after the specified time.

The shorter the retention period, the greater effect the setting has on the database size.

<table>
<thead>
<tr>
<th>DATABASE STATISTIC</th>
<th>RETENTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detailed Statistics</td>
<td>7 days</td>
</tr>
<tr>
<td>Hourly Statistics</td>
<td>30 days</td>
</tr>
<tr>
<td>Daily Statistics</td>
<td>365 days</td>
</tr>
</tbody>
</table>

You can also adjust retention periods for other statistics.

Changing the detailed retention period has the greatest effect on the database size.

Assuming a 10-minute polling interval, one new entry is added to the database for each monitored object every 10 minutes. That means 144 new entries a day are added for each monitored object during the Detailed Statistics Retention period. In the Daily Statistics Retention period, only one entry a day is added to the database for each object.

5. Click Submit to commit the changes.

Launch database maintenance manually

2. Click Start.

Security enhancements and exceptions for SolarWinds Orion Platform products

By default, SolarWinds Orion products use HTTP instead of HTTPS. You can increase the security of your data by using SSL or SSL and FIPS.

- Configure the Orion Web Console to use SSL
- Enable FIPS for Orion Platform products

For best performance, SolarWinds also recommends creating an antivirus directory exclusion for the SolarWinds install folder.

Configure the Orion Web Console to use SSL

SolarWinds Orion products supports binding Secure Sockets Layer (SSL) certificates to your Orion server port to enable secure communications with the Orion Web Console.

⚠️ Due to security concerns, SolarWinds recommends that you disable SSL v3.0 and earlier.
Select the Enable HTTPS option in the Configuration Wizard to bind an existing certificate to your Orion server port or create a certificate for binding. The process is automatic when this option is selected.

To configure your website bindings manually or leave your current website configuration as it is, select Skip website binding in the Configuration Wizard.

- SolarWinds recommends that you install a certificate from a certificate authority before adding the bindings to the website, and that you enable the certificate auto enrollment group policy to prevent the certificate from generating browser errors.
- This information refers to SolarWinds products running on Orion Platform version 2017.1.

Use a previously installed SSL certificate

1. Select Enable HTTPS.
2. Choose the certificate you want to use. Certificates with a green check mark are least likely to generate browser warnings.
3. Complete the Configuration Wizard.

The Configuration Wizard enables the Orion Web Console to use SSL for the specified port, adds the website binding to the Orion Web Console, and forces the website to use HTTPS by default.

After the Configuration Wizard is finished, the Orion Web Console opens using HTTPS. If you used a certificate with a green check mark next to it, there should be no browser warnings. If you used a certificate with a yellow warning sign next to it, you may have a browser warning.
Generate a self-signed certificate

You can generate a self-signed certificate directly in the Configuration Wizard.

1. Select Enable HTTPS.
2. Scroll to the bottom of the list and select Generate Self-Signed Certificate.

3. Complete the Configuration Wizard.

A self-signed certificate is issued to the machine host name or fully qualified domain name (FQDN) when the computer is part of a domain, and the certificate is added to the trusted certificate store. After the Configuration Wizard is finished, the Orion Web Console opens using HTTPS.

The certificate authority for self-signed certificates is the computer hosting your Orion server. Depending on your security and group policy settings, the Orion Web Console may generate browser errors because the certificate was not issued by a known certificate authority.
Use SSL after you install an Orion product

You can still use the Configuration Wizard to add the binding to your Orion Web Console after you have installed a SolarWinds Orion product.

⚠️ You must install an SSL certificate on the Orion server before performing the following steps.

1. Log in to your Orion server as an administrator.
2. Run the Configuration Wizard from the Start menu.
3. Select Configure the website, and click Next.
4. Clear the Skip website binding option.
5. Select Enable HTTPS.
6. Choose the installed certificate. If the certificate does not show in the list, review how certificates are categorized.

Certificate categories

Green ✅

The certificate is valid and should not generate browser warnings. Certificates are marked green if they meet one or more of the following criteria:

- The certificate's Issued To (CN) field fully matches the server's FQDN
- The certificate's Issued To (CN) field partially matches the server's FQDN using wildcards
- The certificate's Issued To (CN) field partially matches the server's FQDN
The certificate can be used, but may generate browser warnings. Certificates are marked yellow if they meet one of the following criteria, ordered from least likely to most likely to generate browser errors:

- Self-signed certificates where the Issued To and Issued By fields match the server’s FQDN
- Certificates issued to the IP address instead of the host name or FQDN
- Certificates issued to a computer with different hostname

Invalid certificates

Some certificates are not valid. Client certificates or certificates that have expired or use an untrusted certificate authority are invalid and do not display on the list.

What is the Skip website bindings option?

Use the Skip website binding option in the following circumstances:

- You have already set up SSL/HTTPS on your Orion server
- You do not want to reconfigure the Orion Web Console binding
- You want to configure multiple Orion Web Console bindings manually with the IIS Manager

The Configuration Wizard maintains any existing SSL configuration settings with this option.

For previous versions of the product (products running on Orion Platform version 2016.2 and earlier), if this option is not selected and you have set up SSL/HTTPS, the Configuration Wizard may reconfigure your existing HTTP bindings and clear any SSL configuration settings.

Enable FIPS for Orion Platform products

You can run your Orion Platform product in FIPS-compliant (Federal Information Processing Standard) mode to comply with computer security and interoperability standards used by non-military US government agencies and contractors.

- If FIPS compliance is required, SolarWinds recommends that you enable FIPS as part of a fresh install instead of as part of an upgrade.
- Before you enable FIPS ensure that the hardware is FIPS-compliant. See the Microsoft Support knowledge base for more information.
- Not all Orion Platform products are FIPS-compliant. SolarWinds recommends that you install all FIPS-compliant SolarWinds software on FIPS-compliant servers and maintain all non-compliant SolarWinds software on non-compliant servers.

1. Configure the Orion server for FIPS compliance.
2. Start the SolarWinds FIPS 140-2 Manager (SolarWinds.FipsManager.exe).

By default, SolarWinds.FipsManager.exe is located in the C:\Program Files (x86)\SolarWinds\Orion folder.
3. Read the welcome text, and click Next.

The SolarWinds FIPS 140-2 Manager confirms that the current configuration of your SolarWinds products is FIPS-compliant.

- If an installed product is not FIPS-compliant, click Close, remove any non-compliant Orion Platform products from the FIPS-compliant server, and run the FIPS 140-2 Manager again.
- If FIPS 140-2 is disabled, select Enable FIPS 140-2, and click Next.
- If the FIPS Manager provides a list of objects or saved network discovery definitions that are not FIPS-enabled, complete the following steps.

   "To refresh the list of non-compliant objects after editing the credentials, restart the FIPS 140-2 Manager."

   - Click the non-compliant monitored node, and edit its Polling Method to be FIPS-compliant.
     a. Select SNMPv3 as the SNMP Version.
     b. Select FIPS-compliant Authentication and Privacy/Encryption methods, and provide the passwords.
     c. Click Submit.
   - Click the non-compliant network discovery, and edit SNMP credentials to be FIPS-compliant.
     a. Confirm that all SNMP credentials are SNMPv3. Delete or edit any credentials that are not FIPS-compliant SNMPv3.
     b. Confirm that all SNMP credentials use FIPS-compliant Authentication and Privacy/Encryption methods, and provide the passwords.
     c. Complete the Network Sonar Wizard using the updated credentials.

4. Click Restart now to restart all relevant SolarWinds services.

While the software is FIPS-compliant, you must choose to use FIPS-compliant polling methods, such as SNMPv3, to monitor and discover nodes.

### FIPS-Compliant Methods for SNMPv3

<table>
<thead>
<tr>
<th>Authentication</th>
<th>SHA1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy or encryption</td>
<td>AES128, AES192, AES256</td>
</tr>
</tbody>
</table>

### Encrypt database connections with SSL

When you configure the database settings in the Configuration wizard, you can choose to encrypt the network traffic between the Orion server and the SQL Server using the SSL certificate on the SQL Server.
If you are running NTA 4.4 and later, you can also encrypt the network traffic between the Orion server and the NTA Flow Storage database. When configuring the NTA Flow Storage in the Configuration wizard, select Encrypt connections with SSL.

This option does not apply to legacy desktop applications, such as Orion Report Writer. To encrypt database connections to and from those applications, the SQL Server must require encryption.

This option in the Configuration wizard requires a provisioned SSL certificate on the SQL Server. You do not need to force the SQL Server to require encryption.

The SSL certificate is trusted automatically.

**Update polling settings in the Orion Platform**

Click Settings > All Settings, and in the Thresholds & Polling group, click Polling Settings to configure your polling engine.

Depending on the Orion Platform products you have installed, additional polling settings may be available. See your SolarWinds Orion Administrator Guide for more information about the settings.

**Configure polling interval settings in the Orion Platform**

You can improve your Orion server performance by entering longer polling intervals.

Configure how frequently the polling engine requests information from devices.

See [Configure polling interval setting in the online help](#) for more information.

**Available options**
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Node Poll Interval</td>
<td>120 seconds</td>
<td>The interval for polling the status and response time of monitored devices.</td>
</tr>
<tr>
<td>Default Interface Poll Interval</td>
<td>120 seconds</td>
<td>The interval for polling the status of monitored interfaces.</td>
</tr>
<tr>
<td>Default Volume Poll Interval</td>
<td>120 seconds</td>
<td>The interval for polling the status of volumes.</td>
</tr>
<tr>
<td>Default Rediscovery Interval</td>
<td>30 minutes</td>
<td>The interval for polling the entire network to detect any re-indexed interfaces. Monitored network devices are also checked for IOS upgrades or EnergyWise support. Rediscovery scans your network for changes to your monitored nodes. If you want to discover changes to your environment, schedule a network discovery to occur on a periodic basis and check the scheduled discovery results. The minimum rediscovery interval is five minutes (in earlier versions, the interval was one minute). You cannot submit polling interval settings if the default rediscovery interval is not set to at least five minutes.</td>
</tr>
<tr>
<td>Default Asset Inventory Poll Interval</td>
<td>1 day</td>
<td>The interval for checking asset inventory. Relevant for SAM and SCM.</td>
</tr>
<tr>
<td>Lock Custom Values</td>
<td>Selected</td>
<td>Select this option to keep any customized status polling interval settings.</td>
</tr>
<tr>
<td>Re-Apply Polling Intervals</td>
<td>Button enabled</td>
<td>Click Re-Apply Polling Intervals to apply the settings specified in this section to all objects in the database. Click Submit at the bottom of the page to use the current settings for new objects.</td>
</tr>
</tbody>
</table>

1. If you leave the page without submitting the changes, your settings will be applied to objects in the database, but will not be saved as default. For objects added to the database in the future, the default settings will be used. Not submitting the changes can result in different settings for objects that are already in the database, and different settings for newly added objects.
Timeout information

Polling intervals set the amount of time between polling. When the time passes (in seconds), polling starts by contacting monitored nodes. If polling starts and does not receive a response within the timeout interval, an unknown response enters and displays. The timeout amount sets the amount of time Orion products wait to process and receive responses. Depending on the processing load, you may need to extend the timeout.

Configure polling statistics intervals in the Orion Platform

Configure the default polling intervals for device statistics. To apply poller settings, click Re-Apply Polling Statistic Intervals.

Default Node Topology Poll Interval

Configure the interval for polling topology data of monitored devices. By default, this interval is 30 minutes. To reduce network load, increase this polling interval.

Default Node Statistics Poll Interval

Configure the interval for polling performance statistics of monitored devices. By default, this interval is 10 minutes.

Default Interface Statistics Poll Interval

Configure the interval for polling performance statistics of monitored interfaces. By default, this interval is 9 minutes.

Default Volume Statistics Poll Interval

Configure the interval for polling the performance statistics of volumes. By default, this interval is 15 minutes.

Configure the dynamic IP address and hostname resolution in the Orion Platform

Select the default IP address version (IPv4 or IPv6) to use when resolving the address of monitored dual stack devices.

A dual stack device is capable of providing IP addresses in both IPv4 and IPv6 formats.

To monitor IPv6 devices, enable IPv6 on the Orion server.

Immediately change the settings by clicking Re-Apply Resolution Preference.

Configure Database Settings in the Orion Platform

Configure the time of day when the database maintenance runs, and how long data are retained in the SolarWinds Orion database.
Shortening retention periods can improve your database performance. However, if you increase retention periods, it can cause excessive overhead on your SQL server and introduce issues such as:

- Increased I/O
- Increased table sizes
- Database maintenance issues where nightly maintenance fails to complete or runs indefinitely
- Web performance issues
- Chart loading issues

Consider your SQL environment resources, such as disk space and hardware configuration before you change the retention periods. See this SolarWinds KB article for database best practices.

It can take more than 10 minutes to propagate some changes to SolarWinds Orion database settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive Time</td>
<td>2:15 am</td>
<td>Configure the time of day when the maintenance of the SolarWinds Orion database runs.</td>
</tr>
<tr>
<td>Index Defragmentation</td>
<td>Selected</td>
<td>Select the box to enable database index defragmentation. Defragmenting the database helps troubleshoot performance issues.</td>
</tr>
<tr>
<td>Timeout for Index Defragmentation</td>
<td>3600 seconds</td>
<td>Set a timeout for index defragmentation.</td>
</tr>
<tr>
<td>Enable/disable auto reset logging levels to logging defaults</td>
<td>Selected</td>
<td>Select to automatically reset logging levels to defaults during Maintenance.</td>
</tr>
<tr>
<td>Auditing Trails Retention</td>
<td>365 days</td>
<td>Specify the number of days until the audit trails statistics are deleted from the database.</td>
</tr>
<tr>
<td>Detailed Statistics Retention</td>
<td>7 days</td>
<td>Specify the time period in which all statistics collected in the SolarWinds Orion database are summarized into hourly statistics.</td>
</tr>
<tr>
<td>Hourly Statistics Retention</td>
<td>30 days</td>
<td>Specify the time period in which all statistics collected in the SolarWinds Orion database are summarized into daily statistics.</td>
</tr>
<tr>
<td>Daily Statistics Retention</td>
<td>365 days</td>
<td>Specify how long daily statistics are kept in the SolarWinds Orion database. After the specified time, the daily statistics are deleted.</td>
</tr>
<tr>
<td>Container Detailed Statistics Retention</td>
<td>7 days</td>
<td>Specify when group statistics are summarized into hourly statistics.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Container Hourly Statistics Retention</td>
<td>30 days</td>
<td>Specify when hourly group statistics are summarized into daily statistics.</td>
</tr>
<tr>
<td>Container Daily Statistics Retention</td>
<td>365 days</td>
<td>Specify how long group statistics are kept in the SolarWinds Orion database.</td>
</tr>
<tr>
<td>Baseline Data Collection Duration</td>
<td>7 days</td>
<td>Specify the number of days that are included into the baseline.</td>
</tr>
<tr>
<td>Delete Stale Interfaces</td>
<td>Not selected</td>
<td>If no new data is polled for an interface for a specified time and the Orion Platform cannot remap the interface, delete the interface and all data connected with it. Stale interfaces are deleted one hour before the scheduled database maintenance.</td>
</tr>
<tr>
<td>Stale Interface Retention</td>
<td>7 days</td>
<td>Specify the time interval (in days) after which stale interfaces are deleted from the SolarWinds Orion database.</td>
</tr>
<tr>
<td>Automatically Remove Unknown Volumes</td>
<td>Not selected</td>
<td>Enable to automatically remove 'unknown' volumes.</td>
</tr>
<tr>
<td>Remove Unknown Volumes After</td>
<td>7 days</td>
<td>Remove volumes which have no statistical data and have been 'unknown' for longer than configured days.</td>
</tr>
<tr>
<td>Detailed Wireless Statistics Retention</td>
<td>3 days</td>
<td>Specify the number of days until the detailed wireless statistics in the SolarWinds Orion database are summarized into hourly statistics.</td>
</tr>
<tr>
<td>Hourly Wireless Statistics Retention</td>
<td>14 days</td>
<td>Specify the number of days until the hourly wireless statistics are summarized into daily statistics.</td>
</tr>
<tr>
<td>Daily Wireless Statistics Retention</td>
<td>180 days</td>
<td>Specify the number of days until the daily wireless statistics are deleted from the database.</td>
</tr>
<tr>
<td>Events Retention</td>
<td>30 days</td>
<td>Specify the number of days until the all network events data are deleted from the SolarWinds Orion database.</td>
</tr>
<tr>
<td>Syslog Messages Retention</td>
<td>7 days</td>
<td>Specify the number of days until all data related to received Syslog messages are deleted from the SolarWinds Orion database.</td>
</tr>
<tr>
<td>Trap Messages Retention</td>
<td>7 days</td>
<td>Specify the number of days until all data related to received trap messages are deleted from the SolarWinds Orion database.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Max Alert Execution Time</td>
<td>60 seconds</td>
<td>Specify the time period until the alerts are disabled if they are not executed successfully. If the defined alert condition persists, Orion continues trying to execute the alert.</td>
</tr>
<tr>
<td>Alert Acknowledge URL Text</td>
<td>Click here to acknowledge this alert</td>
<td>Provide text that is displayed when alerts are available for acknowledgment over the web. When viewing an alert, click the text to acknowledge the alert.</td>
</tr>
<tr>
<td>Allow alert actions for unmanaged objects</td>
<td>Not selected</td>
<td>Select this option if you want the SolarWinds Alerting Engine to execute configured alert actions for unmanaged objects.</td>
</tr>
<tr>
<td>Discovery Retention</td>
<td>60 days</td>
<td>Specify the number of days until all network discovery profiles are deleted from the SolarWinds Orion database. The retention starts when a discovery is first defined.</td>
</tr>
<tr>
<td>Downtime History Retention</td>
<td>7 days</td>
<td>Specify the number of days until the downtime history is deleted from the database.</td>
</tr>
</tbody>
</table>

Configure network settings for the Orion Platform

Configure the settings related to ICMP and SNMP requests.

**ICMP Timeout**

Configure the period after which all ICMP (ping) requests made by the poller time out if a response is not received. By default, this period is 2500 ms.

**ICMP Data**

Specify the text that is included in all ICMP packets sent by the poller.

**SNMP Timeout**

Configure the period after which all SNMP requests made by the poller time out if a response is not received. By default, this period is 2500 ms.

**SNMP Retries**

Configure the number of times the poller retries the request if there is no response to an SNMP poll request within the SNMP timeout period. By default, this value is 2.
UCS API Timeout

Configure the period after which all Cisco UCS API requests made by the poller time out if a response is not received. By default, this period is 240 seconds.

Perform reverse DNS lookup

Select this option if you want the Orion server to perform reverse DNS lookups on monitored DHCP nodes. By default, reverse DNS lookup for DHCP nodes is enabled.

Configure calculations and threshold settings in the Orion Platform

The following settings designate methods for calculating availability and transmission rate baselines, selecting the node warning level and counter type, and indicating security preferences for community strings and other potentially sensitive information in the web console.

Availability Calculation (advanced)

Configure the type of calculation that is performed to determine device availability.

Baseline Calculation (advanced)

Enable this option to ensure that baselines for the transmission rates of the elements of your network are calculated upon startup. This baseline is used as a starting point for any comparison statistics.

Enable Auto Dependencies

Enable this option to ensure that the SolarWinds Orion server collates topology information from networked devices and creates dependency links between devices.

Allow Secure Data on Web (advanced)

Select this option if your network is secure and you want to allow users to view community strings and other potentially sensitive information in the Orion Web Console. Sensitive information about your network is not available in the Orion Web Console.

This setting does not affect the display of custom reports that you export to the web.

Node Warning Level

Configure the period after which devices that do not respond to polling are displayed as Down in the Orion Web Console. By default, this period is 120 seconds.

Counter Rollover

Specify a method that decides what happens if a polled value is less than the previous polled value.

Default Assigned IP Address

Specify the node IP address that is recorded if DNS resolution fails for a monitored node. If you leave this field blank, no IP address will be stored.
Disable HTML Encoding for Polled Data

Specify if you want to HTML-encode polled data. HTML encoding provides added security for polled data in the Orion Web Console.
Manage the Orion Web Console for your Orion Platform

The Orion Web Console is an integral part of the Orion Platform products and can be accessed from virtually any computer connected to the Internet.

To customize the Orion Web Console, you need administrator rights.

You can customize the Orion Web Console for multiple users, update polling settings and thresholds, and store individually customized views as user profiles.

Log in to the Orion Web Console

1. Launch the Orion Web Console using either of the following methods:
   - Start Orion Web Console in your SolarWinds Orion program folder.
   - Launch a browser and enter http://ip_address or http://hostname, where ip_address is the IP address of your Orion server, or where hostname is the domain name of your Orion server.

2. Enter the user name and password, and click Login.
   
   See Configure automatic login for details about login options.

Customize the Manage Nodes / Entities view in the Orion Platform

Check out the Manage Entities page with flexible filters and interface improvements introduced in Orion Platform 2017.3.

The Manage Nodes view is the primary view for device management in the Orion Web Console. Nodes and interfaces can also be described as "entities”.

Select the node or interface to manage, and use the available management actions in the toolbar.

To manage more devices at the same time, select the devices.

To manage all monitored devices, select the box to the left of the Name column.
Available actions

The Manage Nodes / Manage Entities views have dynamic menu actions that depend on the following factors:

- Selected entities
- Installed Orion Platform products

Actions for Orion Platform products

- Add a single node for monitoring to the Orion Platform
- Open the Custom Property Editor to see custom properties for monitored entities, add custom properties, or edit values for custom properties.
- Edit node properties
- View the resources and statistics monitored on a node
- Suspend data collection or alerts for nodes in Maintenance Mode
- Change the polling method for a node
- Poll and rediscover devices immediately
- Delete devices from the database

Find devices on the Manage Nodes page

To find the node or interface to manage, search or filter the objects on the Manage Nodes page.

- To find nodes, enter a search string into the Search field above the results table, and click Search.
  
  Orion Platform only searches for the string on properties displayed in the table.

  To add a property, click >> at the far right of the title row of the table, and select system or custom properties.

  To find interfaces, select Interfaces next to the Search field.

  To see monitored interfaces on a node, expand the node.

  To filter devices, select a Group By option in the left section, and select a group. Nodes display in the results table.

  The Group By list includes custom properties.

Manage Entities

Orion Platform 2017.3 introduced the Manage Entities page that provides a list of entities monitored by your Orion Platform products.

To switch to its predecessor, Manage Nodes page, click Commands > Switch Back to Legacy Page.
Find entities on the Manage Entities page

To find the entity to manage, use the search box or filter the entities.

To search for a string in entity names, enter a string to the search box. The Manage Entities page lists entities with the string included in their name.

To filter by a property, expand the property in the Filter Results pane, and select the values the results should have.

The Manage Entities page displays the entities that have the selected values for the properties. Available filters provide options you can use to further refine the results.

**Add properties to filter by**

To refine property filters, add the property to the Filter Results pane.

1. Click Edit filter properties.
2. Select and add the properties.
The Filter Results pane displays the properties with at least one value in the database. You can expand the property and select values to filter by.

Customize information on Manage Entities

Add or remove custom or system properties displayed for entities on the Manage Entities view.

1. On the Manage Entities view, click More > Edit Row Properties in the menu.
2. Select properties to display on the Manage Entities view.

   Use the drop-down list to display available Custom or System properties. Custom properties are displayed next to the Entity name, and System properties below the Entity Name.

3. Click Save Changes to confirm your changes.

Displayed properties and available filters adjust to your selection.
View related entities on the node

Related entities have a relationship to the parent entity. For example, entities related to nodes are interfaces monitored on the node. By default, the interfaces are grouped by Type.

1. Click the arrow at the end of a node line. The Related Entities pane opens.

2. Expand interface groups to see monitored interfaces on the node.
   - Hover over an interface to see an overview.
   - Click an interface to go to the Interface Details view.
   - Click the close icon next to a node to hide interfaces on the node from the Related Entities pane.

Entities with muted alerts

Click the muted icon to resume muted alerts or cancel the planned period of suspended alerts.

Thresholds in the Orion Platform

Many Orion Web Console resources can display warning and critical states when a monitored value on a device exceeds a threshold. Orion Platform products come with predefined static thresholds for monitored statistics, but you can override these and customize them for each object.

You can use thresholds to define trigger conditions for alerts.

Orion Platform products provide 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, use a static threshold or a dynamic baseline threshold.

- **A Static threshold** is a constant value that you set for a 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.

- **A Dynamic baseline threshold** uses deviations. Data for a statistic are collected for a week, and then used to calculate the 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).

The way baselines are calculated depends on installed Orion Platform products. In SAM, baselines are calculated once, after data has been collected for a week. You can recalculate baselines on demand. Other Orion Platform products use dynamic moving baselines which are constantly adjusting.

### Set general thresholds in the Orion Platform

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

> Thresholds set on specific objects are not affected by changes made to general thresholds.

1. Click Settings > All Settings in the menu bar.
2. In the Thresholds and Polling grouping, click Orion Thresholds.
3. Enter values for Critical Level or Warning Level for selected thresholds.

<table>
<thead>
<tr>
<th>PERCENT PACKET LOSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Level</td>
</tr>
<tr>
<td>Warning Level</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RESPONSE TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Level</td>
</tr>
<tr>
<td>Warning Level</td>
</tr>
</tbody>
</table>

4. Click Submit.

Monitored thresholds are changed on a global level.

> To access thresholds for virtual objects, go to Settings, and click Virtualization Thresholds in the Thresholds & Polling grouping.
Disable thresholds

Starting with Orion Platform 2019.2, you can disable critical or warning thresholds in your Orion Platform.

1. Click Settings > All Settings in the menu bar.
2. In the Thresholds and Polling grouping, click Orion Thresholds.
3. Clear the box for the critical or warning thresholds you want to disable in your system.

After the next poll, the disabled thresholds will not be reflected in your Orion Platform.

You can override this global setting for individual nodes.

Customize thresholds for single objects in the Orion Platform

Get notified when polled values on critical devices reach different values than on other objects. For example, set warning and critical thresholds for CPU load on critical devices to a lower percentage than the default settings.

1. Click Settings > All Settings in the menu bar.
2. In the Node & Group Management grouping, click Manage Nodes.
3. Find the node or interface for which you want to set custom thresholds.
4. Select the object, and click Edit Properties.
5. Scroll down to Alerting Thresholds, select the Override Orion General Thresholds check box by the metric, and provide values for Warning and Critical thresholds.

Starting with Orion Platform 2019.2, you can use sustained thresholds and specify how long the condition must be true for the threshold to be exceeded.

![Node Thresholds](image)

If you want to use dynamic thresholds, click Use Dynamic Baseline Thresholds. The integer values will be replaced with macros for dynamic thresholds ($\text{USE_BASELINEWARNING}$, $\text{USE_BASELINE_CRITICAL}$).

When the polled values for the selected metric cross the thresholds on the object, the object will be highlighted, and appropriate alerts triggered.

To customize thresholds for virtual objects, go to Settings, and click Manage Virtual Devices in the Node & Group Management grouping. Select a VMware object, click Edit Thresholds, and change the thresholds.
Baselines and baseline calculations in the Orion Platform

With baselines, you can define what is normal for individual monitored objects based on polled data. By default, the baseline calculator uses the last seven days of collected statistic values to determine what is normal for individual monitored objects. The baseline is calculated using mean and standard deviation.

You can use baselines to detect deviations from the average polled values and be alerted on the deviations. Baselines can be displayed on some charts in the Orion Web Console.

What data is subject to statistical baseline calculation?

<table>
<thead>
<tr>
<th>Nodes</th>
<th>Interfaces</th>
<th>Volumes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Load</td>
<td>Received (Incoming) Errors &amp; Discards</td>
<td>Percent Disk Usage</td>
</tr>
<tr>
<td>Percent Memory Used</td>
<td>Transmitted (Outgoing) Errors &amp; Discards</td>
<td></td>
</tr>
<tr>
<td>Response Time</td>
<td>Received (Incoming) Percent Utilization</td>
<td></td>
</tr>
<tr>
<td>Percent Loss</td>
<td>Transmitted (Outgoing) Percent Utilization</td>
<td></td>
</tr>
</tbody>
</table>

Use mean and standard deviations as thresholds

To get notified when polled values for a node or interface are outside the range specified by mean and standard deviations, set dynamic baseline thresholds.

If you have a contextual understanding of the metric you are monitoring, consider defining the thresholds manually. Baselines are calculated values and do not know what is crucial for your environment.

1. Click Settings > Manage Nodes.
2. Locate and select the node or interface, and click Edit Properties.
3. Scroll down to Alerting Thresholds, select Override Orion General Thresholds, click Use Dynamic Baseline Thresholds.

Before you use calculated deviations as thresholds, click Latest Baseline Details to review the latest baseline statistics.

Mean and standard deviations will now be used as alerting thresholds for the node or interface.

Customize how the baseline is calculated

A baseline is a period when things are operating normally in your environment. Any anomalies that occur during the baseline period will be calculated into the results and skew the recommended values. If you are aware of an anomaly, re-baseline to ensure that the recommended values are accurate.

Consider customizing baselines if significant changes happen that influence what is normal in your environment, such as merging a new company, onboarding a large number of users, or making substantive improvements to the infrastructure.
By default, baseline calculations are based on data collected during seven days. Node baseline calculations are performed daily, and interface baseline calculations are performed weekly on Sunday.

1. Log in to the Orion Web Console using an account with administrative privileges.
2. Click Settings > All Settings in the menu bar.
3. In Thresholds & Polling, click Polling Settings.
4. Scroll down to Database Settings, and adjust the number of days in the Baseline Data Collection Duration field so that the time does not include a known deviation from the normal status.

   The Baseline Data Collection Duration cannot exceed the Detailed Statistics Retention configured in the same section.

5. To change the frequency of calculating interface baselines, choose the Interface Baseline Calculation Frequency.

   You can customize the calculation frequency only for interface baselines. The number of monitored interfaces is usually much larger than the number of nodes. Calculating baselines for nodes usually does not affect performance as much as performing the same calculations for all monitored interfaces.

6. Click Submit.

Your settings will now be used for calculating baselines.

Define baselines for nodes in the Orion Platform

Using the baseline feature, you can display baselines on different charts in the Orion Web Console.

Define a baseline for an individual node

1. Click Edit thresholds on the resource, and select the thresholds you want to edit.
2. Select Override Global Orion Threshold or Set Dynamic Threshold, and set either a static threshold, or click Use Dynamic Baseline Thresholds to define a formula for calculating a baseline. For information about threshold types, see Thresholds in the Orion Platform.
3. Click Submit.

Define a baseline for multiple nodes

1. Click Settings > All Settings > Node & Group Management > Manage Virtual Devices in the Orion Web Console.
2. Click the Thresholds tab.
3. Select the entity type for which you want to configure a baseline threshold from the Show list.
4. Select the nodes for which you want to configure a baseline.
5. Click Edit Thresholds, and select the thresholds you want to edit.
6. Select Override Global Orion Threshold or Set Dynamic Threshold, and set either a static threshold,
or click Use Dynamic Baseline Thresholds to define a formula for calculating a baseline.

7. Click Submit.

For example, to configure thresholds for all virtual machines under a given host, first select all vNodes, and deselect the vNodes for which you do not want to define thresholds.

General threshold types in the Orion Platform

Use these settings to:

- Specify devices to be included in reports that identify devices with high values for a specific metric, such as High CPU load, High Disk Usage, ...
- Highlight values for devices that exceed the threshold for a specific metric in Top X widgets, such as Top X Devices by Packet Loss. See an example.
- Highlight values that exceed thresholds for specific metrics in gauges. See an example.

Starting with Orion Platform 2019.2, you can include thresholds in calculating the node status.

Avg CPU Load

Define when the CPU load on devices is critical and what value you want to be warned about.

Devices with CPU load higher than the Warning Level are included in High CPU Load reports.

Specify how you want the Orion Platform to calculate whether your environment is exhausting its resources based on this metric. You can choose to calculate exhaustion using average daily values or peak daily values.

**Critical Level**

When the values of CPU load on a device exceeds the Critical Level, the value for this metric and the metric names are displayed as bold red in Top X widgets and in gauges.

**Warning Level**

When the value of CPU load on a device is higher than the Warning Level, values for this metric and the metric name are displayed as red in Top X widgets and in gauges.

Disk Usage

Define when the disk usage on devices is critical and the value you want to be warned about.

Devices with disk usage higher than the Warning Level are included in High Disk Usage reports.

Specify how you want the Orion Platform to calculate whether your environment is exhausting its resources based on this metric. You can choose to calculate exhaustion using average daily values or peak daily values.

**Critical Level**

When the disk usage value on a device is higher than the Critical Level, the value and the metric name are displayed in bold red in Top X widgets and in gauges.
Warning Level

When the disk usage value on a device is higher than the value set for the Warning Level, but lower than the value set for the Critical Level, the metric name and values are displayed in red in Top X widgets and in gauges.

Percent Memory Used

Define when the percentage of used memory on devices is critical and what value you want to be warned about.

Devices with Percent Memory Used higher than the Warning Level are included in Percent Memory Used reports.

Specify how you want the Orion Platform to calculate whether your environment is exhausting its resources based on this metric. You can choose to calculate exhaustion using average daily values or peak daily values.

Critical Level

When the percent memory used on a device is higher than the value set for the Critical Level, the metric name and values are displayed as bold red in Top X widgets and in gauges.

Warning Level

When a percent memory usage value on a device is higher than the value set for the Warning Level, but lower than the value set for the Critical Level, the metric name and values are displayed as red in Top X widgets and in gauges.

Percent Packet Loss

Define when the Percent Packet Loss on devices is critical and at what value you want to be warned about.

Devices with Percent Packet Loss higher than the Warning Level are included in High Percent Loss reports.

Critical Level

When the percent packet loss on a device is higher than the value set for the Critical Level, the metric name and values are displayed as bold red in Top X widgets and in gauges.

Warning Level

When the percent packet loss on a device is higher than the value set for the Warning Level, but lower than the value set for the Critical Level, the metric name and values are displayed as red in Top X widgets and in gauges.

Orion Platform products calculate percent packet loss using ICMP ping requests made on the Default Poll Interval. The poller sends a ping to monitored devices and records the results of the ten most recent ping attempts. Percent packet loss is expressed as the number of failed ping requests, X, divided by the number of ping requests, 10.

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

Define when the response time on devices is critical and what value you want to be warned about.

Devices with response time higher than the Warning Level are included in High Response Time reports.

**Critical Level**

When the response time value on a device is higher than the value set for the Critical Level display, the metric name and values are displayed as bold red in Top X widgets and in gauges.

**Warning Level**

When the response time value on a device is higher than the value set for the Warning Level, but shorter than the value set for the Critical Level, the metric name and values are displayed as red in Top X widgets and in gauges.

Orion Platform products calculate response time using ICMP ping requests made on the Default Node Poll Interval. The poller sends a ping to monitored devices and records the results of the ten most recent ping attempts. Average Response Time is expressed as the average response time of these last 10 ping requests. If the poller does not receive a ping response within the Default Poll Interval, it will attempt to ping the non-responsive device once every 10 seconds for the period designated as the Warning Interval.

**Example: Warning and Critical threshold exceeded in a Top X widget**

In this widget, the packet loss of the first node (kyiv..) has exceeded the critical threshold (that's why the percentage is bold red). The whole node has the critical status, so the node has the critical icon and the progress bar is red.

The packet loss for the second node (solar...) has exceeded the warning threshold, so the percentage is red. The whole node is in the warning status, that's why there's the warning icon and the progress bar is yellow.

### Top 10 Nodes by Percent Packet Loss

<table>
<thead>
<tr>
<th>NODE</th>
<th>PERCENT LOSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>kyiv1</td>
<td>70%</td>
</tr>
<tr>
<td>solar</td>
<td>40%</td>
</tr>
</tbody>
</table>
Example: Warning threshold exceeded in a gauge

This widget displays two gauges: Response Time and Packet Loss. Packet loss on the node has exceeded the warning threshold, that's why the metric name and the current percentage are both red.

Filter nodes in Orion Platform widgets using SQL queries

When you are managing or monitoring large numbers of network devices, node list widgets can easily become very large and difficult to navigate. Filters are optional SQL queries that are used to limit node list displays for easier navigation in widgets. SQL queries can be made on any predefined or custom properties.

If you have upgraded to Orion Platform version 2015.1.x or later, your custom SQL or SWQL query or filter may no longer work correctly.

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

SQL query examples

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

The following are valid status levels:

- 0 = Unknown (current up/down status of the node is unknown)
- 1 = Up (The node is responding to PINGs)
- 2 = Down (The node is not responding)
Custom properties in the Orion Platform

Every object you monitor includes a list of default properties used to describe the devices, such as IP address, host name, or MAC address. You can also create custom properties and use them to create special alerts, reports, views, and groups.

Custom properties are user-defined fields, such as country, building, asset tag, or serial number, that you can associate with monitored network objects.

Custom property uses include:

- Add information to nodes, such as contact, owner, or support contract.
- Add a custom property that is used as an account limitation on nodes.
- Add a custom property to nodes for grouping on the web or in a report.
- Add a custom property and display it as an annotation on a chart.

A collection of the most commonly used properties is available out-of-the-box, but you can create custom properties to meet your precise requirements.

When a custom property is defined, you can import values for the property from a text- or comma-delimited file.

To apply a property to only a few objects, go to the Edit view in the Orion Web Console.

You may also create external records by exporting custom properties from selected objects as a spreadsheet.

Create a custom property in the Orion Platform

Custom properties help you add custom labels to monitored objects, group objects based on the property or alert on objects with a certain value for the property.

Depending on the selected object type, some options are not available.

1. Click Settings > All Settings in the menu bar.
2. In the Node & Group Management grouping, click Manage Custom Properties.
3. Click Add Custom Property.
4. Select the object type for the property, and click Next.

   The available object types depend on the Orion Platform products installed. All installations allow you to create Node and Volume custom properties.

5. Define the custom property, and click Next.

   Frequently used custom properties are available as templates. Select a template, and adjust the settings if necessary. Templates ensure that naming conventions are met when necessary for certain workflows.

   a. Edit the Property Name and Description fields.

      Property names are not case-sensitive, and must be unique for each object type. For example, you can have separate Comment properties for Nodes, Volumes, and other object types.

   b. Select the Format for the property.

      We recommend that you limit the string length for text properties. The string length can affect SQL performance, especially when custom properties are used in limitations. The shorter the string length, the faster the queries.

      To limit the string length, click Edit, and provide the maximum number of characters.

      ![Format: Text](Any alpha and numeric text (up to 400 characters) Edit]

   c. Create a drop-down menu with specific values for the property by selecting Restrict values, and adding the values.

      Restricting values helps to maintain the consistency of values for individual custom properties.

   d. If you want to limit how the custom property for nodes should be used, clear boxes in the Usage section.

      When you select a Usage option, you cannot clear the option after you submit the custom property. This prevents you for example from disabling a custom property for reports in case it is already used in a report.

      - Alerts: the custom property is offered only in alerts.
      - Filtering: the custom property is offered when adding Filter Properties in AppStack Environment.
      - Grouping: the custom property is offered in Group by drop-down lists.
      - Reports: the custom property is offered when designing the layout for web-based reports.
      - Object Details Views: the custom property appears in the Custom Properties
Nodes resource in the Orion Web Console.
- Asset Inventory: selected only if you have SAM installed on the server. The custom property appears in the Custom Asset Information resource.

6. Select objects for which you want to define the custom property.
   a. Click Select <Objects>, and locate, and select the objects in the Available <Objects> pane.
   b. Click Add, and then click Select <Objects>.

7. Enter or select a default value for the property.
   Do not use angle brackets <, > as a value for custom properties.

   ![Select Nodes and Assign value for "Device_Owner" to selected Nodes]

   To add a value for properties with restricted values, select Add New Value from the dropdown menu, and enter the new value.

8. To apply the selected property to a different group of objects, click Add More, select the objects, and click Submit.

You have created a custom property and provided its value for the selected objects.

Now, you can specify the property value in the object properties. For example, for node properties, click Settings > Manage Nodes, select the object, and click Edit Properties.

![Custom Properties]

City: City where the Node is located
Comments: Any comments about the Node
Department: Department this Node services
Device_Owner: Person or team responsible for the device
You can now use the custom property for sorting objects of the type in Group By lists.

Remove a custom property in the Orion Platform

⚠️ If the custom property is used in reports or alerts, remove it from the definition of all alerts and reports before you remove it from the Orion Web Console. Reports defined using removed custom properties do not work, and alerts stop triggering.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Custom Properties.
4. Select properties you want to remove, and click Delete.
5. Confirm your action when prompted.

Import custom property values in the Orion Platform

If you have a spreadsheet listing custom property values, such as asset tags of all your network nodes, you can make this information available for reporting and publication in the Orion Web Console.

Things to consider before the import

- The import will overwrite existing custom properties.
- Your data must be formatted as a table.
- At least one column title should match an existing object property, such as IP Address.
The import supports the following formats: .csv, .txt, .xls or .xlsx.
If your .xls or .xlsx file has multiple worksheets, only the first worksheet will be imported.

Import steps
1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Custom Properties.
4. Click Import Values.
5. On Select File, browse to the custom property data file, and click Open.
6. Select the object type you want in the Import Values For drop-down.
7. Specify whether you want to import everything or only items that have changed, and click Next.
   - To import everything and overwrite existing values, clear the Remove unchanged rows box.
   - To overwrite only values that changed, keep the Remove unchanged rows box selected.
     This option expects that you had exported custom properties and edited some values in the exported file. Selecting the box means that before importing the file, the Orion Platform will identify the changed rows and will only import the updates.
8. On the Match Columns tab, select an Orion Database Column for each detected column, and select the Relationship between the columns.
   - Select Matches to indicate columns in the spreadsheet that correspond to existing columns in the SolarWinds Orion database, such as IP Address or MAC address.
     Select Imports To to import the data in the spreadsheet column to the selected SolarWinds Orion database column.
     This option overwrites any existing data in the corresponding custom properties.
   - Select Imports To, and select <No Match Found, Ignore> for any spreadsheet column you do not want to import.
   - Click Create This Custom Property Now to open the Add Custom Property in a new browser tab if you need to create a custom property for this spreadsheet column.
9. Click Import.

When you view the values of the object type, the values of the custom property you selected are populated.
Export custom property data in the Orion Platform

If you want to keep records of custom properties for selected monitored nodes, you can export them as a spreadsheet. For example, you can create a single spreadsheet that lists the asset tags of all your network nodes.

You can only select custom properties for a single object type.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Custom Properties.
4. Select the custom properties you want to export, and click Export Values. You can Filter objects to find the custom properties more easily.
5. To export custom property data for specific objects, click Select <Objects>, and select the objects.
6. Select the database columns you want to export. You can also change which custom properties you want to export.
7. Select the file type for the exported data. This can be .csv, .txt, .html or xls.
8. Click Export.

The exported file is downloaded to your browser's default download location.

Change custom properties values in the Orion Platform

You can change the value of a custom property from the Manage Custom Properties page or bulk edit the values of a custom property assigned to objects.

You can only edit properties of one object type at a time.

Edit values for custom properties

When you are entering a large amount of data, it can be easier to import the values from a spreadsheet.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Custom Properties.
4. Select the custom properties, and click View / Edit Values. You can Filter objects to find the custom properties more easily.
5. To add or change a value for a property, enter the value into the field.
   Do not use angle brackets <, > as a value for custom properties.
6. To add the same custom property value for multiple objects, select the objects, and click Edit Multiple Values. Select the property, enter the value, and click Save Changes.
7. When you have added or edited the values, click Save Changes.
Filter objects when assigning custom properties in the Orion Platform

You can limit objects displayed in the Custom Property Editor to find the objects you want to edit.

1. Click Settings > All Settings in the menu bar.
2. In the Node & Group Management grouping, click Manage Custom Properties.
3. Select the custom properties for which you want to assign values, and click View / Edit Values.
4. In the column captions, click the Filter icon, and enter filter text.

The table will only display objects matching the filter options. The condition is added above the Group by section of the Custom Property Editor.

To remove the filter, click the trash icon next to the filter.

Draw horizontal lines in Orion Platform widgets

Customize charts for specific objects to include a horizontal line that marks certain values. For example if you have an SLA that requires response time on a key interface to stay below certain value, you can draw a line into the response chart which marks the value that should not be exceeded.
This is possible for most charts, such as availability charts, response time, CPU load, memory, percent memory, or buffer charts.

You can use lines to control the upper end of the y-axis. Set the [metric name]_Marker value at the required high value and set no label. The chart will always go at least to the defined value, regardless of the data.

1. **Create two custom properties for nodes** based on property templates:
   - [metric name]_Marker, for example ResponseTime.Marker, designating the value where the line will display.
   - [metric name]_Annotation, for example ResponseTime.Annotation, provide a label for the line.

2. In Property Templates, select [metric name]_Marker.

   ![Property templates screenshot]

<table>
<thead>
<tr>
<th>Property Templates</th>
<th>Select Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>ResponseTime.Marker</td>
</tr>
<tr>
<td>Model</td>
<td>Annotation value - draw line</td>
</tr>
<tr>
<td>UPS</td>
<td>Floating Point Number</td>
</tr>
<tr>
<td>CustomerName</td>
<td>Value must be specified</td>
</tr>
<tr>
<td>CustomerID</td>
<td>Create a drop-down list</td>
</tr>
<tr>
<td>ResponseTime_Marker</td>
<td>Select how this property is used</td>
</tr>
<tr>
<td>ResponseTime_Annotation</td>
<td></td>
</tr>
<tr>
<td>Availability_Marker</td>
<td></td>
</tr>
<tr>
<td>Availability_Annotation</td>
<td></td>
</tr>
</tbody>
</table>

3. On Assign Values, select the objects, and provide values for the line.

4. Create the [metric name]_Annotation custom property based on the template, select the objects, and provide the label for the line.
When you now go to the details view for the node and consult the Response time graph, you will see a labeled line signifying the selected value there.

Create a custom location property in the Orion Platform

The Custom Property Editor allows you to choose from a collection of many commonly used properties, or to build your own custom properties. Once your custom property is defined, the Import Wizard allows you to populate your new property from either a text- or comma-delimited file.

Alternatively, if you only have a few individual changes or additions, you may choose to make those changes using the Edit view.

The following procedure shows how to create a custom location property that is applied to monitored nodes.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. Click Manage Custom Properties in the Node & Group Management grouping.
4. Click Add Custom Property.
5. Select Nodes, and then click Next.
6. Enter NodeLocation as the Property Name, provide an appropriate Description.
7. If you want this to be a mandatory property required for all nodes, click on Required.
8. Click Next.
9. Click Select Nodes.
10. Select all the nodes to which you want to assign the same value for `NodeLocation`, and click Add.
11. When all nodes that can be given the same value are selected, click Select nodes.
12. Enter the `NodeLocation` for this selection of nodes, and click Submit.
   The `NodeLocation` custom property is now defined for all selected nodes.
13. To add values to other nodes, select `NodeLocation`, and click View/Edit Values. Enter the values in the `NodeLocation` column, and click Save Changes when completed.
Customize the Orion Web Console look, views, settings, charts, and maps in the Orion Platform

You need the Allow Administrator Rights privilege.

Customize the Orion Web Console look for the Orion Platform

- My Dashboards in the Orion Platform
- Change the Orion Web Console color scheme in the Orion Platform
- Change the Orion Web Console logo in the Orion Platform
- Use Orion Web Console breadcrumbs in the Orion Platform

My Dashboards in the Orion Platform

The My Dashboards menu provides shortcuts to Orion Web Console views. The default menu bars include Home, and a menu bar for each installed Orion Platform product.
Click My Dashboards to show the default menus.

You can customize the views and labels in default menus for individual users.

💡 If you do not want to show all items in menu bars, and prefer navigating to display items in a menu bar, click My Dashboards > Collapse.
Customize My Dashboards

Menu bars available in My Dashboards depend on both the settings in your user account and the products you have installed.

1. **Find out** which menu bar is assigned to Home, Network, or other product-specific tab for your user.
2. **Add an Orion Web Console view or an external web page to the menu bar.** The change will concern all users who access the menu bar from My Dashboards.

   ![Tips](image)

   To add a link to a details view for an important device, go to the view, copy the URL, and add it as an extra item to the view.

3. To provide access to a specific set of links for specific users, create a menu bar, add the links and assign the menu bar as the Home tab for the users.

Specify My Dashboards and Alerts & Activity items for users

The items users see in My Dashboards and in Alerts & Activity are specified in their user accounts.

![Tips](image)

Improve performance by setting the Home Page View to a view with a limited number of resources on it.

1. Click Settings > All Settings in the menu bar.
2. In the User Accounts grouping, click Manage Accounts.
3. Select a user, and click Edit.
4. Scroll down to Default Menu Bars and Views, and select top menu bars from the lists.

![Default Menu Bar and Views](image)

5. Select Yes for the items the user can see in the Alerts & Activity menu bar.
6. Select an item and use the arrows to change the order of menu bars. Select an item from the list to specify the default Home page view.

7. Click Submit.

The user can now use the specified links in My Dashboards and Alerts & Activity menu bars.

Add items to My Dashboards

What users see in My Dashboards depends on menu bars assigned to them in their user account. To add an item to My Dashboards for all users who can see a menu bar, add the item to the menu bar.

1. Click My Dashboards > Configure.
2. Click Edit.
3. Drag available items from the left-hand column to Selected Items on the right.
4. Click Submit to save your changes.
You can also add links to node details views for specific nodes, or to external Internet pages as a menu item.

a. Click Add below the Available items list, provide a name, URL and description for the menu item, and click add.

b. Drag the new item to the Selected items column.

Users who can see the menu bar in My Dashboards will see the added items.

Add menu bars

When you have a list of items you want users to access from My Dashboards, create a menu bar.

1. Click My Dashboards > Configure.
2. Scroll to the bottom of the page, and click New Menu Bar.
3. Name the menu bar.
4. Drag views from the Available items column into Selected items.

5. Click Submit.

The new menu bar is created. You can now assign it to users who will see the items in My Dashboards.

Change the Orion Web Console color scheme in the Orion Platform

1. Click Settings > All Settings in the menu bar.
2. In the Customize Navigation & Look grouping, click Color Scheme.
3. Select a color scheme, and click Submit.
Change the Orion Web Console logo in the Orion Platform

1. Create a graphic to replace the SolarWinds logo.
   The recommended logo size is 250 x 50 pixels. The maximum allowed size is 900 x 500 pixels.
2. Place your graphic in the images directory.
   The default location of the directory is C:\Inetpub\SolarWinds\NetPerfMon.\images.
3. Click Settings > All Settings in the menu bar.
4. In the Product Specific Settings grouping, click Web Console Settings.
5. Ensure the Site Logo box is selected, and click Browse to navigate to your logo.
   ![SITE LOGO]
   ![SolarWinds.Logo.png][BROWSE]
   ![Upload logo from external path]
6. Click Submit.

Use Orion Web Console breadcrumbs in the Orion Platform

As you navigate Orion Web Console views, you can use breadcrumbs to pick other views that are on the same or higher navigational level as your current view.

- You cannot view breadcrumbs in wizards, dashboards, or full-page resources such as All Active Alerts.
- Only the first 50 monitored nodes, listed in alphanumeric order by IP address, are displayed.

1. Click a breadcrumb to open the view.
2. Click > next to a breadcrumb to open a clickable list of all views at the same navigation level. For example, if you are on a Node Details view, clicking > displays a list of other monitored nodes.

Customize breadcrumbs

1. Click > at an appropriate level in the breadcrumbs to open the drop-down.
2. Click Customize This List.
3. Select an option from the menu, and click Submit.
   ![All items in the customized list will be identical for the selected criterion.]

ADMINISTRATOR GUIDE: ORION PLATFORM
Add custom properties to node popovers in the Orion Platform

Popovers are UI elements displayed when you hover over a monitored object on an Orion Web Console view. They provide additional information and quick access to commands without taking up space or cluttering the page with too much information.

You can include up to five custom properties in your popovers for nodes.

To include custom properties in node popovers, select the Object Details Views option in the Usage section.

You can do this when creating a custom property or edit an existing custom property.
How custom views work in the Orion Platform

Orion Web Console views are configurable pages of network information that can include maps, charts, summary lists, reports, events, and links to other resources. Summary views provide data about multiple objects. Detail views provide more information for a specific object.

For example, the default Summary view displays an overview of all monitored nodes. Clicking on a node in the Summary view opens the Node Details page for that node, where you can see all of the statistics monitored for that device.

To customize views, the user must have the following privileges set to Yes:
- Allow Administrator Rights
- Allow Account to Customize Views

Create views in the Orion Web Console for your Orion Platform products

You can customize the Orion Web Console for individual users by creating views.

You need Administrator Rights to create views.

Check out this video on creating a new view.

1. Log in to the Orion Web Console, and click Settings > All Settings.
2. Click Add New View in the Views grouping.
3. Name the view, and select the view type.

4. Click Submit.

You have now created an empty view. The Customize view page opens automatically. Add widgets that contain the information you want to see or add the view to a dashboard.

The Type of View affects how the view is made accessible to users, and your choice may not be changed later. For more information, see Specify views for device types in the Orion Platform.
Add widgets to Orion Platform views

1. Go to the view to customize.
2. Click the pencil icon on the upper left.
3. Click the Add Widgets button on the upper right.
4. Search for widgets, or resources, and drag and drop them on the page where you want them to be, including in new columns.
   - You can limit offered widgets by criteria in the Group by list, or search for a widget in the Search box.
5. When complete, click Done adding widgets, and then Done editing.

The view is now populated with the widgets you selected.

Administrators can also access views by clicking Settings > All Settings > Manage Views.

Optimize Orion Platform views for TV screens or mobile devices

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

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

Enable NOC Views

1. Log in to the Orion Web Console as an administrator.
2. Open a view, and click the Customize Page (pencil) icon > Page Settings in the top left corner of the view.
3. Select Enable NOC view mode.
4. If the view contains several subviews, select the rotation interval for the subview.
   - To get a direct link to a NOC view, use the Link to NOC View link.
5. Click Done & Go to NOC View.

The view is now displayed in the NOC mode, with a compressed header and footer, and without the left navigation area.
Manage NOC Views

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

1. Click Settings > All Settings.
2. In the Views grouping, click Created NOC views.

You can view NOC views from any view. Click Customize Page, and click List of created NOC views in the NOC view section.

3. Manage the NOC views:
   - To add a new view, click Add New View.
   - To edit a NOC view, select the view, and click Edit.
   - To disable a NOC view and maintain the default view, select the view and click Disable NOC.

Change the NOC view logo

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

**Logo requirements:**

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

To use a customized logo on your NOC views:

1. If you already are in a NOC view, click the NOC Settings icon and select Customize NOC View Logo.
2. To hide the logo, clear the NOC View Logo option.
3. To change the logo:
   a. Make sure that NOC View Logo is selected.
   b. Click the Browse button for NOC View Logo and navigate to the appropriate logo image.

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

4. Click Submit to apply your changes in the view.
Limit objects on a view in the Orion Platform

As a security feature, administrators can limit which devices are displayed on a view.

1. On the view, click the pencil icon > Page Settings.
   
   You can also access the View Limitation section from Manage Views: Click Settings > All Settings > Manage Views, then select the view, and click Edit.

2. Scroll down and click Edit in the View Limitation area.
3. Select the type of view limitation you want to apply, and click Continue.
4. Provide or select strings or options to define the device types that you want to include or exclude from the selected view, and click Submit.
   
   The asterisk (*) is a valid wildcard. Pattern limitations restrict views to devices for which the corresponding fields include the provided string.

Use a view as a template in the Orion Platform

When you want to create multiple views, create one view, and use it as a template to create other new views.

1. Click Settings > All Settings in the menu bar.
2. In the Views group, click Manage Views.
3. Select the view you want to copy, and click Copy.
4. Edit the copied view.

Delete views in the Orion Platform

1. Click Settings > All Settings in the menu bar.
2. In the Views group, click Manage Views.
3. Select the view you want to delete, and click Delete.

Specify views for device types in the Orion Platform

In the Orion Web Console, you can specify views displayed for each type of device you have on your network, such as routers, firewalls, or servers.

1. Click Settings > All Settings in the menu bar.
2. In the Views grouping, click Views by Device Type.
3. Select a Web View for the individual types of devices currently monitored on your network.
4. Click Submit.

When you click a device now, the view specified for the device type will be displayed.

Widget configuration examples in the Orion Platform

Several widgets, or resources, that may be selected from the Add Resources page require additional configuration.

Display a Network Atlas map in the Orion Web Console

Network maps created with Network Atlas can give a quick overview of your network. Add a Network Atlas map on a view.

1. Open a view where you want to add the map, and click the pencil icon on the left.
2. Click the Add widgets button.
3. Search for map in the Search box.
4. Drag and drop the Map widget to the page.
5. Click Done adding widgets > Done editing.
6. Click Edit on the widget.
7. Select a map.
8. Specify the Zoom percentage at which you want to display the map.

If you leave the Zoom field blank, the map displays at full scale, based on the size of the column in which the map displays.

The map is added to the view.

Display a list of objects on a network map

1. Open the view where you want to add the list of objects on a map, and click the pencil icon on the left.
2. Click the Add widgets button.
3. Search for map in the Search box.
4. Drag and drop the List of Objects on Network Map widget to the page.
5. Click Done adding widgets > Done editing.
6. Click Edit on the widget.
7. Select a network map from the list of maps, and click Submit.

The view will now include a resource listing objects on the selected map.
Display a custom list of available maps

Clicking a map in the list opens the map in a new window.

1. Open the view where you want to add the list of maps, and click the pencil icon on the left.
2. Click the Add widgets button.
3. Search for map in the Search box.
4. Drag and drop the Custom List of All Maps widget to the page.
5. Click Done adding widgets > Done editing.
6. Click Edit on the widget.
7. Select maps you want to include in your maps list.
8. Click Submit.

Display the Worldwide Map

The worldwide map provides a quick geographical overview of your network at any level from global down to street.

1. Open the view where you want to add the Worldwide Map, and click the pencil icon on the left.
2. Click the Add widgets button.
3. Search for map in the Search box.
4. Drag and drop the Worldwide Map widget to the page.
5. Click Done adding widgets > Done editing.

You have now added the Worldwide map to the view. Customize the world map now.

1. Click Edit in the Worldwide Map resource title bar.
2. Provide a Title and Subtitle for the map.
   
   ▲ Titles and subtitles can be entered as either text or HTML.

3. Enter a value for Height. The default is 400 px.
4. Click Set Location and Zoom Level if you want to change the default location (the center of the map) and zoom of the map.
   To set the default zoom and location manually, click Advanced, and enter the latitude and longitude of the default location and the zoom level.
5. To filter the groups and nodes to be displayed, click Group and/or Nodes, and enter a SWQL filter.
   Click Examples to see a few SWQL filter samples.
6. Click Submit.

Display events received during a given time period

1. Open the view where you want to add the events summary, and click the pencil icon on the left.
2. Click the Add widgets button.
3. Search for event in the Search box.
4. Drag and drop the Event Summary widget to the page.
5. Click Done adding widgets > Done editing.
6. Click Edit on the widget.
7. Select the time period for displaying events in Time Period.
8. Click Submit.

Specify user-defined links

You can copy URLs of external websites or customized views from preview pages, and copy them to the User Links resource.

1. Open the view where you want to add the links resource, and click the pencil icon on the left.
2. Click the Add widgets button.
3. Search for links in the Search box.
4. Drag and drop the User Links widget to the page.
5. Click Done adding widgets > Done editing.
6. Click Edit on the widget.
7. Enter the following information for each link you want to define:
   a. A link Name and the URL of your link.
   b. If you want your links to open in a new browser window, select Open in New Window.
     
     *Info Icon* - Hsps URLs are not supported.

8. Click Submit.

Specify Custom HTML

When you have static information that you want to provide in the Orion Web Console, add the Custom HTML resource on a view. This resource can also provide quick access to customized views.

1. Open the view where you want to add the custom resource, and click the pencil icon on the left.
2. Click the Add widgets button.
3. Search for html in the Search box.
4. Drag and drop the Custom HTML widget to the page.
5. Click Done adding widgets > Done editing.
6. Click Edit on the widget.
7. Enter HTML formatted content as required.
8. Click Submit.
Filter nodes

The Orion Web Console can maintain a customizable node list for your network. Node lists can be configured for specific views using SQL query filters.

1. Open the view where you want to add the node list, and click the pencil icon on the left.
2. Click the Add widgets button.
3. Search for nodes in the Search box.
4. Drag and drop the All Nodes - Table widget to the page.
5. Click Done adding widgets > Done editing.
6. Click Edit on the widget.
7. To filter your node list by text or IP address range, provide the text or IP address range by which you want to filter your node list in the Filter Text field:
   - Type Home in the Filter Text field to list all nodes with "Home" in the node name or as a location.
   - Type 192.168.1.* in the Filter Text field to list all nodes in the 192.168.1.0-255 IP address range.
8. Select the property for the filter text provided above:
   - If you typed Home in the Filter Text area, select Node Name or Location to list nodes with "Home" in the node name or as a location.
   - If you typed 192.168.1.* in the Filter Text area, select IP Address to list only nodes in the 192.168.1.0-255 IP address range.
9. To apply a SQL filter to the node list, enter an appropriate query in the Filter Nodes (SQL) field.

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

10. Click Submit.

Group nodes within a view

The Orion Web Console can maintain a customizable node list for your network. Node lists can be configured for specific views with node grouping.

1. Open the view where you want to add the node list, and click the pencil icon on the left.
2. Click the Add widgets button.
3. Search for nodes in the Search box.
4. Drag and drop the All Nodes - Tree widget to the page.
5. Click Done adding widgets > Done editing.
6. Click Edit on the widget.
7. Select up to three criteria, in specified levels, for Grouping Nodes within your web console view.
8. Select whether you want to put nodes with null values in the [Unknown] Group or ungrouped at the Bottom of the List.

9. To apply a SQL filter to the node list, enter an appropriate query in the Filter Nodes (SQL) field.

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

10. Click Submit.

Add a Service Level Agreement Line to charts (SolarWinds NPM)

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

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

1. Click Settings > All Settings in the menu bar.
2. In Node & Group Management, select Manage Custom Properties.
3. Click Add Custom Property.
4. Select Interfaces as the custom property object type, and click Next.
5. Click SLA in the list of predefined Property Templates, make any required changes to the fields displayed, and click Next.
6. Click Select Interfaces.
7. Select and add all interfaces to which you want to apply the same service level, and then click Select Interfaces.
8. Enter the SLA value (in bps) in the SLA column for each interface you want to label with SLA values. For example, type 1544000 for a T1 interface (1.544 Mbps) or 225000 for a serial connection running at 225 Kbps.
9. To enter a different SLA value for a different set of interfaces, click Add More.
10. Click Submit.

Browse to the Interface Details view of one of the interfaces you edited. The SLA line displays on any chart showing Min/Max/Average bps.
Add external websites to the Orion Platform

You can select any external website and add it to the Orion Web Console as a view.

You need Administrator Rights.

1. Log in to the Orion Web Console and click Settings > All Settings in the menu bar.
2. In the Customize Navigation & Look grouping, click External Websites.
3. Click Add.
4. Provide a Menu Title. This will be used for the website in the My Dashboards menu bar.
5. If you want to include a heading for the view, provide an optional Page Title.
6. Provide the URL of the external website, in the following format:
   http://domain_name
7. Select the Menu Bar to which you want to add the website link. See My Dashboards in the Orion Platform.
   [Note: If you select Admin as the menu bar, the website will be available from My Dashboards > Home for administrators.]
8. Click OK.
9. Click Preview to see the external website in the Orion Web Console.

Customize the Custom Summary view in the Orion Platform

Use the Custom Summary view template in My Dashboards to select specific entities and display specific data for them.

- Custom Object widgets
- Custom Table widgets
- Custom Chart widgets

You need the Allow Account to Customize Views right enabled.

Specify entities and the metric in Custom Object widgets

1. Click My Dashboards > Home > Custom Summary.
2. Click Edit in any Custom Object Resource.
3. Provide a Title and Subtitle for the resource.
4. Select an object type from the Choose Object Type drop-down.

![Object Type Selection](image)

5. Click Select Object.

6. On the Select Objects window, use the Group by selection field to filter the list of monitored objects.

7. Select one or more objects on which to base the selected resource, click the green arrow to move objects into the Selected Objects pane and click Submit to add the objects.

8. Specify what information about the selected object(s) you want to see in the resource, and click Submit.

![Resource Configuration](image)
The fields displayed and information required depend upon the object type selected.

Specify entities and metrics for Custom tables

1. Locate the blank custom table widget on the view.
2. Click Configure this widget.
3. Enter a title, and click Select Data Source.

4. Select the object you want to report on, for example, Node.

5. Define a condition that specifies the type of nodes to include, for example, all nodes owned by the New York IT Department.

6. Click Add column, select properties, and click Add Column.
The custom table resource populates with the node status, the owner, and a contact email address.

<table>
<thead>
<tr>
<th>STATUS</th>
<th>NODE NAME</th>
<th>DEVICE_OWNER</th>
<th>EMAIL_ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up</td>
<td>BranchRouter.lab.loc</td>
<td>New York IT</td>
<td><a href="mailto:NY-IT@mail.com">NY-IT@mail.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Department</td>
<td></td>
</tr>
<tr>
<td>Up</td>
<td>MainRouter.lab.local</td>
<td>New York IT</td>
<td><a href="mailto:NY-IT@mail.com">NY-IT@mail.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Department</td>
<td></td>
</tr>
<tr>
<td>Up</td>
<td>Perm_Tex-Mds9120</td>
<td>New York IT</td>
<td><a href="mailto:NY-IT@mail.com">NY-IT@mail.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Department</td>
<td></td>
</tr>
<tr>
<td>Up</td>
<td>respTex-Colubris-map320</td>
<td>New York IT</td>
<td><a href="mailto:NY-IT@mail.com">NY-IT@mail.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Department</td>
<td></td>
</tr>
<tr>
<td>Up</td>
<td>Tex-2821.tex</td>
<td>New York IT</td>
<td><a href="mailto:NY-IT@mail.com">NY-IT@mail.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Department</td>
<td></td>
</tr>
</tbody>
</table>

Specify entities and metrics for Custom charts

1. Click Edit in the Custom Chart widget.
2. Click SelectDatasource.
3. Use one of the following methods to configure the objects displayed in the chart or table:
   - Specific Objects (static selection) - use when you know which objects you want to include in your chart or table.
     a. Filter or search for the objects you want to include.
     b. Select the objects' check boxes.
       This is the most straightforward selection method, and recommended for new users. It is also the preferred method for relatively permanent network objects.
   - Dynamic Query Builder - use to select objects based on object properties.
     a. Select Basic Selector to create and/or queries or select Advanced Selector to create complex queries.
     b. Choose the object type you want to include.
     c. Enter your conditions.
       This is the preferred selection method for groups of objects of a specified type that may change over time. "All Cisco nodes in Austin" is an example of a group best defined using the Dynamic Query Builder.
Advanced DataBase Query (SQL, SWQL) - only use if you are comfortable querying your SolarWinds database directly using SQL or SWQL.
   a. Select SQL or SWQL, and enter your query.
   b. Click Preview Results to test your query.

4. Click Add Data Series in Left Y-axis.
5. Filter or search for the data series, and select the one you want to use.

   - The groups available and the data series within these groups will depend on the object selected.

6. Click Add Data Series. The data series is added to the Left Y-axis.
7. For additional settings for each data series, click More. Here you can:
   - Edit the Display name for this data series.
   - Select a custom Color for this data series.
   - Show the 95th percentile line for this data series.
   - Show Trend for this data series.

8. Enter a Custom label for the Left axis.
9. Select the Units displayed, Chart type, and select the Show the sum of all data series, if required.
10. Select the Sample Interval. This can be as frequent as once a minute to once a week. Data within each sample interval are summarized so that a single point or bar is plotted for each of these periods.

   - It is possible to select a sample interval that is longer than the reporting period.

11. Choose how you want to filter the data.
    a. Select how you want to sort this selection of records from the Sort records by drop-down menu. The choices depend on the data series selected.
    b. Select either Ascending or Descending from the Sort order drop-down.
    c. Select the Data aggregation method required to summarize your data by time period.
    d. Click Advanced if you want to sort records using a secondary field.

12. Set up additional data series using the right axis to superimpose two charts using different labels, units, and chart type.

   - You cannot use a separate time period or filter results settings for the right axis series.

13. Click Submit.
Orion Web Console and chart settings for the Orion Platform

On the Web Console Settings page, administrators can customize the Orion Web Console user environment.

1. Click Settings > All Settings in the menu bar.
2. In the Product Specific Settings grouping, click Web Console Settings.
3. When you finish configuring the settings, click Submit.

When you edit the Web Console settings, the following options are available:

**Session Timeout**

Provide the amount of time, in minutes, that Orion Web Console waits through user inactivity before the user is logged out.

**Windows Account Login**

Select whether you want to enable or disable automatic login with Windows Active Directory Credentials. With this feature enabled, the user can log in automatically.

**Page Refresh**

Specify the amount of time that passes before an Orion Web Console view reloads automatically.

**Site Logo**

Select the box, and provide a path to a banner graphic that appears at the top of every Orion Web Console page.

**NOC View Logo**

Select the box, and provide a path to a banner graphic that appears at the top of every NOC view.

**Site Login Text**

Provide a text all Orion Web Console users will see before they log in. Enter up to 3500 characters. HTML tags are allowed.

**Help Server**

Provide the URL of the server where online help for Orion Platform products is stored. The default location is [http://www.solarwinds.com](http://www.solarwinds.com).

> If you are in an Internet-restricted network environment but require access to online help, download the online help for your products, including the Orion Platform offline help, copy it to a web server, and change the Help Server URL to that of the web server. You can download the online help from the documentation page for your product at [https://support.solarwinds.com/Success_Center](https://support.solarwinds.com/Success_Center).
Status Rollup Mode

Specify how the availability status of nodes in node trees or on maps is displayed in the Orion Web Console.

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

- Show Worst Status ensures the worst state in a node group is displayed for the whole group.
  
  Examples:
  Up + Down = Down
  Unreachable + Shutdown = Shutdown.

Child Status Rollup Mode

Relevant only for Classic Node Status Calculation: Specify how the status of any single node on the node tree or on a map is displayed.

- Select Show Worst Status to ensure that the worst status of the node group is displayed for the whole group (e.g. red if any of the nodes are down).
- Select Show Worst Status (Interfaces only) to ensure that the worst status of any of the interfaces on a selected node is displayed. Only if you have SolarWinds NPM installed.
- Select Show Worst Status (Applications only) to ensure that the worst status of any of the applications on a selected node is displayed.
- Select Show only ICMP Status to only display up/down status for monitored interfaces.

Child Status Display Mode

Relevant only for Classic Node Status Calculation. Select whether you want to use a static or blinking icon to display the status of the children of any single node on the node tree or on a map. By default, a static icon displays the status of child objects.

Integration Tips

Specify whether you want to show or hide the list of products in the How SolarWinds Products Work Together section of the Settings page.

Drag and Drop Views

Turn on or off the ability to drag resources around on views.
Auditing Settings

Enable Audit Trails
Select Enable Audit Trails to keep a record of all actions taken by Orion Web Console users. Depending on the number of technicians or the activity level of your installation, this may increase the storage needs of your database.

Chart Settings
The following settings apply only to classic charts:

Chart Aspect Ratio
Chart Aspect Ratio is the height/width ratio for web console charts. This ratio should be set between 0.25 and 3.0 to avoid erratic display problems, though the performance of individual systems may differ.

Thumbnail Aspect Ratio
Thumbnail Aspect Ratio is the height/width ratio for chart thumbnails.

95th Percentile Calculations
95th Percentile Calculations adds annotation lines to charts at the entered percentile. This value is normally set to 95.

Maximum Number of Data Series Displayed on Chart
The Maximum Number of Data Series Displayed on Chart setting determines the maximum number of data series that will display on a chart at the same time. The default value for this setting is 10.

Export charts as image in PDF
If modern or classic charts exported in PDFs are empty due to performance issues, enable this option. Instead of rendering charts, the Orion Platform exports the charts as images and includes them into the PDF.

Migrate charts to modern style charts
Click Migrate to upgrade legacy charts and classic charts to the modern style charts. Click Roll Back to revert to original charts.

Discovery Settings
Notify About New Removable Volumes
Select the box if you want to be notified when removable volumes are added to your network and discovered during network discovery. You should configure the default send email action to receive notifications.
Worldwide Map Settings

**Automatic Geolocation**

Select the box to place nodes automatically on worldwide maps.

Active Alert Settings

**Active Alerts Refresh**

Specify how often the active alerts grid page is refreshed.

**Customize charts in the Orion Web Console for the Orion Platform**

Use the customization options available in the chart to customize the data, layout and time frame shown by the chart.

Available customization options depend on the chart style:

- Modern
- Classic
- Legacy

As of Orion Platform 2018.4, legacy and classic charts are being deprecated. SolarWinds recommends that you use modern charts instead of legacy and classic charts.

See Orion Web Console and chart settings for details about global chart settings.

**Modern chart customization options**

Use the time options below the title.

Click Edit to customize the title or subtitle.

You can also display/hide statistical lines, such as trend or 95th percentile line.

If there is the Open in PerfStack button, you can display the metric in a Performance Analysis Dashboard.

**Classic chart customization options**

Click the zoom buttons to zoom in/out the chart.

Use the slider below the chart to zoom in/out.

Click Export to go to the Custom Chart page.

Click Edit to change the following settings:
Titles and subtitles

You can customize the title and subtitle for the resource and for the chart.

To change the chart labels, click Advanced, and enter a text or variable that displays as the chart title or subtitle.

ℹ️ The default for the chart subtitle is `${ZoomRange}`, which shows the selected zoom range.

Other options depend on the chart type.

**Calculated series: Show a trend line**

Select the box to display a trend line on the graph. This shows potential future results as extrapolated from collected historical data.

ℹ️ The trend lines are intended only as approximate predictions of future data.

**Calculated series: Show the sum of all data series**

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

**Calculated Series: Show the 95th percentile line**

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

**Maximum Number of Items to Display:**

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

**Time periods: Default zoom range**

Select the default range of data to be displayed from the drop-down list.

**Time periods: Amount of historical data to load**

Select the amount of historical data to load from the drop-down list.

**Time periods: Sample interval**

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

Legacy chart customization options

Legacy charts are not interactive. You can only change the time frame or do the edits on Custom Chart page.
Legacy charts customization options are available as a drop-down menu with the following options:

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

Custom Chart page: customization common for legacy and classic charts

Available from legacy and classic charts.

To access the Custom Chart page:

- Click Export on a classic chart.
- Click the chart.
- Select Edit Chart in the drop-down menu (legacy chart).

The Custom Chart page opens in a new tab. Change the chart settings and click Refresh to see the changes applied in the same tab.

Title, Subtitle, Subtitle #2

Enter a title and optional subtitles to be displayed above the chart.

Time Period: Select a Time Period

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

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

Time Period: Beginning Date/Time

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

Time Period: Ending Date/Time

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

Sample Interval

Select the sample interval. Each sample interval is represented on a chart by a single point or bar. Data within a selected sample interval is summarized automatically.

Chart Size: Width

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

Chart Size: Height

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

Select the font size for the chart from the drop-down list.

Trend Line: Show Trend

Select the box to display a trend line on the graph. This shows potential future results as extrapolated from collected historical data.

Due to the broad array of factors that can affect the performance of devices, trend lines are intended as approximate predictions of future data only.

Display Chart Data: Raw Data

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

Display Chart Data: Chart Data

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

Migrate charts to modern charts

Orion Platform 2018.4 replaces legacy charts and certain classic/historical charts with their modern-style counterparts. If you are upgrading from a previous Orion Platform version and are using legacy or classic charts, they will be retained in your Orion Web Console.

SolarWinds recommends that you switch to modern charts at your earliest convenience.

- To find out how to distinguish between chart types, see A brief history of Orion Platform charts.
- To find out what charts have modern-style counterparts, see Modern charts replacing legacy and classic charts in Orion Platform 2018.4.

Migrate classic charts automatically

Use this option to migrate all historical/classic charts that have a modern counterpart simultaneously. Only classic charts that have a modern counterpart will be migrated.

1. Log in to the Orion Web Console using an account with Administrator privileges.
2. Click Settings > All Settings > Web Console Settings.
3. Scroll down to Migrate charts to modern style charts, and click Migrate.

Classic charts with a modern version are automatically upgraded to modern charts.

To revert to the classic version of the charts, find the Migrate charts to modern style charts in Web Console Settings, and click Roll Back.
Migrate charts manually

If you only want to migrate single legacy or historical/classic charts and want to retain others as is, migrate the charts manually.

1. Navigate to the view where you have the chart.
2. Click the pencil icon, and then click Add widgets.
3. In the widget palette, search for the chart name and filter the results by charts by clicking Charts below the Group by drop-down list.
   - The chart names might differ slightly, for example instead of Average of Average CPU Load (historical chart), you will find Average CPU load (modern chart).
4. Drag and drop the chart labeled as Modern to the view.
5. Click the x button for the deprecated chart, and then click Remove.
6. Click Done Adding Widgets, and then click Done Editing.

You have replaced the legacy or classic chart by its modern counterpart.
A brief history of Orion Platform charts

<table>
<thead>
<tr>
<th>Name</th>
<th>Example</th>
<th>notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy charts</td>
<td><img src="image" alt="Legacy chart" /></td>
<td>Legacy charts are not interactive. You can only edit them by clicking the chart and going to the Custom Chart view. These are only gif images rendered at the time of the page load. All chart controls are hidden behind the Edit button and are only accessible to the Orion Administrator. Starting with Orion Platform 2018.4, you cannot add these charts to the Orion Web Console views any more.</td>
</tr>
<tr>
<td>Historical, or classic charts</td>
<td><img src="image" alt="Historical chart" /></td>
<td>Interactive: You can zoom in/out easily, select relative time frames without having Orion Administrator rights. You can easily identify them by the zoom panel with drag handles at the bottom of each chart. If your classic chart has a modern-style equivalent, consider replacing it with the modern chart. Although you can add and use classic charts now, they will not be supported in a future version.</td>
</tr>
<tr>
<td>Modern charts</td>
<td><img src="image" alt="Modern chart" /></td>
<td>Modern charts use client-side rendering and are thus faster to load than their predecessors. Rendering offloaded to the client improves the performance of the Orion Web Console, and allows for more users logged in concurrently. They also handle responsive design much better than classic charts. Purpose-built and designed based on customer feedback. These charts reflect the time in the browser, not the server time.</td>
</tr>
</tbody>
</table>
95th Percentile Calculations in the Orion Platform

The 95th percentile, a well-known statistical standard used to discard maximum spikes, is based on 5 minute data samples. The calculation gathers these values every 5 minutes for the duration you select, throws away the top 5%, yielding the 95th percentile value at the beginning of the list.

The following example shows how the 95th percentile is calculated for a 10 hour work day from 8 am to 6 pm (600 minutes).

1. Over the 10 hours, the following 120 values were collected for inbound traffic (Mb/s):

   0.149 0.623 0.281 0.136 0.024 0.042 0.097 0.185 0.198 0.243 0.274 0.390
   0.971 0.633 0.238 0.142 0.119 0.176 0.131 0.127 0.169 0.223 0.291 0.236
   0.124 0.072 0.197 0.105 0.138 0.233 0.374 0.290 0.871 0.433 0.248 0.242
   0.169 0.116 0.121 0.427 0.249 0.223 0.231 0.336 0.014 0.442 0.197 0.125
   0.108 0.244 0.264 0.190 0.471 0.033 0.228 0.942 0.219 0.076 0.331 0.227
   0.849 0.323 0.221 0.196 0.223 0.642 0.197 0.385 0.098 0.263 0.174 0.690
   0.571 0.233 0.208 0.242 0.139 0.186 0.331 0.124 0.249 0.643 0.481 0.936
   0.124 0.742 0.497 0.085 0.398 0.643 0.074 0.590 0.771 0.833 0.438 0.242
   0.092 0.376 0.231 0.627 0.249 0.663 0.181 0.636 0.224 0.342 0.697 0.285
   0.108 0.211 0.074 0.490 0.271 0.133 0.338 0.242 0.519 0.376 0.331 0.227

2. The values are reordered from high to low.

   0.971 0.942 0.936 0.871 0.849 0.833 0.771 0.742 0.697 0.690 0.663 0.643
   0.643 0.642 0.636 0.633 0.627 0.623 0.590 0.571 0.519 0.497 0.490 0.481
   0.471 0.442 0.438 0.433 0.427 0.398 0.390 0.385 0.376 0.376 0.374 0.342
   0.338 0.336 0.331 0.331 0.331 0.323 0.291 0.290 0.285 0.281 0.274 0.271
   0.264 0.263 0.249 0.249 0.249 0.248 0.244 0.243 0.242 0.242 0.224 0.222
   0.238 0.236 0.233 0.233 0.231 0.231 0.228 0.227 0.227 0.224 0.223 0.223
   0.223 0.221 0.219 0.211 0.208 0.198 0.197 0.197 0.197 0.196 0.190 0.186
   0.185 0.181 0.176 0.174 0.169 0.169 0.149 0.142 0.139 0.138 0.136 0.133
   0.131 0.127 0.125 0.124 0.124 0.121 0.119 0.116 0.108 0.108 0.105
   0.098 0.097 0.092 0.085 0.076 0.074 0.074 0.072 0.042 0.033 0.024 0.014

3. The first 6 values are dropped, as these equal the top 5% of the values.

   0.771 0.742 0.697 0.690 0.663 0.643 0.643 0.642 0.636 0.633 0.627 0.623
   0.590 0.571 0.519 0.497 0.490 0.481 0.471 0.442 0.438 0.433 0.427 0.398
   0.390 0.385 0.376 0.376 0.374 0.342 0.338 0.336 0.331 0.331 0.331 0.323
   0.291 0.290 0.285 0.281 0.274 0.271 0.264 0.263 0.249 0.249 0.249 0.248
   0.244 0.243 0.242 0.242 0.242 0.238 0.236 0.233 0.231 0.231
   0.228 0.227 0.227 0.224 0.223 0.223 0.221 0.219 0.211 0.208 0.198
   0.197 0.197 0.197 0.196 0.190 0.186 0.185 0.181 0.176 0.174 0.169 0.169
   0.149 0.142 0.139 0.138 0.136 0.133 0.131 0.127 0.125 0.124 0.124 0.124
   0.121 0.119 0.116 0.108 0.108 0.105 0.098 0.097 0.092 0.085 0.076 0.074
   0.074 0.072 0.042 0.033 0.024 0.014

4. The 95th percentile is 0.771.
View monitored objects on Open Street map or on Network Atlas maps in the Orion Platform

Apart from Orion Maps, you can display monitored nodes, interfaces and volumes, SAM applications and components, and network links on Open Street maps and on Network Atlas maps.

Open Street Map

Display nodes on maps powered by Open Street Map.

Network Maps

Create customized maps in Network Atlas, and display them in the Orion Web Console.

Display the Worldwide Map of Orion nodes in the Orion Platform

Nodes and groups that contain information about their location in the OpenStreet format are displayed automatically. See Place nodes automatically on the Worldwide Map in the Orion Platform

Objects with the same position are displayed as one location.

Although there is one Worldwide map, you can add the Worldwide Map resource to multiple views, and display different objects and information on each view. For example, you can apply different zoom levels, use different titles and subtitles, or center the map on different coordinates.

If you cannot see the Worldwide Map resource on a view, add the resource. See Add widgets to Orion Platform views.

Add nodes manually

Add a new location into the map, and define the nodes positioned in the location.

1. Click Manage Map in the Worldwide Map resource.

2. Click Place Nodes on the Map Manually, and click into the map where you want to place the nodes.

3. Use the Grouping and Search tools to select nodes which you want to place on the map.

4. Provide a name for the location.

5. Click Place on Map.

6. Click Submit.
   
   If you want to further edit the map, click Save and Continue.
Edit the position of locations

If the exact position is not known or important, you can drag locations to their positions.

1. Click Manage Map in the Worldwide Map resource.
2. Click a map location, and click Edit Location.
3. Provide the Latitude and Longitude of the new location, and click Save.
4. Click Submit.
   If you want to further edit the map, click Save and Continue.

Add or remove nodes in locations, or rename locations

1. Click Manage Map in the Worldwide Map resource.
2. Click the map location you want to edit, and click Edit at the top right of the list of nodes at the selected map location.
3. Add or remove nodes in the location.
   - Select nodes to be added in the Available Objects section.
   - To remove nodes, click x next to the node in the Selected Objects section.
4. Click Save Changes.
5. To apply your changes in the resource, click Submit or Save and Continue if you want to further edit your worldwide map.

Delete locations

1. Click Manage Map in the Worldwide Map resource.
2. Select the map location.
3. Click Remove from Map, and then confirm the map location removal.
4. Click Submit.
   If you want to further edit the map, click Save and Continue.

Place nodes automatically on the Worldwide Map in the Orion Platform

If your devices contain information about their location in the OpenStreetMap format, they can be added into the Worldwide Map widget automatically.

You can specify the position for automatic geolocation with custom properties. See Place objects into the map using custom properties in the Orion Platform.
Objects with the same position appear as one location in the map.

To verify whether the automatic placement of objects is enabled:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Product Specific Settings, click Web Console Settings.
4. Scroll down to Worldwide Map Settings and make sure Automatic Geolocation is selected.

   Locations will display in the Worldwide Map resource within an hour after you select this option.

5. Click Submit to apply the current settings.

**Important:** Automatic geolocation does not change locations for manually placed objects. If you move an automatically placed location, its position will not be updated if you change the values for longitude and latitude.

In what format should the location on a Cisco device be configured?

You can use any format the mapquest API is able to parse.

<table>
<thead>
<tr>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>city (AA5), state (AA3)</td>
<td>city (AA5), state (AA3)</td>
</tr>
<tr>
<td>city, state, postalCode</td>
<td>Lancaster, PA, 17601</td>
</tr>
<tr>
<td>postalCode</td>
<td>17601</td>
</tr>
<tr>
<td>street, city, state</td>
<td>300 Granite Run Dr, Lancaster, PA</td>
</tr>
<tr>
<td>street, city, state, postalCode</td>
<td>300 Granite Run Dr, Lancaster, PA, 17601</td>
</tr>
<tr>
<td>street, postalCode</td>
<td>300 Granite Run Dr, 17601</td>
</tr>
<tr>
<td>latLng</td>
<td>40.07546,-76.329999</td>
</tr>
</tbody>
</table>

Place objects into the map using custom properties in the Orion Platform

If you have longitude and latitude for your nodes or groups defined as custom properties, you can use the coordinates to automatically place the nodes on the WorldWide Map.

You can create the custom properties using the Longitude and Latitude property templates.
1. **Export the values for the custom properties** Longitude and Latitude.
   a. Click Settings > All Settings, and then click Manage Custom Properties.
   b. Select Longitude and Latitude, click Export Values, and click Export.

2. **Import the .csv file** with longitude and latitude custom properties, and match these to Latitude and Longitude (World Map) column.
   a. In the Custom Property Editor, click Import Values, select the export file with Longitude and Latitude.
   b. Clear the Remove unchanged rows box, and click Next.
   c. Match Longitude and Latitude to the World Map columns.
   d. Click Import.

---

![Import Custom Properties](image-url)
3. Optional: Verify that the values were imported successfully.
   a. Click Settings > All Settings, and click Manage Custom Properties.
   b. Select Longitude and Latitude and click View / Edit Values.
   c. Add the Longitude (World Map) and Latitude (World Map) columns.

![ADD CUSTOM PROPERTY](image)

The values for Longitude (World Map) should match the Longitude values, and values for Latitude (World Map) should match the Latitude values.

4. Ensure that the Automatic Geolocation option is enabled.

When the automatic geolocations are updated, you will see the nodes in the Worldwide Map, as specified by the Longitude and Latitude (World Map) properties. The default interval for updating automatic geolocation is 1 hour. You can speed up the update by restarting the Module Engine Service, for example in the Orion Service Manager.

Network Atlas for the Orion Platform

Network Atlas is an application for creating custom maps and network diagrams. It is preinstalled with your Orion Platform product.

Maps provide a graphical depiction of the network. You can export or print maps, and use them to document your network. You can also view Network Atlas maps in the Orion Web Console.

What can you see on maps?

- Monitored SolarWinds NPM nodes, interfaces, and volumes, SAM applications and components, nested maps, and network links

What customization options are there?

- Customize the map background with default colors, textures, or images. Add custom background graphics, such as floor plans.
- Link dynamic real-time weather or natural disaster maps to your network maps as the background.
- Customize the shape, size, color, and style of map links to illustrate the status of the relative bandwidth of associated objects.
Select a graphical style for objects to reflect the network status on maps.
Nest maps, so that you can drill down to reveal increasing levels of detail, and the status of nested map child objects may be bubbled up to the parent map. You can for example nest floor maps into a map of a building, and be notified if devices on the floor map are down.

Install Network Atlas for the Orion Platform

Network Atlas is pre-installed on Orion EOC and SolarWinds NPM, and it can be run as a local application on those Orion servers.

Users can also run Network Atlas as a standalone application on a remote computer.

Network Atlas Requirements

Network Atlas users must have the Map Management rights in SolarWinds NPM or in Orion EOC.

⚠️ The user logged in to Network Atlas must be able to access the Network Atlas synchronization folder to ensure synchronization with the SolarWinds Orion database.

<table>
<thead>
<tr>
<th>Hardware/Software</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows Server 2012 and 2012 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td></td>
<td>Windows 8 or 8.1 (64-bit, Standard Edition is not supported)</td>
</tr>
<tr>
<td></td>
<td>Windows 10 (64-bit)</td>
</tr>
<tr>
<td>Memory</td>
<td>1 GB</td>
</tr>
<tr>
<td>Hard Drive Space</td>
<td>150 MB</td>
</tr>
<tr>
<td>Ports</td>
<td>Remote instances of Network Atlas require TCP on port 17777 to either the SolarWinds NPM or the Orion EOC server.</td>
</tr>
<tr>
<td>.NET Framework</td>
<td>.NET 4.5 or later</td>
</tr>
</tbody>
</table>

Network Atlas ports

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>Service/Process</th>
<th>Direction</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>17777</td>
<td>TCP</td>
<td>SolarWinds</td>
<td>Bidirectional</td>
<td>Remote instances of Network Atlas require TCP on port 17777 to either the SolarWinds NPM or the SolarWinds EOC server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Service</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Install Network Atlas on a remote computer

1. Log in to your SolarWinds NPM or Orion EOC server.
2. Start the Orion Web Console in the SolarWinds Orion program folder.
3. In the Map resource, click Download Network Atlas.
   
   ![Info](Note) If you do not see the download link in the Map resource, click Edit, select Show Network Atlas Download Link, and click Submit.

4. Save the installer (`NetworkAtlas.exe`) on the remote computer.
   
   ![Info] You can also locate the installer on your local server in the location: `\inetpub\SolarWinds\NetworkAtlas\NetworkAtlas.exe`

5. Run the installer on the remote computer, and click Next on the Welcome window.
   
   ![Info] If you have previously installed Network Atlas, you may be prompted to change, repair or remove your installation. Click Repair, click Repair again on the Ready to repair window, and complete the Setup Wizard.

6. Accept the terms in the license agreement, and click Next.
7. Provide a destination folder for the installation, and click Next.
8. Click Install on the Ready to Install window.
9. Click Finish when the Setup Wizard completes.

See [Create network maps for the Orion Platform](#).

Start Network Atlas for the Orion Platform

![Info] Users must have the Map Management right in SolarWinds NPM or in Orion EOC.

1. Log in to the computer hosting your Network Atlas installation.
3. Connect to your primary Orion server:
   a. Provide your Orion Web Console user name and password.
   b. Provide the IP address or hostname of your primary Orion server in the Address field.
   c. If you are connecting to an SolarWinds NPM server, select Orion as the Connect To target.
   d. If you are connecting to an Orion EOC server, select EOC as the Connect To target.
   e. Click Connect.
4. Now on the Network Atlas Welcome screen, select what map you want to open:
   - To open a recent map, select it in the Open Recent section.
   - To open a map available in a certain location, click Browse and navigate to the map.
   - To create a new network map, click Network Map in the Create New section. See [Create network maps for the Orion Platform](#).
Create network maps for the Orion Platform

Before you start creating maps, prepare a map management strategy. Consider the following recommendations:

- Map only static objects. If objects move, you need to adjust their location on maps, and it is difficult to keep maps up-to-date.
- Build maps to match the column width of your Orion Web Console views. Rescaling maps in views results in distorting of icons and texts.

To create a network map:

1. Start the Network Atlas in the SolarWinds program folder.
2. Provide your Orion Web Console credentials.
3. If you are launching Network Atlas on the local computer, type localhost into Address. If you are starting Network Atlas on a remote computer, provide the IP address of the main polling engine.
4. Click Connect.
5. Click Network Map in the Create New section.

A new empty network map will open in the Network Atlas.

Add objects on a map for the Orion Platform

Any objects monitored by SolarWinds NPM or SAM may be added to a Network Atlas map, such as:

- SolarWinds NPM nodes, interfaces, volumes, and Universal Device Pollers (UnDPs)
- SAM applications and components
- VoIP & Network Quality Manager operations
- Network Atlas maps
- Network links

To add objects on a map:

1. If you are creating a new map, click the Network Atlas button ( ), and click New Map.
2. If you are adding objects to an existing map:
   a. Click the Network Atlas button ( ).
   b. Click Open Map.
   c. Navigate to your existing map, and click Open.
3. Expand and navigate the node tree in the left pane to locate the network nodes and monitored objects you want to add to your map.
4. Drag selected objects onto the drawing area.
   - To add all the objects of a type on a node to your map, click + next to the node name to reveal all its associated monitored network objects, and drag all objects in the object group onto the drawing area.
   - A check mark (✓) next to a node or network resource indicates you have already added it to your map.
   - To view details about a map object, hover over it with the mouse pointer.
   - To locate a specific map object in your map, click its network resource in the left pane. This selects the map object.

Automatically connect objects on maps in the Orion Platform with ConnectNow

Using the ConnectNow tool, Network Atlas can automatically draw lines between directly connected nodes on your network.

ConnectNow displays connections based on data polled for nodes with enabled L2 and L3 topology pollers, and for unidentified nodes.

An unidentified node is a node that was found on the network but which is not managed by Orion. These devices might be switches, hubs, routers, or other devices without names or addresses. Unidentified nodes can be virtual, generated to signify an indirect connection in your map. For example, when a topology calculation cannot find any direct connections between two nodes, an unidentified node is generated between the two known nodes.

- The ConnectNow tool cannot draw indirect connections between nodes. For example, if nodes A and C are connected indirectly through node B, you must manually add node B to the map to create the connections.
- Orion Enterprise Operations Console (EOC) does not support ConnectNow.

Connect objects on maps automatically using ConnectNow

1. Add the nodes to an open network map.
   See Add objects on a map for the Orion Platform.

2. Click ConnectNow (✓) in the Home ribbon.

Update the Topology

ConnectNow displays data stored in the TopologyConnections database table. By default, the data are recalculated every 30 minutes. You can update the data manually.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Nodes.
4. In the More Actions drop-down list, select Update Topology.
The values in the TopologyConnections table will be re-calculated and your topologies will be updated.

Connect objects on maps manually in the Orion Platform

You can represent network links in your map by drawing lines between map objects. If a connected object is down, any connected links change color to red.

1. Make sure the Home ribbon is selected.
2. Click Straight ( ) or Curved Line ( ) in the Lines group, as appropriate.
3. Click an object with the line drawing tool to begin drawing the link.
4. Click and drag as needed to set optional anchor points along the link path.
5. Click a second object to finish drawing the link.
6. If you want the links connecting your mapped objects to communicate the status of connected interfaces:
   a. Right-click a link, and select Properties.
   b. Select Status in the left pane of the Link Properties page.
   c. Drag the appropriate interface objects from the left pane of the Network Atlas window to the link status assignment areas.

Reshape map links in the Orion Platform

You can use anchor points to change the shape of object links on your map. Use multiple anchor points to create more complex shapes and curves.

1. Select ( ) in the Tools group, or click the middle mouse button.
2. Click and drag the link you want to reshape.

Configure display of connections on maps for the Orion Platform

Links created on Network Atlas maps are not merely connectors between network objects. They can display status of the connection, the link speed, or utilization.

1. Right-click a link, and select Properties.
2. Click Status and review the objects from which the link gets its status. To change the objects, drag objects from the Network Atlas navigation tree to the appropriate endpoint box.
3. Click Appearance and set the default width and style for the link. Select the color for links that are UP. Down links are always red.
4. Click Hyperlink to specify what should open when you click the link in the Orion Web Console.
5. To add a label, right-click a link, and select Add Label. A default label appears. Edit the label text or move the link label.
6. To specify what should be displayed for connections:
   a. Expand Connection Display Options.
   b. To display the link speed, select Show Link Speed.
   c. To show the link utilization in percent, select Link Utilization.

   To hide all labels for the connections, clear the Include Link Labels, and click Don’t Show Additional Info.

You can set interfaces through which linked objects are connected. Links can then display the status, speed or link utilization of the connection. Interface states and performance data are determined from SolarWinds NPM polling data.

Interface performance information in maps can be communicated using the interface status or performance:

- Determine interface status in connections for the Orion Platform
- Specify interfaces that determine the status of connections on maps for the Orion Platform
- Display interface performance in links on the maps in the Orion Platform

Determine interface status in connections for the Orion Platform

Connections are shown as either solid or dotted lines. A solid line indicates that the connection is UP. A dotted line indicates that the connection is DOWN.

The connection status depends on the status of interfaces at both ends of the connection.

   The connection status is only shown as either UP or DOWN. To emphasize potential problems, DOWN status is granted a higher priority.

The following table shows how interface states are reflected in the status of a connection between NodeA, with InterfaceA, and NodeB, with InterfaceB.

<table>
<thead>
<tr>
<th>InterfaceA Status</th>
<th>InterfaceB Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>UP</td>
</tr>
<tr>
<td>UP</td>
<td>UP</td>
</tr>
<tr>
<td></td>
<td>DOWN</td>
</tr>
<tr>
<td>DOWN</td>
<td>DOWN</td>
</tr>
<tr>
<td>UNKNOWN</td>
<td>UP</td>
</tr>
<tr>
<td></td>
<td>DOWN</td>
</tr>
<tr>
<td></td>
<td>DOWN</td>
</tr>
</tbody>
</table>

Specify interfaces that determine the status of connections on maps for the Orion Platform

   1. Right-click a link in a map, and select Properties.
   2. Select Status in the left pane of the Link Properties page.
3. Drag the interface objects from the left pane of the Network Atlas window to the link status assignment areas.

Display interface performance in links on the maps in the Orion Platform

Map links can show either interface utilization or interface connection speed. A legend is available to interpret colors representing interface performance data.

1. Expand Connection Display Options in the bottom left pane.
2. Select display options:
   - Show Link Speed provides interface connection speed information in colored links.
   - Show Link Utilization provides interface utilization information in colored links. This option is default on new maps.

   *Utilization data is not shown for manually created links.*

   - Don't Show Additional Info provides only interface UP/DOWN status information on device links. This is the default option for previously created maps.
   - Include Link Labels enables or disables displaying connection labels.

Add a background to Network Atlas maps for the Orion Platform

You can select colors, textures, and locally-hosted or Internet-hosted images to serve as your map backgrounds.

- Select a background color
- Select a background texture
- Select a background image

   *To clear the current map background, click Home, and click Background > Clear Background (x).*

Select a background color

Network Atlas supports 24-bit color backgrounds.

1. Click Home > Background > Background Color ( ).
2. Select a color from the palette, or click More Colors to select a custom color.

The color is used as the background.
Select a background texture

1. Click Home > Background > Background Texture.
2. Enter the Width and Height of your map in the Map Size in Pixels area.
   - The default values are the smallest area bounding the existing map objects and labels.
3. Select a texture, and click OK.
   The texture is used as the background.

Select a background image

Add images accessible on the hard drive or on the Internet as the background for your maps.

**Requirements and recommendations**

- Files used for linked backgrounds must be continuously accessible by URL reference.
- Files used for static backgrounds must be available within the local file system.
- To ensure optimal quality of images, plan graphics to display at full size in the Orion Web Console.
- When determining map size and resolution, consider web page layouts and display screen resolutions.

- Example backgrounds are in the NetworkAtlas Backgrounds folder located in your default shared documents folder.

**Supported formats**

- Graphics Interchange Format (.gif, non-animated)
- Tagged Image File Format (.tiff)
- Joint Photographic Experts Group (.jpg)
- Microsoft Windows Bitmap (.bmp)
- Portable Network Graphics (.png)

Linked backgrounds are updated when you access the map, or refresh the browser page.

**Add an image as the background**

1. Open the map in the Network Atlas, and click Home.
2. To use a background image the disk, click Background > Background Image, and navigate to the image.
3. To use a background image from the Internet:
   a. Click Background > Linked Background.
   b. Type the URL of the image.
   c. Click Validate.
   d. Click OK.

The image displays as the map background.
Add a dynamic background for a map

Weather conditions can affect availability of a certain location. You can add weather maps displaying the current weather as a background for maps.

1. Navigate to the page which you want to link as the background, and copy the static link.
2. Open the map in the Network Atlas.
3. Click Linked Background, and paste the URL.
4. Validate the URL, and click OK.

The dynamic map will now display as the map background.

When you add the map to the Orion Web Console, the map will refresh every time the Orion Web Console refreshes.

Save Network Atlas maps for the Orion Platform

Network Atlas saves your maps directly to the server to which you are connected.

1. Click the Network Atlas button ( ), and click Save.
2. If you are saving the map for the first time, name the map, and click OK.
3. If you want to save your map to your hard drive:
   a. Click > Export > Export Map.
   b. Navigate to a location on your hard drive.
   c. Provide a File name, and click Save.

Open maps for the Orion Platform in Network Atlas

Maps are loaded from the Orion server to which you are connected. They appear in the left pane of the Network Atlas window.

1. Click + to expand the Maps group in the left pane of the Network Atlas window.
2. Double-click the map you want to open.

Disable the wireless heat map poller in NPM

The wireless heat map poller collects information about the signal strength on monitored access points. By default, this poller is disabled on your devices because of performance issues.
Network Atlas enables the wireless heat map poller on wireless controllers used in wireless maps because the information collected by the poller is required for including access points into wireless heat maps.

**When do I need to disable the wireless heat map poller?**

If you experience performance issues when working with wireless heat maps, disable the wireless heat map poller on the devices.

*Disabling the poller resolves performance issues, but your wireless heat maps will no longer be updated. The Orion Web Console resources and the Network Atlas will both display the last status generated before you disabled the wireless heat map poller.*

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Pollers.
4. Locate the wireless heat map poller in the pollers table, and click the item in the Assignments column, such as 1 Node. Clicking the assignments link opens the Assign Wireless Heat Map to Nodes view.
5. Select all nodes for which you want to disable the poller, and then click Off: Disable Poller in the table title.

*Clicking the grey Off icon for the nodes in the Poller Status column disables the poller for the nodes. The icon will turn to green On, and the poller will be disabled.*

**Set a floor plan as the background for visualizing wireless coverage in NPM**

The floor plan should reflect the real dispositions of the office or buildings on the map, so that you can correctly position the wireless access points and reflect the wireless signal coverage on your map.

**Requirements:**

The floor plan must be a graphic file in one of the following graphics formats:

- Graphics Interchange Format (.gif, non-animated)
- Tagged Image File Format (.tiff)
- Joint Photographic Experts Group (.jpg)
- Microsoft Windows Bitmap (.bmp)
- Portable Network Graphics (.png)

*To ensure the readability of wireless heat maps, use black and white images.*

To set a background for wireless heat maps:

1. Create the wireless heat map in the Network Atlas.
2. Click Background Image on the Home ribbon.
3. Navigate to the floor plan image, select the image, and click Open.
   The floor plan will appear as the background for your heat map.

Set the wireless heat map scale in NPM

The correct scale is necessary for an accurate display of the wireless coverage provided by your wireless access point.

You can use online maps, such as the full version of Google Maps, to measure your office building. Locate the building on Google Maps, right-click one wall, and measure the distance to the other wall of the building.

Requirements

- You have already inserted a background image for your wireless heat map (a floor plan).
- You know the distance of two objects displayed on the background image.

To minimize error, set the scale for the longest distance possible, such as the building or floor length.

To set the map scale:

1. Create the wireless heat map in the Network Atlas.
2. Click Set Scale in the Home ribbon. A blue line segment with squares as end points will appear in the plan.
3. Drag endpoints of the segment to the objects on the map whose distance you know.
4. Fill in the distance between the endpoints into the appropriate field, and select the units (feet or meters).

   Example: In floor plans, you usually know the dimensions of individual rooms. Drag and drop the line segment endpoints so that the endpoints are located on the opposite walls, and fill in the width of the room.

5. Click Set Scale to apply the scale to the wireless heat map.

Add wireless access points for NPM wireless heat maps

To generate a wireless heat map, add wireless access points used by client devices into the map.

Requirements

- The wireless LAN controllers must already be managed in your Orion Platform product.
- Only Cisco controllers are supported.
- The wireless heat map poller must be enabled on the wireless LAN controllers that you use in the map.
- To display connected wireless clients on a heat map, add at least four access points, or three access points and a signal sample on the map.
To add wireless access points:

1. Create a wireless heat map in the Network Atlas.
2. Go to the navigation tree on the left of the Network Atlas main screen.
3. Locate the wireless access points that you want to add to the map.

   To find access points on a node, navigate to Orion Objects > vendor name, such as Cisco > appropriate node > Wireless Access Points.

4. Drag the access points to their location on the map.
   The selected access points will appear on the map. You can now generate the map.

   To make the map more accurate, take signal samples.

Improve the accuracy of NPM wireless heat maps by taking samples of the signal strength on real devices

Wireless heat maps display the ideal wireless signal coverage, they do not count with physical obstacles, such as office walls. To make wireless heat maps more real, measure the signal strength on real devices, such as cell phones, laptops, or tablets connected to your wireless network. The measured values are stored as signal samples and used for calculating the signal coverage on wireless heat maps.

Signal samples represent the signal strength measured in a specified location.

Take signal samples in places where you expect the signal to be blocked by walls or other obstacles, or in places where the signal strength does not correspond with your heat map.

Take signal samples with cell phones, because polling the signal is usually faster for them.

Simple signal samples

Take a wireless device, walk it to a certain location, and take a signal sample there. Then, walk the device to another location, and take another signal sample. This procedure is called "walking edition" because it requires you to walk through the office.

Multiple signal samples

If you have multiple devices connected to your wireless access points, take multiple signal samples at once (called "sitting edition" because you can do it sitting at your desk).

Signal samples stay in the map and influence the calculation of wireless heat maps even after the client moves from its position. When you move access points in a map, the signal samples might not be accurate any more. Delete obsolete signal samples, and add new ones.

Requirements

- You need to have a wireless heat map created and open in the Network Atlas.
- You need to have wireless access points added into the map.
You need to have clients, such as cellular phones, tablets, laptops, connected to the access points positioned in your wireless heat maps.

Take simple signal samples

1. Click Take Signal Sample in the Home ribbon. The Signal Sample wizard will display on the right side of the Network Atlas screen as a tab.
2. Walk your device to the location where you want to measure the wireless signal strength and click Next.
3. Select the wireless client (cellular phone, laptop, or tablet) in the drop-down list, and click Next.
4. Drag the client into its current location on the map, and click Next. Network Atlas will start measuring the wireless signal strength in the spot. It can take a few minutes, depending on the device.
5. To add another signal sample, click Repeat, walk the device to a new location, and repeat steps 3 - 4.
6. To apply the measured signal strength to the heat map, click Generate Map.
7. Network Atlas will regenerate the map. Click Close to hide the Signal Sample wizard tab.

Take multiple signal samples at the same time

1. Click Take Signal Sample in the Home ribbon. The Signal Sample wizard will display on the right side of the Network Atlas screen as a tab.
2. Click Use Multiple Devices to Take Signal Samples.
3. Drag the clients to their positions on the wireless heat map, and click Next.

   - If there are too many devices, use the search box to find the devices you want to use for creating signal samples.
   - Measuring the wireless signal strength can take a few minutes.
   - If the signal measuring fails, you can either repeat the measurement for the device, or restart the wizard.

4. Network Atlas will automatically regenerate the map according to the defined signal samples. Click Close to hide the Signal Sample wizard tab.

Troubleshoot NPM wireless heat maps

If your wireless signal coverage on your wireless heat maps is not as expected, you can take the following troubleshooting measures.

- Make sure that the map scale you have entered is precise.
- Make sure that your access points are located correctly.
- Verify that signal samples are up-to-date.
- The signal samples stay in the map even after the device you measured the signal strength on moves away. If you change the position of your access points, or the dispositions of your office, the signal samples might not be accurate and could affect the calculated wireless heat map.
Delete obsolete signal samples.

To delete a signal sample, open the wireless heat map in the Network Atlas, select the signal sample, and press the Delete key.

Add new signal samples. See Improve the accuracy of NPM wireless heat maps by taking samples of the signal strength on real devices.

Advanced mapping techniques in Network Atlas for the Orion Platform

- Zoom in and out of a Network Atlas map
- Create nested maps in the Network Atlas
- Display the status of child objects on Network Atlas maps, and change metric thresholds
- Add independent map objects and floating labels into Network Atlas maps
- Change the appearance of objects on Network Atlas maps
- Customize the width, color, and line styles of network links in Network Atlas maps
- Customize labels
- Customize the page that opens when you click on a Network Atlas map object
- Link or embed Network Atlas maps in web pages using the map URL

Zoom in and out of a Network Atlas map

Zoom into a map to enlarge details or to zoom out to reduce its size. Zoom level is a visual aid, and it is not saved with the map.

Use any of the following methods:

- Press and hold CTRL while rotating the mouse wheel button.
- Click the Zoom slider on the status bar, and then slide the zoom control to the zoom level you want.
- Click View, and select the type of zoom you want to use from the Zoom group.

Create nested maps in the Network Atlas

Nested maps allow you to navigate through a map to see multiple levels of detail.

For example, a map of the United States can include an icon for a child map of Oklahoma. You can then click the Oklahoma object to open the child map.
The map of Oklahoma can become a parent map to a network diagram.

Each child map can include a view of the objects, either devices or other maps, deployed on it.

Click any nested object to view the next level of map detail, until you reach the final network device and see all available network information.

The total number of objects on a map, including objects on child maps, affects how fast the map loads in the Orion Web Console. If your maps load slowly, decrease the number of map objects.

1. Create all maps to be nested in the Network Atlas.
2. Open the parent map, and drag a map from the Maps group onto the parent map.
3. Position the new map object on the parent map, and save the map.
4. If you want the status of a child map to also indicate the status of its child objects, complete the following steps:
   a. Right-click the child map icon on the map, and select Properties.
   b. Select Include Child Status on the Status properties page, and click OK.
      The object status icon now includes the secondary status indicator.

Display the status of child objects on Network Atlas maps, and change metric thresholds

The status of a map object icon reflects its current state, such as up or down. You can add a secondary status indicator to a map object to reflect metrics such as response time, CPU load, or the state of any child objects. This secondary status indicator appears at the bottom right corner of the status icon.

To add the secondary status indicator:

1. Right-click the map object, and select Properties.
2. Select Include Child Status on the Status properties page, and click OK.
To change the thresholds of the metrics:

1. Right-click the map object, and select Properties.
2. Click Metrics to view the Metrics properties page.
3. To change the warning or critical threshold for a metric, click the threshold value, and type a new value.
4. To ignore a metric, clear the metric.
5. Click OK.

- The secondary status indicator respects the Orion Web Console Status Rollup Mode setting for displaying status.
- All child objects and selected metric thresholds are taken into account to determine secondary status.

Add independent map objects and floating labels into Network Atlas maps

Independent objects and floating labels do not have associations to network nodes or resources.

To add an independent object:

1. Click Home.
2. Click Add Object in the Objects group to add a gray map object to the map.

To add an independent label:

1. Click Home.
2. Click Add Label in the Labels group. A label is added to the map.

Change the appearance of objects on Network Atlas maps

Changing the graphics that represent map objects allows you to increase the information density of your map without increasing the map complexity.

Set the default representations of map objects

1. Click the Orion Network Atlas button, and click Network Atlas Settings.
2. Click Graphic Styles in the left column.
3. Select an appropriate default style for each available map object.

For example, you can set an object icon to visually designate the type of the monitored device. You can then select a status style, such as 3D Pad Underneath, to illustrate the object status.
Change the representation of single map objects

1. Right-click a map object, and select Properties.
2. Click Appearance in the left column of the Properties page.
3. If you want the map object to appear as a fixed-size, LED-type graphic, complete these steps:
   a. Select Orion LED Status Icon.
   b. Select a style from the Orion LED Status Icon Style list, and click OK.
4. If you want the map object to appear as a scalable shape, complete these steps:
   a. Select Shape.
   b. Select a style from the Shape Style list, and click OK.
   c. Drag a corner handle on the map object to resize the shape.
5. If you want the map object to appear as a scalable graphic, complete these steps.
   a. Select Graphic.
   b. Click Select Graphic, select an appropriate graphic, and click OK.
   c. Select a status style from the Graphic Style list, and click OK.
   d. Drag a corner handle on the map object to resize the graphic.

Paste custom icons from the Windows clipboard into Network Atlas maps

You can paste graphics from the Windows clipboard into Network Atlas maps, and display an overlay behind them to depict their status.

Icons that you paste into Network Atlas are saved to the SolarWinds Orion database, and made available for reuse in other maps under the "Imported" icon grouping. Pasted icons saved to the SolarWinds Orion database can be used by remote instances of Network Atlas.

1. Open the icon image in a graphics program, such as Visio or Photoshop.
2. Copy the image to the Windows clipboard with the Copy command.
3. Open the appropriate map in Network Atlas.
4. Paste the image as a new object following these steps:
   a. Right-click on the map and then click Paste.
   b. Select Paste the Image From the Clipboard as a New Object.
   c. Enter a name for the image.
   d. Click OK.

The added icons are also saved on the Orion server in the path
%APPDATA%\SolarWinds\NetworkAtlas\Maps\Orion\<orion server address>\NetObjects\Imported.
%APPDATA% is typically located in C:\Users\<logged on user>\AppData\Roaming
Delete a custom icon

1. Determine which file on the Orion server contains the icon (for example, mypicture.wmf), and delete the file.
2. Start the Database Manager, and add the default server.
3. Right-click the SolarWinds database, select New query, and execute the following query:
   
   ```sql
   delete FROM [dbo].[MapStudioFiles] where FileName = 'NetObjects\Imported\mypicture.wmf'
   ```

   Replace mypicture.wmf with the name of your icon file.

4. Start the Network Atlas on the Orion server to delete the icons from the database.
   The icon is deleted.

Add custom icons from graphics files to Network Atlas maps

The custom graphic files must meet the following requirements:

- Supported image formats: Windows Media File (.wmf) or Graphics Interchange Format (.gif).
- Name the graphic files according to their roles.
- The file name must not contain any dash (-) characters.

If you have used dash characters in your file names and are upgrading to a SolarWinds Orion product released during 2016, the file names are no longer recognized.

Add custom icons from graphics files

1. Prepare the icons and save them as .gif or .wmi files.
2. On your SolarWinds server, paste the icons into the following folder:
   
   `%APPDATA%\SolarWinds\NetworkAtlas\Maps\Orion\<orion server address>\NetObjects\User Graphics`

   `%APPDATA%` is typically located in C:Users<logged on user>\AppData\Roaming.

   You can now assign the custom icons to objects on Network Atlas maps.

Assign a custom icon to an object

1. Right-click the object on the map, and then click Select Graphic.
2. Select User Graphics in the left pane.
3. Select the graphic image, and click OK.

The custom icon displays on the map.
Customize status icons on Network Atlas maps

1. Prepare the icons and save them as .gif or .wmi files.

   i The recommended status icon size is 16 x 16 pixels.

2. To specify the status an image is used for, add a suffix to the image file name:

<table>
<thead>
<tr>
<th>Role</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical status</td>
<td>iconNamecritical.gif</td>
</tr>
<tr>
<td>Down status</td>
<td>iconNamedown.gif</td>
</tr>
<tr>
<td>External status</td>
<td>iconNameexternal.gif</td>
</tr>
<tr>
<td>Unknown status</td>
<td>iconNameunknown.gif</td>
</tr>
<tr>
<td>Unmanaged status</td>
<td>iconNameunmanaged.gif</td>
</tr>
<tr>
<td>Unplugged status</td>
<td>iconNameunplugged.gif</td>
</tr>
<tr>
<td>Unreachable status</td>
<td>iconNameunreachable.gif</td>
</tr>
<tr>
<td>Up status</td>
<td>iconNameup.gif</td>
</tr>
<tr>
<td>Warning status</td>
<td>iconNamewarning.gif</td>
</tr>
</tbody>
</table>

3. On your SolarWinds server, paste the icons into the following folder:

   %APPDATA%\SolarWinds\NetworkAtlas\Maps\Orion\<orion server address>\NetObjects\User Graphics.

   Customized icons are used for the status defined by the file name suffix on maps in the Network Atlas and in the Orion Web Console map resources.

Customize the width, color, and line styles of network links in Network Atlas maps

1. Right-click a link, and select Properties.
2. Select Appearance in the left column of the Properties page.
3. Select a line width in pixels from the Width list.
4. Select a line color from the Color list.
5. Select a line style from the Style> list.
6. Click OK.

   i The color setting only changes the color of links that have the Up status.
Customize labels

To move a label, drag it to the new location.

Edit a label text

1. Double-click the label.
2. Press <SHIFT>+<ENTER> to separate multiple lines within the same label.

Customize text attributes, borders, and background colors

1. Right-click the label, and select Properties.
2. Select Appearance in the left column of the Properties page.
3. Make your changes:
   - To change the font attributes, click the … button, select the font attributes, and click OK.
   - To change the text alignment, select an alignment from the Text Alignment list.
   - To change the text color, click the Text Color box, and select a color.
   - To add a label border, select the border width in pixels from the Border Width list.
   - To change the label border color, click the Border Color box, and select a color.
   - To remove label borders, select 0 from the Border Width list.
   - To add a label background, clear Transparent Background.
   - To change the label background color, click the Background Color box, and select a color.
   - To remove a label background, select Transparent Background.
4. Click OK.

Customize the page that opens when you click on a Network Atlas map object

By default, map objects are linked to the most relevant details page for the object. Customize the URL hyperlink to link to external web sites and pages.

1. Right-click the map object, and select Edit Hyperlink.
2. To link to the relevant Orion page for the map object, select Logical Page in Orion.
3. To link to a custom URL, select Manually Set Address, and type the URL.
4. Click OK.

Link or embed Network Atlas maps in web pages using the map URL

The map URL is in the form:

http://orionServer/Orion/NetPerfMon/MapView.aspx?Map=mapName
orionServer

This is the IP address or host name of your SolarWinds NPM server.

mapName

This is the display name of the map. If the name contains space characters, substitute %20 for the spaces when specifying the name.

Customize map tooltips in the Orion Platform

When you hover over map objects in the Orion Web Console, a tooltip with the current identification and status of the object appears.

Customize tooltips for all map object types in the Orion Web Console to display additional information using alert variables, custom properties, and other text.

- Tooltip customizations are global, and affect all maps.
- Orion EOC does not support custom web console tooltips.
- To enter a carriage return, use \${CR}.

Add additional information to map object tooltips

1. Log in to the Orion Web Console as an administrator.
2. Locate the Map widget, and click Edit.
3. Click Customize Map Tooltips.
4. Type the variables and any text in the text field for the map object type.
5. Click Submit.

Import Network Atlas maps into Orion EOC

Maps created for use in SolarWinds NPM must be converted before they may be used in Orion EOC.

Map import requirements and configuration for EOC

The Orion to EOC Map Converter utility imports maps into Orion EOC v1.5 from other SolarWinds Orion products.

Environment requirements

- Orion EOC must currently be managing at least one SolarWinds Orion server.
- If Orion EOC is configured to use Active Directory accounts to access Orion servers, confirm that you have entered the password for the AD account in the Orion Logins section of EOC. Additionally, only AD accounts that were individually added to the Orion Server may be used to import a map. Active Directory group accounts are not compatible with Map Converter.
User requirements

To run the Orion to EOC Map Converter utility, the user must also meet the following specifications:

- The user must run the Map Converter using a Windows Administrator account that also has Orion EOC Administrator role permissions.
- The user must log into the Map Converter using an Orion EOC account that was individually added to Orion EOC. Active Directory group accounts are not compatible with Map Converter.
- The user must have Orion EOC access to at least one Orion server.
- The user must have Node Management rights on the remote Orion server.

Configure environment for the map import

1. Copy `SolarWinds-OrionToEOCMapConverter-1.5.exe` to your Orion EOC server.

   ![Download](http://downloads.solarwinds.com/)

2. Execute `SolarWinds-OrionToEOCMapConverter-1.5.exe`, and complete the installer.

3. Provide members of the Users group Full Control of files in the folder
   `<volume>:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files`. See [Microsoft TechNet Library](http://microsoft.com) for more information.

4. Allow the Everyone group Full Control to the folder
   `<volume>:\Windows\Temp\SolarWinds\NetworkAtlas\EOC\SolarWinds\NetworkAtlas\MapsWeb\EOC\localhost` and all of its child objects. See [Microsoft TechNet Library](http://microsoft.com) for more information.

Import maps into Orion EOC

1. Log in to the Orion EOC server with a Windows Administrator account that has Orion EOC Administrator role permissions.
2. Start the converter utility by running `Convert Orion Maps to EOC` in your SolarWinds program folder.
3. Select the Orion server hosting your maps from the Orion list.
4. Select the maps you want to import into Orion EOC.

   ![To edit the name of an Orion EOC map you are importing, click the map name in the New Name column, and edit the name.](http://microsoft.com)

5. Click Import.
Troubleshoot importing maps into Orion EOC

Map name conflict

Maps you import from different Orion servers may share the same name.

Resolution: Rename the maps so that each has a unique name in Orion EOC.

- Any pre-existing child/parent relationships for any renamed map will break. You must manually reconfigure parent/child relationships after importing.

Windows 2008 issues

Windows 2008 customers may encounter problems either after manually clicking the Refresh button or after selecting a different Orion server. If the utility crashes, restart it and resume importing.

User Access Control (UAC)

If using an operating system that has UAC, you must run the program using Run as Administrator.

Set when a Network Atlas map is displayed as Up on parent maps using the Up status threshold

The UP status threshold is the percentage of map objects that must be in an up state on a given map for the map to be represented as up on the parent map.

1. Right-click any empty portion of the map, and select Map Properties.
2. Slide the Map Status Will Be UP slider to configure the up state threshold on the Map Properties page.

Display restricted nodes on maps in the Orion Platform for users with account limitations

If Orion Web Console users have account limitations that prevent them from seeing network nodes, set whether the users should see the restricted nodes on maps.

Users with restricted access to the nodes will only see the restricted nodes, but cannot retrieve any additional information about the nodes.

Hide nodes from users who have account limitations

1. Right-click any empty portion of the map, and select Map Properties.
2. Select Remove Nodes That Users Do Not Have Permission to View.

Reveal nodes to all users

1. Right-click any empty portion of the map, and select Map Properties.
2. Select Allow All Users to View All Nodes On This Map.
Advanced layouts in Network Atlas maps

- Position objects on Network Atlas maps
- Display grid
- Align objects on Network Atlas maps
- Distribute objects on Network Atlas maps
- Arrange objects on Network Atlas maps according to a layout style

Position objects on Network Atlas maps

Drag objects from the tree on the left to the appropriate position on the map.

To nudge a map object, select the object, and press <Ctrl> + <arrow>.

To reposition a map object:

1. Click the map object.
2. Click the Edit ribbon.
3. In the Size & Position area, enter the X and Y coordinates.

<i>Map center is designated as (X,Y) = (0,0).</i>

Display grid

A grid guide helps you maintain structural and spatial relationships as you arrange your map objects.

Grids are neither saved with a map, nor displayed in the Orion Web Console.

1. Click the View ribbon.
2. Click Show Grid in the Grid group.

Customize grid

1. Click View.
2. To display grid lines, click Grid Option > Grid Lines.
3. To display grid points, click Grid Options > Grid Points.
4. To change the grid size, click Grid Options > Grid Size, and select a grid size.
Align objects on Network Atlas maps

1. Click the Edit ribbon.
2. Select the map objects you want to align.
3. Click the button in the Align group to arrange the object.

<table>
<thead>
<tr>
<th>Button</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Align Left</td>
<td>Aligns all selected objects on the left edge of the group</td>
</tr>
<tr>
<td></td>
<td>Align Right</td>
<td>Aligns all selected objects on the right edge of the group</td>
</tr>
<tr>
<td></td>
<td>Align Bottom</td>
<td>Aligns all selected objects on the bottom edge of the group</td>
</tr>
<tr>
<td></td>
<td>Align Top</td>
<td>Aligns all selected objects on the top edge of the group</td>
</tr>
<tr>
<td></td>
<td>Center Vertically</td>
<td>Centers all selected objects vertically</td>
</tr>
<tr>
<td></td>
<td>Center Horizontally</td>
<td>Centers all selected objects horizontally</td>
</tr>
</tbody>
</table>

Distribute objects on Network Atlas maps

1. Click Edit.
2. Select the map objects you want to distribute.
3. Click a button in the Distribute group to arrange the selected objects.

<table>
<thead>
<tr>
<th>Button</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Distribute Horizontally</td>
<td>Distributes all objects so that they are equidistant from the left edge of the leftmost object to the right edge of the rightmost object</td>
</tr>
<tr>
<td></td>
<td>Distribute Vertically</td>
<td>Distributes all objects so that they are equidistant from the top edge of the topmost object to the bottom edge of the bottommost object</td>
</tr>
</tbody>
</table>
Arrange objects on Network Atlas maps according to a layout style

1. Click Edit.
2. Click a layout style from the AutoArrange group.

<table>
<thead>
<tr>
<th>Button</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Circular icon]</td>
<td>Circular</td>
<td>Emphasizes the clusters inherent in the topology of a map. It emphasizes prominent links between main objects and its peripherals. Object groups have radial placements. Use circular layouts for maps containing ring and star network topologies.</td>
</tr>
<tr>
<td>![Symmetrical icon]</td>
<td>Symmetrical</td>
<td>Emphasizes the symmetrical patterns inherent in the map topology. It emphasizes an even distribution of objects, and minimizes edge crossings. Object groups have star spiral placements. Use symmetrical layouts for maps that have fairly homogenous or uniform clusters.</td>
</tr>
<tr>
<td>![Hierarchical icon]</td>
<td>Hierarchical</td>
<td>Emphasizes mapped dependency relationships by placing objects at different levels. Use hierarchical layouts to depict data dependencies.</td>
</tr>
<tr>
<td>![Orthogonal icon]</td>
<td>Orthogonal</td>
<td>Emphasizes compact drawings, and uses only horizontal and vertical edges. Objects are enlarged if necessary to provide enough space for edge connections. Use orthogonal layouts for maps that need to depict multiple clusters in a space-efficient manner.</td>
</tr>
<tr>
<td>![Tree icon]</td>
<td>Tree</td>
<td>Emphasizes parent and child relationships. Child objects are arranged farther from the root object than their parent objects. Use tree layouts for maps that have a central control object.</td>
</tr>
<tr>
<td>![Reorganize icon]</td>
<td>Reorganize</td>
<td>Moves all mapped objects back to the center of the map view.</td>
</tr>
<tr>
<td>![Arrange Labels icon]</td>
<td>Arrange Labels</td>
<td>Restores the default relative position of all object labels.</td>
</tr>
</tbody>
</table>

Display Network Atlas maps in the Orion Web Console

To see a graphical overview of devices on your network, create a Network Atlas map, add the Map widget on the view, and specify the map you want to see in the widget.

1. Log in to the Orion Web Console as an administrator.
2. Click Edit in the Map widget.
3. Select your map from the Select Map list.
4. Click Submit.

The selected map will now appear in the Map resource.

Display Network Atlas maps in the Orion EOC Web Console

Network Atlas maps must be converted to display in an Orion EOC Web Console. See Import maps into Orion EOC.

1. Log on to the Orion EOC web console with an administrator account.
2. Click Settings.
3. Click Manage Views.
4. Select Home, and click Edit View.
5. Click Resource.
6. Click Network Map in the Added list.
7. Select the map from the Select Network Map list, and click Save.
8. Click OK, Save Changes.
9. If prompted to confirm your changes, click OK.
10. Click the Home view to see the map.
Orion Maps for Orion Platform products

Orion Maps are a troubleshooting feature that displays a map of physical and logical relationships between entities monitored by the Orion Platform products you have installed. Orion Maps help you quickly isolate and identify critical health and performance issues.

Orion Map types

Auto-generated Orion Maps

Orion Maps automatically generate contextual maps that display critical relationships for monitored entities in the Orion Platform. Go to an entity details page and click the Map subview to display a map of relationships relevant for the entity.

Custom Orion Maps

Starting with Orion Platform 2019.2, you can create custom Orion Maps. Select entities to map and the Orion Maps feature displays physical and logical relationships between them. You can add the custom map on any Orion Web Console view using the Orion Map widget.

Auto-generated Orion Maps

The auto-generated Orion Maps open in the Orion Web Console as a subview and display both physical and logical relationships between entities.

Auto-generated Orion Maps are created without any user intervention: entities are added or removed as changes occur in the environment.
To access auto-generated Orion Maps, go to an entity Details view and click the Map subview in the menu on the left.

1. **Map icon**: Click the icon to view the Orion Map.

2. **Canvas**: Displays the map of relationships of the entity.

3. **Seed object**: The entity whose relationships the map displays. This is the entity from which you accessed the map.

   The color or the ring around the entity signifies the entity health, based on thresholds set for the entity. See [Thresholds](#) for details.

   For more details about an entity on the map, click the entity. The map adjusts accordingly and details about the entity are displayed in the Inspector Panel (7).

4. **Healthy topology connection**: For topology connections, the line width represents the interface bandwidth. T

   See [Understand connections on Orion Maps](#).

5. **Metric pill**: By default, it displays the outbound traffic and percent utilization. If polled values for the metric exceed the threshold, the pill displays errors and discards. Hover over the metric pill to show which metric it displays.
Connection with issues: The color signifies that a threshold has been exceeded. Yellow means warning and red signifies a critical threshold. See Thresholds for more details.

Click the connection to see details in the Inspector Panel (8).

Tools to adjust the map: Zoom in, zoom out, pan, or change layout. See Adjust the Orion Map.

Inspector Panel: Displays details about the entity or connection selected on the map, according to the active navigation bar.

When you open the Map from an entity details page, the Inspector Panel only displays the entity name, IP, vendor, and machine type.

- To show more details about an entity, click the navigation bars in the Inspector Panel (8, 9, 10, 11).
- To show more details about a connection, select it on the map. The details displayed in the Inspector Panel depend on the connection type.
- To show all entities on the map, click into the map. The Inspector Panel displays a list of all entities on the map called the Map Summary.

Related: Click this button to display entities related to the selected entity in the Inspector Panel: descendants, ancestors, and dependencies.

To add a related entity to the map, select the check box in front of the entity, and click Apply.

Connected: Click this button to display entities connected to the selected entity by a protocol-based relationship or actual data flow, such as topology (NPM) or Application Dependency Connections (SAM), in the Inspector Panel.

To add a connected entity to the map, select the check box in front of the entity, and click Apply.

Alerts: Click this button to display a list of active alerts associated with the entity in the Inspector Panel.

Recommendations (only with VMAN): If you have VMAN installed, this section presents recommendations for the entity.

Custom Orion Maps

Starting with Orion Platform 2019.2, you can create Orion Maps either based on the auto-generated maps, or from scratch.

- Maps summary view
- Edit Mode
- View Mode
- Orion Map widget
View a list of maps, create maps, and edit maps from the Maps view.

To access Orion Maps created by users, click My Dashboards > Orion Maps in the Home section.

1 **List of maps**: Review available Orion Maps. By default, the list shows maps created by you. If you have Administrator rights, you can display Orion Maps created by other users (4).

   Click a map name to [view the map](#) (View mode).

2 **Button bar**: Create a new map, or select a map in the list (1) and edit or delete it.

3 **Sort, filter, and search controls**: Use the filter and search options to find Orion Maps. Sort maps by name, time since last update, or creation date.

4 **All Users**: Toggle to display all maps or only maps created by you. This toggle is available only to administrators.
Add entities or adjust connections in Edit mode

Edit mode is where you create or edit maps. To enter Edit mode:

- On the [Maps view](#), select a map and click Edit.
- In [View mode](#), click More > Edit.

1. **Entity Library**: Drag entities from the library to the canvas.
2. **Canvas**: Place entities in the correct position. If there are relationships between entities on the map, the connections are automatically added to the map as well.
3. **Button bar**: Save the map or use commands in the More menu, such as create a new map, save the map under another name, delete the map, or switch to [View mode](#).
4 **Map controls:** Zoom in, zoom out, and center and adjust the map to the view.

<table>
<thead>
<tr>
<th>Shortcut</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>Zoom in.</td>
</tr>
<tr>
<td>-</td>
<td>Zoom out.</td>
</tr>
<tr>
<td>Ctrl + Mouse wheel up</td>
<td>Zoom in.</td>
</tr>
<tr>
<td>Ctrl + Mouse wheel down</td>
<td>Zoom out.</td>
</tr>
<tr>
<td>Space bar + Click + Drag</td>
<td>Pan the map in the viewport.</td>
</tr>
</tbody>
</table>

**Map Editor Only**

<table>
<thead>
<tr>
<th>Shortcut</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Del</td>
<td>Remove the selected object(s) from the map. Excludes auto-discovered connections.</td>
</tr>
<tr>
<td>Ctrl + S</td>
<td>Save the map.</td>
</tr>
<tr>
<td>Ctrl + Shift + S</td>
<td>Save the map under a new name.</td>
</tr>
<tr>
<td>Esc</td>
<td>Clears object selection.</td>
</tr>
<tr>
<td>Arrows</td>
<td>Nudge the selected object.</td>
</tr>
<tr>
<td>Shift + arrows</td>
<td>Move the selected object.</td>
</tr>
<tr>
<td>Ctrl + Z</td>
<td>Undo previous map modification</td>
</tr>
<tr>
<td>Ctrl + Y</td>
<td>Redo previously undone map modification</td>
</tr>
</tbody>
</table>
View popups and display details on mapped entities in View mode

View mode displays a full screen view of user-created maps for easy troubleshooting and investigation.

1 **Entity**: Click an entity to display details in the Inspector Panel.

2 **Inspector Panel**: Displays details about the entity or connection selected on the map. See [Inspector Panel](#) above.
   - Click inside the canvas to review mapped entities on the Map Summary.
   - Click an entity to view related and connected entities.
   - Review alerts.
   - If you have VMAN installed, review VMAN recommendations.

   In the View mode, you cannot add related entities to the map. Entities in the Inspector Panel do not have check boxes. This is only available from the auto-generated map subviews.

3 **Popup**: Hover over an entity to see additional details.

   You can also execute commands from the command menu, such as go to details view, edit the entity, mute alerts for the entity, or unmanage the entity.
4 **Button bar:** Click Share to copy the map address to the clipboard, click More > Edit to switch to Edit mode.

5 **Map controls:**

<table>
<thead>
<tr>
<th>Key</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>Zoom in.</td>
</tr>
<tr>
<td>-</td>
<td>Zoom out.</td>
</tr>
<tr>
<td>Esc</td>
<td>Remove entity selection.</td>
</tr>
</tbody>
</table>

**Orion Map widget**

When you [create a custom Orion Map](#), you can [add it to a view](#) in the Orion Map widget.

Click an entity on the map to go to the entity details view.

Hover over an entity to display a popover, or to run commands for the entity from the Commands drop-down.

**What can you do with Orion Maps?**

- View details for entities on mapped entities, such as the Map Summary, connected entities, dependent entities, related alerts, or VMAN recommendations
- View connections between displayed entities, such as topology connections, application dependency connections, or Orion dependency connections
- **Customize the auto-generated maps**, such as add/remove related entities, create a group from mapped entities
- **Adjust the auto-generated map** by zooming in, zooming out, or panning
- **Create a custom Orion Map, add entities, adjust their position, and save the map**
- **Add the Orion Map to your views as a widget**
- **Create a custom alert** based on the Orion Maps entity
- **Send mapped objects via email as a report** and **send the Orion Map as a PDF**

### View details for Orion Platform entities on Orion Maps

The [Orion Maps](#) feature provides the following details:

- View a list of entities on the map
- View a filtered list of entities
- View related entities
- View connected entities
- View alerts
- View recommendations (VMAN)
- View maps for groups

ℹ️ You can also customize auto-generated maps, or create custom maps. To learn more, see [working with entities](#).

### View all entities on the map

Click in an empty space on the map to display the Map Summary in the Inspector Panel.

The Map Summary lists all entities on the current map.

### View a filtered list of entities

On the Map Management page, create a new map or select a map.

Under the Entity Type drop-down, click the filter button. This opens a panel containing available options for filtering entities on, such as Machine Type, Polling Method, and Status.
If the desired filter is not included in the default drop-down, click the pencil in the upper-right corner of the panel.

In the Add/Remove Property dialogue box, select the relevant properties you want to use when creating a filter. Click Add Selected Properties to include the new property in the list of entity filters under Entity Library.

Use the Control Key to individually select entities from the filtered list, or use the Shift Key to grab a selection at one time, and place them on your canvas.

**View related entities**

On an Orion Map, select an entity. The entity name is displayed in the Inspector Panel.
Click the icon for related entities. The Inspector Panel lists all related entities. Entities with check boxes selected are displayed on the map.

You can further filter the related entities to display:

- Descendents (1)
- Ancestors (2)
- Dependencies (3)
- Or any combination of the above items

**What are descendents and ancestors?**
For example, if you select a server hosting a virtual machine, the virtual machine will be listed as a descendant of the server. If you click ancestors for the host, you will see entities such as a cluster, datacenter, or vCenter server.

Use the Sort, Show, and Search boxes to fine-tune the list of related entities.

**View connected entities**

On an Orion Map, select an entity. The entity name is displayed in the Inspector Panel.
Click the icon for connected entities. The Inspector Panel lists entities connected to the selected entity by a protocol-based relationship or actual data flow, such as topology (NPM) or Application Dependency Connections (SAM). Entities with check boxes selected are displayed on the map.

Use the Sort, Show, and Search boxes to fine-tune the list of related entities.
View alerts for the entity

In Orion Maps, you can see all active alerts for the selected entity.

1. On an Orion Map, select an entity. The entity name is displayed in the Inspector Panel.
2. Click the Alerts tab (bell icon).
   - To filter alerts, click the alert group(s) to be listed: Critical, Warning, or Informational. By default, the Inspector Panel displays all active alerts. You can sort and search the alerts.
   - To see more details about an alert, click the alert name. The Active Alert Details page opens in a new browser window.

View recommendations for the entity (VMAN)

If you have VMAN installed, the Inspector Panel displays VMAN recommendations.

On an Orion Map, select an entity. The entity name is displayed in the Inspector Panel.
Click the Recommendations tab to review recommendations for the entity. Click a recommendation to open the recommendation in a pop-up window, see more details, and apply it if appropriate.

View groups on Orion Maps

You can view an Orion Map for a group, just as you can for an interface, volume, node, or any other object monitored in Orion Platform products. However, Orion Maps for groups are slightly different because they do not show all related entities.

The Map subview for a group only shows connections between the members in the group.

If you create groups using dynamic queries, the Map subview automatically updates as new members are monitored.

**Group status**

Starting with Orion Platform 2019.2, you can specify what metrics should influence the node status.
However, when you add groups to an Orion Map, the group status does not affect the overall status of the map. Even if members in the group are down, the map is displayed as Up.

![Orion Map Example](image)

**Work with entities in auto-generated Orion Maps in the Map subview**

- Display relations, connections, alerts and/or recommendations (if you have VMAN installed) for an entity on the Map
- Go to an entity from the Inspector Panel
- Center the map around an entity
- Add single entities from the Inspector Panel
- Automatically add all related entities
- View performance metrics for a mapped entity in Performance Analysis dashboards
- Remove entities
- Revert an action
- Create a group from mapped objects

**Display details of a mapped entity in the Inspector Panel**

1. Click an entity on the map.
2. When the entity is selected, its details are displayed in the Inspector Panel, and the map changes focus.

You can list related entities, connected entities, alerts, and recommendations (if you have VMAN installed).
Select an entity on the map from the Inspector Panel

For each entity on the map there is a selected box in the Inspector Panel. To the right of the entity there is a right arrow icon.

The Inspector Panel lists entities on the map, as well as related or connected entities that are not on the map:

- Entities on the map have a selected box on the left and a right arrow icon on the right.
- Related or connected entities have an empty box on the left.

Click the arrow icon in the Inspector Panel to select an entity on the map. The Inspector Panel displays details for it - related and connected entities, alerts, and/or VMAN recommendations.
Center the map around an entity

1. Press the Alt key. The chevron icons in the Inspector Panel change into the center icon.
2. Click the center icon for the entity to center the map around.

The map centers around the entity.

Add entities to the map from the Inspector Panel

You can only add entities from the Inspector Panel on auto-generated maps in the Map subview. Custom Orion Maps do not support this feature, and the check boxes are not available.

For auto-generated Orion Maps, review the check boxes in front of entities in the Inspector Panel. A grey box indicates the seed entity that you cannot remove from the map. The name of the seed entity is also in the map title.

- If a box is selected (blue with a checkmark), the entity is displayed on the map.
- If a box is not selected, click it, and click Apply to add the entity to the map.

Automatically add related data on the map

To automatically add relational data, use the "Map It" feature.

Map It is only available for auto-generated Orion Maps. It is not available on custom Orion Maps.

1. On the Orion Map, hover over an entity, hold the Alt key down, and click the Map It icon.
2. Related entities are added on the map.
Open an entity in PerfStack

1. To view performance metrics for a mapped entity, open the entity in PerfStack.
2. On the Orion Map, hover over an entity, and hold the Alt key down, and click the PerfStack icon.
3. The selected entity opens as a new Analysis project showing default metrics.

Remove an entity from the map

**To remove an entity from the Inspector Panel:**
Clear the blue box for the entity in the Inspector Panel, and click Apply.

**To remove an entity from the map:**
1. Select an entity on the map, and click Delete on your keyboard.
2. The entity, and all connected entities, are removed from the Orion Map.

Revert an action

This feature is only available on auto-generated Orion Maps.

- When you apply your changes, the Revert button in the top right corner of the map becomes active.
- Click Revert to undo the last action.
Save entities on a map as a group

This feature is only available on auto-generated Orion Maps.

You can create groups from entities on a map.

1. Make sure the map displays the entities to include in the group.
2. Click Save > Save as New Group.
3. Provide a name for the group. The group details view opens.

To add entities to the group, open the map for the group. On the Maps subview, adjust the map, and then click Save > Update This Group.

Adjust auto-generated Orion Maps in the Orion Platform

When you initially view an Orion Map, it is focused on the seed entity.

To better focus on an entity, group, or connection, move the map within the canvas. Left-click into the map and hold the left mouse button to drag the map.

To adjust the map, use the controls in the lower right area of the Canvas.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="grid.png" alt="Icon" /></td>
<td>Hover over the Change Layout icon to display available layout options.</td>
</tr>
<tr>
<td><img src="grid.png" alt="Icon" /></td>
<td>Grid: Arrange mapped entities to a grid layout. This layout does not display metric pills.</td>
</tr>
<tr>
<td><img src="hierarchical.png" alt="Icon" /></td>
<td>Hierarchical: Arrange mapped entities according to hierarchy layout.</td>
</tr>
<tr>
<td><img src="force-directed.png" alt="Icon" /></td>
<td>Force-Directed: Arrange mapped entities with the selected entity in the center.</td>
</tr>
<tr>
<td><img src="zoom-in.png" alt="Icon" /></td>
<td>Zoom in. You can also use the scroll wheel of your mouse.</td>
</tr>
<tr>
<td><img src="zoom-out.png" alt="Icon" /></td>
<td>Zoom out. You can also use the scroll wheel of your mouse.</td>
</tr>
<tr>
<td><img src="center.png" alt="Icon" /></td>
<td>Center: Reposition the map to the center of the canvas.</td>
</tr>
<tr>
<td><img src="fullscreen.png" alt="Icon" /></td>
<td>Full Screen: Hide the navigation panel.</td>
</tr>
</tbody>
</table>
Understand connections on Orion Maps in the Orion Platform

Orion Maps show you how entities are connected.

Click a connection on the map to display more details in the Inspector Panel.

Orion Maps display the following connection types, based on the seed entity:

- Orion dependency connections
- Application dependency connections
- Topology connections

View Orion Platform dependencies

A dependency connection shows that a relationship exists between two entities. It could be a user-defined dependency, or a dependency identified through its ancestry.

Orion Platform dependencies are displayed as lines.

Requirements for displaying dependencies on Orion Maps

- Orion Platform dependencies are available on all Orion Maps.
- The "seed entity" must have inherited or user-defined dependencies. If you see only the entity, there are no connections.
Example: Inherited dependency on Orion Maps

For example, if you select a virtual machine (VM), the VM (1) can have a relationship to its host (2), which can have a relationship to its cluster (3).

View Application Dependency connections

Application Dependency connections display applications or systems communicating with each other.

The information available on the map and in the Inspector Panel depends on the Application Connection Settings.

Requirements and recommendations for Application Dependency connections

- SAM 6.6.1 or later
- Connection Quality Polling enabled (recommended)

Enable Connection Quality Polling to see TCP latency, packet loss, and other details on Orion Maps

If Connection Quality metrics aren't enabled, the relationship on the canvas is represented by a light blue line with no metric pill.

1. Click Settings > All Settings, and then click Application Connection Settings in the Product-specific grouping.
2. Ensure that Connection Quality Polling is enabled.

View Application Dependencies on Orion Maps

1. Go to the Details view for an application.
2. Click the Map icon on the left.
3. Pay attention to red or yellow connections on the map. The colors highlight that latency or packet loss are breaching the warning (yellow) or critical (red) threshold. See Thresholds for more details.

4. Click an Application Dependency connection to display a list of the processes communicating between the two entities in the Inspector Panel.

5. To display the Connection Details page for a connection, double-click the connection on the map or an item in the inspector panel.

Topology connections

Topology connections show the network traffic between entities.

To quickly identify if bandwidth is properly distributed across the environment, review the width of the topology connections. The width represents interface bandwidth, so that you can easily determine differences between a 1 GB link, 10 GB link, or 100 MB link across the map.

Requirements for displaying topology connections

- NPM
- Topology Polling enabled

In Orion Platform products, it is enabled by default.

To verify, go to the Node Details view, and click List Resources in the Management widget. Make sure
that boxes for Topology: Layer 2 and Topology: Layer 3 are selected.

View topology connections

1. Go to the Details view of the entity.
2. Click the Map subview on the left.
3. Review details in the metrics pill. By default, the metric pills highlight outbound traffic and utilization details on either side of the connection.
4. Review the connection colors. Based on thresholds set in NPM, the connections change to yellow when the warning threshold is exceeded, or red for an exceeded critical threshold. See Thresholds for more details.

5. Review the connections between the entities in the Inspector Panel on the right.

6. Click a connection to display more details.

If the texts in the Inspector Panel are too close together or even cut off, consider expanding the Inspector Panel. Grab the handle and drag the Panel to the left.

Example: Topology on the Map

In the example below, the map shows a problem link and indicating a threshold has been met, while the inspector panel displays all data between each connection.
On either side in the panel, you can see the interfaces associated with the device above, along with the most recent polled data for traffic, errors & discards, utilization, and the maximum bandwidth.

Create and edit Orion Maps

with Orion Platform 2019.2, you can use the Map Editor to create and customize Orion Maps:

- Create custom Orion Maps from scratch
- Import automatically generated maps to the Map Editor and adjust the maps
- Select multiple entities in the Map Editor
- Duplicate and customize already available maps
- Find related or connected map entities
- Manually connect entity objects
- Add custom images to the Map Editor

You can add Orion Maps to your views in a widget.

See the Orion Maps 3.0 post on THWACK.

If your user account does not have Node Management rights, you can save maps only as entities without status. You can display such maps in a widget or in the View mode, but you cannot nest maps without status into other maps.
Create an Orion Map from scratch

1. Click My Dashboards > Orion Maps in the Home section.

2. In the Map Management page, click New Map. An empty canvas opens. You are now in **Edit mode**.

3. Select desired entities in the Entity Library and drag them to the canvas. Any relationships to mapped entities, such as topology connections, manual dependencies, or ADM relations, are automatically displayed.

4. Filter the list of entities shown from the Entity Type drop-down. Select the filter button to choose from a number of options, such as, Machine Type, Polling Method, or Status. If your desired option is not shown, click the edit pencil to open a dialogue box and type in any relevant property to filter by.

5. To display more details about the entity, click an entity on the map. The details are displayed in the panel on the right. The panel lists related entities, connected entities, alerts, and recommendations (VMAN) for the selected entity. Selecting an entity also changes the focus of the map.

6. To identify an entity from the list on the map, click the right arrow next to the entity in the list. The entity becomes selected on the map and the panel displays entities relevant for the selection.

7. To place an entity, use the Control Key to select individual entities from the list, or use Shift to grab all entities between two selections. Drag the selections to the canvas to place the nodes in staggered grid formation. By click and dragging across the canvas, you can perform a marquee selection of entities.

8. Adjust the position of entities on the map. You can use the following shortcuts:

<table>
<thead>
<tr>
<th>Shortcut</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>Zoom in.</td>
</tr>
<tr>
<td>-</td>
<td>Zoom out.</td>
</tr>
</tbody>
</table>
### Shortcut | Explanation
--- | ---
Ctrl + Mouse wheel up | Zoom in.
Ctrl + Mouse wheel down | Zoom out.
Space bar + Click + Drag | Pan the map in the viewport.

### Map Editor Only

<table>
<thead>
<tr>
<th>Shortcut</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Del</td>
<td>Remove the selected object(s) from the map. Excludes auto-discovered connections.</td>
</tr>
<tr>
<td>Ctrl + S</td>
<td>Save the map.</td>
</tr>
<tr>
<td>Ctrl + Shift + S</td>
<td>Save the map under a new name.</td>
</tr>
<tr>
<td>Esc</td>
<td>Clears object selection.</td>
</tr>
<tr>
<td>Arrows</td>
<td>Nudge the selected object.</td>
</tr>
<tr>
<td>Shift + arrows</td>
<td>Move the selected object.</td>
</tr>
<tr>
<td>Ctrl + Z</td>
<td>Undo previous map modification</td>
</tr>
<tr>
<td>Ctrl + Y</td>
<td>Redo previously undone map modification</td>
</tr>
</tbody>
</table>

9. To preview the map, click More > View. This opens the map in **View mode**.
   In View mode, you can:
   - Hover over an entity to display the pop-up.
   - Review the list of entities on the map.
   - Click an entity to display the **Inspector Panel**.

   You cannot add entities from the Inspector Panel. To add entities, you need to switch to the Edit mode.

10. To save the map, click More > Edit to return to the Edit mode.
11. Click Save and provide a unique name. The Orion Map is saved. If your user account does not have Node Management rights, the saved map does not have a status and does not appear in the list of entities.

### Select multiple entities in Map Editor

The multi-select tool allows you to select, click, and position multiple entities at one time. Use the Control Key to individually pick entities from the entity list, or the Shift Key to grab a group of entities, and drag your selections onto the canvas as a unit.
The click and drag process performs a marquee selection of entities. Once your placement is complete, use the Control key again to select and adjust individual entities when necessary.

Create a new map from an auto-generated Orion Map

1. Go to the details view of the entity you want to base your map on, and click the Map subview.
2. Add related or connected entities on the map.
3. Position the elements as needed.
4. Click Open Map in Editor in the top right corner. The map opens in the Map Editor.
5. Complete the map definition, and save the map.

Duplicate and edit an existing Orion Map

If you want to create a map similar to one you have already created, save the map using another name, and adjust your copy of the map.

If you have Administrator privileges, you can also display and edit maps created by other users.

To duplicate and edit an Orion Map:

1. Click My Dashboards > Home > Orion Maps.
2. To edit a map created by other users, toggle the All users switch on.
3. Select the map to adjust, and click Edit.
4. Click More > Save as.
5. Provide a name for the copied map and edit as required.

Find related and connected map entities

From Orion Maps, you can view relationship information across a stack of connected entities. Connected entities are any nodes or interfaces that are connected based on NPM's Topology data or SAM's Application Dependency Connections. Related entities are all other nodes, such as volumes or applications, associated with a server.

1. Locate and add an entity to the map. To the right of the entity is a menu.
2. Select Show Related Entities. This opens a panel of all related entities.
3. From the panel, you can search and filter based on entity type. Additionally, you can continue to click new options, and each opens a new panel of connected or related entities.

Manually connect entity objects

Starting with Orion Maps 2019.4, you can connect objects and define custom connections within the map editor.
1. Click and drag to select two unconnected entities.
2. Click the entity connection button. This opens the Configure custom topology connection window.
3. For the first entity, click Configure and select the desired interface to connect to. The panel displays all objects related to that specific entity. You can filter or search for a specific entity.
4. Click Apply to associate the two objects.
5. Repeat steps 3 and 4 to connect the second entity to an interface.
6. Click Create.

Add custom images to Map Editor

Starting with Orion Maps 2019.4, you can enhance your maps by adding images outside of the monitored entities in Orion. This allows you to highlight the location of important elements, help users easily interpret a map, or enhance the overall look of your maps, such as adding your company's logo to a map.

From the Map Editor toolbar, select the Insert Images options, and browse to your desired image file.

Images are layered behind entities and connections, and in the order they are added to the map. Images can be selected, moved, and deleted.

Add Orion Maps to views as a widget

Before you begin, be aware of the following:

- You need Edit View privileges.
- Create the map. If it is a map created by another user, make sure you can view it in the Maps list. Click My widgets > Home > Orion Maps, and toggle All Users on.
- Orion Maps comply with account limitations. If users are authorized to see only specific objects, maps will only show them what they are allowed to see.

Add Orion Maps to views

1. Go to the view to add the map.
2. Click the pencil icon in the top left corner of the view, and then click Add Widgets in the top right corner of the Orion Web Console.
3. In the Group by section, select Network Maps, and drag the Orion Map widget to the view, and click Done Editing.

4. Click Choose Map.

5. Provide the width.

6. Select the map. If you're an administrator and want to add a map created by someone else, toggle All users on.
7. Click Save.

The map auto-fits in the widget. Hover over an entity to display the pop-up.

Orion Maps now reflect the enhanced status calculation, giving you information about what’s wrong with individual entities.

### Use Orion Maps in alerts and reports

There are no out-of-the-box alerts for Orion Maps. You can create custom alerts based on the Orion Maps entity, report on objects available on a map, and schedule a map to be emailed to you on a schedule.

### Create a custom alert based on the Orion Maps entity

1. Click Alerts & Activity > Manage Alerts.
2. Click Add new alert.
3. Enter the alert properties, which includes who can view the alert, severity, and how frequently the alert conditions are evaluated.
4. Define the conditions that must exist to trigger the alert:
   a. On the Trigger Condition screen, select Orion Map, and Map Name.
   b. Select is equal to, and provide the Map Name. This is the name you used to save the map.
      You can also use the Name property. This is the map ID.
   c. Complete the trigger definition. For example, you might want to be alerted when the status of
      the map is not up.

5. Define what event occurs to reset the alert.
6. Schedule when you want the alert to monitor your environment.
7. Define what happens when an alert is triggered.
On the Trigger Action screen, specify how you want to be alerted. For example, you can define that an email with more details is sent to you. In the Message section, click Insert Variable, and review the variables you can use in the message.

8. Define what happens when the alert is reset.

9. Review your alert, including the number of alerts that will be triggered based on the conditions you defined.

Create a custom report on mapped entities

You can create a report that displays the list of entities on the map, together with their status.

You cannot add Orion Maps to reports, but can configure the Orion Platform to send the Orion Map to you as a PDF.

To create a custom report for an Orion Map:

1. Click Reports > All Reports.
2. Click Manage Reports, and then click Create New Report.
3. **Specify what to report on:**
   a. Select Custom Table.
   b. Select Specific Objects (static selection).
   c. Search for the Orion Map to report on.

---

**Add Content**

1. **Resource: Custom Table (Reporting)**

2. **Select objects you are going to report on...**

   **Selection method:**
   
   - Specific Objects (static selection)
   
   Monitored objects added after the creation of this report will not be included.

   **Available Orion Maps:**

<table>
<thead>
<tr>
<th>SHOW</th>
<th>GROUP BY</th>
<th>SEARCH FOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orion Maps</td>
<td>[No Grouping]</td>
<td></td>
</tr>
</tbody>
</table>

   ![Selection Options]

   - Active Directory Map
   - Demo Map
   - Hyper V Map
   - Lab Map 001 Smokey
   - Map of Groups
   - Map of Maps including a map of nested groups
   - Map User DC Map
   - Map vCenter Map
   - Map User Switch Map
   - NetPath Services
   - Network Map
   - Read’s ILM
   - Read’s Topology
   - Smoke Test 01
   - Smoke Test 02

   **Selection Name:** Active Directory Map
4. **Select columns to display on the report** for the map, such as group member display name. You can also add group availability and group member availability from Group Status History.

   ![Add Column](image)

5. Complete the Create report wizard.

### E-mail a PDF with the map

Configure the Schedule Manager to automatically email you a copy of the Orion Map in the PDF format.

1. Open the Orion Map to send with your report, and click Share. This copies the map link to the clipboard.
2. Click Reports > All Reports.
3. Click Manage Reports, and then click the Schedule Manager tab.
4. Click Create New Schedule.
5. Click Assign Webpage, paste the link to the map to the field, and click Next.
6. (Optional) To also send the report on map members and their status, click Assign Report, and specify the report.
7. **Complete the schedule definition.**
   The map and the report if specified will be sent to the email address as defined.
Manage and view reports in the Orion Platform

SolarWinds provides predefined reports for each Orion Platform product. Use the web-based interface to customize these predefined reports and create your own reports.

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

To maintain legacy reports created with the Orion Report Writer, you must use the deprecated Orion Report Writer.

Predefined reports in the Orion Platform

Your SolarWinds installation comes with many predefined reports that can be used as soon as there is data to be reported on. View a list of predefined reports by clicking Reports > All Reports in the menu bar.

These predefined reports are sufficient for most needs, but can be further customized. You can also create new reports.

Modify an existing web-based report for the Orion Platform

Modifying an existing web-based report is often the simplest way to generate a new report. You can add pre-existing resources or create a custom table or chart. You can also edit information about each resource.

1. Click Reports > All Reports in the menu bar, and click Manage Reports.
2. Select Report Origin in the Group by drop-down menu in the left pane, and select Web-based from the list.
3. Select the report to use as the basis for your new report, and click Duplicate & Edit.
4. Click Add Content.
5. Select the resource to add to the report, and click Select and Continue.

Some resources require you to choose a specific object to report on. For example, if you want to track how many people use a specific application, you must choose the application when adding the resource.

6. Click the Edit button on the resources to make changes such as filtering the objects, group columns, or setting a sample interval. Available options depend on the type of resource you add.
7. Click Next to display the Preview view, and click Next.
8. Add report properties, such as categories or custom properties. Use the report limitation category to restrict the report to specific user accounts. Click Next.
9. Schedule the report by clicking Schedule this report to run regularly, and creating a new schedule or
adding the report to an existing schedule. Click Next.

10. Review the Summary and click Submit to save the report.

Create a web-based report in the Orion Platform

Web-based reports are created in the Orion Web Console, and can be restricted to specific users through report limitations. Users may be assigned specific report limitation categories and can only view reports that are in the same report limitation category.

SolarWinds recommends that you duplicate and edit an existing web-based report instead of creating a new one.

1. Click Reports > All Reports > Manage Reports > Create New Report.
2. On the Layout Builder panel, click Add Content. You may be prompted to add content as soon as you click Create New Report.
3. Select the first resource to add to the report and click Select and Continue.

Some resources require you to choose a specific object to report on. For example, if you want to track how many people use a specific application, you must choose the application when adding the resource.

The Layout Builder view is displayed with the selected resource added.
4. In the Content area, add resources and sections to the report.
   a. Click Add content to add resources to your report.
   b. Click Add section to add more rows of content to this report.

5. To filter a resource to include a specific set of data, click Edit Resource. Not all resources can be filtered.

6. Filter the resource and click Submit.
Each resource has different filter options.

7. After adding and filtering the resource, enter a report name, and click Next.

8. On the Preview panel, click Next.

9. Add report properties, such as categories, custom properties, or limitations, and click Next.

10. To schedule the report, click Schedule this report to run regularly, create a new schedule or assign a schedule, and click Next.

   You can schedule a report to be generated, emailed, saved, or printed.

11. Review the Summary and click Submit to save the report.
Customize a web-based report layout in the Orion Platform

You can customize how the report looks, such as the width, header, or number of columns. By default a report is 960 pixels wide with a header and footer, and a single column for content.

1. Select a report to edit from the Report Manager.
2. In the Layout Builder page, change the width of your new report by doing one of the following:
   - Click Fit to window width so the content of the report expands to the width of the browser window.
   - Enter a new value, in pixels (px), in the Report width field.
3. Click Browse for logo to change the default logo. The Logo check box must be selected in the Header area.Changing the logo does not affect other reports.
   - The maximum image size is 600 pixels wide and 240 pixels high.
4. In the Content area, change the number of columns or rows. You can select a predefined page layout or manually add columns and rows.
   - Enter a number in the Layout columns field to change the number of columns.
   - Click Add section to add more rows.
5. Select the Footer check box to include a footer in your report. Select each option you want included.

Add content to a web-based report in the Orion Platform

You can include any Orion Web Console widget, including charts and graphs, in a report.

The following procedure assumes you are already creating or editing a report in the Orion Web Console.

- Resources can be dragged between columns and sections.

1. On the Layout Builder page, click Add Content in the column to which you want to add a new widget, or resource.
2. Use the Group by field to filter the available resources or search for a specific widget.
   - The Classic category grouping provides the most comprehensive list of available widgets.
3. Select the widget from the list in the main pane.
   - If you are an advanced user and want to add a Custom Chart or Table, see Add a custom chart or table to a web-based report in the Orion Platform.
4. Click Select and Continue.
5. If the widget requires you to select specific objects:
   a. Select the required objects from the left pane.
   b. Click Add to Layout.

6. You can edit the widget if you want to change the title or subtitle.

7. If you want to add another row to your report, click Add section. You can now add content to this row as described above.

Add a custom chart or table to a web-based report in the Orion Platform

When you are familiar with the SolarWinds Orion database, or comfortable with creating SQL or SWQL queries, you can create custom charts or tables and use them in reports.

To ensure that the charts and tables show meaningful results, you need to know what data you are using, from which instances it originates, and what you do with the data.

You can reuse customized charts or tables by clicking Use previously specified objects when adding the chart or table and then selecting the object.

1. Click Add Content in the column to which you want to add a custom chart.
2. Group by Reports to find the Custom Chart or Custom Table resources.
3. Select Custom Chart or Custom Table, and click Select and Continue.
4. Use one of the following methods to configure the objects displayed in the chart or table:
   - Specific Objects (static selection) - use when you know which objects you want to include in your chart or table.
     a. Filter or search for the objects you want to include.
     b. Select the objects' check boxes.

   - Dynamic Query Builder - use to select objects based on object properties.
     a. Select Basic Selector to create and/or queries or select Advanced Selector to create complex queries.
     b. Choose the object type you want to include.
     c. Enter your conditions.

   This is the preferred selection method for groups of objects of a specified type that may change over time. "All Cisco nodes in Austin" is an example of a group best defined using the Dynamic Query Builder.
Advanced DataBase Query (SQL, SWQL) - only use if you are comfortable querying your SolarWinds database directly using SQL or SWQL.

a. Select SQL or SWQL, and enter your query.
b. Click Preview Results to test your query.

5. Enter a name for this selection in the Selection Name field, and click Add to Layout.

You must now edit the chart or table to choose the data series or columns you want to use and modify display and filtering settings.

Add a data series and customize a chart

Once you have specified the objects for your custom chart, you need to select the data series. You can also change the sample interval and filter the results.

1. If you have just added a custom chart, the Edit Resource page opens. Click Edit Chart on the resource in the Layout Builder page to open this page.

2. Click Add Data Series in Left Y-axis.

3. Filter or search for the data series, and select the one you want to use.

4. Click Add Data Series. The data series is added to the Left Y-axis.

5. For additional settings for each data series, click More. Here you can:
   - Edit the Display name for this data series.
   - Select a custom Color for this data series.
   - Show the 95th percentile line for this data series.
   - Show Trend for this data series.

6. Enter a Custom label for the Left axis.

7. Select the Units displayed, Chart type, and select the Show the sum of all data series, if required.

8. Select the Sample Interval. This can be as frequent as once a minute to once a week. Data within each sample interval are summarized so that a single point or bar is plotted for each of these periods.

9. Choose how you want to filter the data.
   a. Select how you want to sort this selection of records from the Sort records by drop-down menu. The choices depend on the data series selected.
   b. Select either Ascending or Descending from the Sort order drop-down.
   c. Select the Data aggregation method required to summarize your data by time period.
   d. Click Advanced if you want to sort records using a secondary field.
10. Set up additional data series using the right axis to superimpose two charts using different labels, units, and chart type.

You cannot use a separate time period or filter results settings for the right axis series.

11. Click Submit to return to the Add Report page.

Add a data series and customize a table

After you have specified the objects to be reported on for a custom table, select the data series. You can also sort and filter the results.

1. If you have just added a custom table, the Edit Resource page opens. You can open this page by clicking Edit Table on the resource in the Layout Builder page.

2. Click Add Column.

3. Filter or search for the column, and select the column you want to use.

The columns and options available depend on the objects selected.

4. Click Add Column.

5. For additional settings for a column, click Advanced. Here you can:

   - Edit the Display name for this column.
   - Select Hide this column in the resulting table, if you want to use this column when querying the database but do not want to show it. For example, you may want to use this column’s data in the time-based settings but not show the data in the table.
   - Select Allow HTML tags, if you want to use any HTML tags retrieved from the database for this column.
   - Select the Display settings to be used for this column. This applies the selected formatting to the data in this column.
   - Select the Data aggregation method to use for this column, to summarize your data by time period.
   - Select the Alignment for this data. This can be left, right, or center.

6. Click the plus sign in the table layout section to add more columns.

7. Filter the number of records shown in the table by either a specific number or a percentage.

8. Restrict data in your table to a specific time period by selecting Yes from the Time-based settings drop-down menu.

You can only do this if your table contains a column with historical data.

   a. Select the column used to specify the time period from the Date/Time column in this table drop-down menu.
   b. Select the Sample Interval. This is used to summarize your data by time period.

9. Use the Group results by option to organize the table by the values in the columns you select.

10. Click Submit to return to the Add Report page.
Build conditions

Use the Dynamic Query Builder selection when objects may change over time. For example, as your network ages, you will replace or upgrade various pieces of equipment. You can select each piece of equipment individually, or you can create a dynamic query that adds objects to the custom chart or table based on the properties you select.

The Advanced Selector provides access to all network object characteristics, and the Basic Selector provides access to a smaller subset of the most frequently used network object characteristics.

1. Select the type of selector query you want to use (Basic or Advanced).
2. Select the type of objects to report on from the I want to report on drop-down menu.
3. For the Basic Selector:
   a. Click Add Condition.
   b. Select All child conditions must be satisfied (AND) or At least one child condition must be satisfied (OR).
   c. Select a property of the monitored object, a conditional relation, and provide a value.
   d. Click Add Simple Condition if you want to add another condition.
4. For the Advanced Selector:
   a. Select All child conditions must be satisfied (AND) or At least one child condition must be satisfied (OR).
   b. Select which field you want to evaluate, a conditional relation, and provide a value.
   c. Click the + sign to add child conditions.
      - Add Single Value Comparison (Recommended) - The child condition evaluates a single field, like Status
      - Add Double Value Comparison - The child condition evaluates two conditions, such as Status and OS
      - Add And/Or block - Adds a sub condition block

Restrict who can access reports in the Orion Platform

If you need to restrict users to access only specific reports, use report limitation categories.

- Step 1: Specify reports you want a user to see by assigning a report limitation category to them.
- Step 2: Specify reports a user can see by assigning the report limitation category to the user account.
Before you begin

Before you start using report limitation categories, review the following considerations and prepare a plan for restricting access to reports:

- You can only assign **one report limitation category to each report**. For example, if you define a "finance" category to a report, only users with the "finance" restriction can access the report. Users with a "marketing" category won't see the report.

- Users can only **see reports from one report limitation category**. You must decide what group of reports each user should be able to see: does the user need "finance" or "marketing" reports?

- **You cannot prevent users from accessing reports they created**. When a user creates a report, the user becomes the owner of the report. Report owners can access the report, even if the report is not in the report limitation category assigned to the report owner.

- You can **prevent users from accessing all reports**. To do so, apply the **No Reports** limitation to the user account.

- You can **allow administrator users to see all reports**. To do so, apply the **No Limitation** Report Limitation Category to the user account.

Assign a report limitation category to a report

1. Start **creating** or **editing a report**. To do so, click Reports > All Reports > Manage Reports.
3. Specify the Report Limitation category:
   - To create a new category, click Add new and provide a name for the new category.
   - To use an existing limitation category, select it.

   > Each report can have only one limitation.

4. Complete the Add Report or Edit Report wizard. If you created a new report limitation and saved the report, the limitation is available in the user settings.
Specify the report limitation for a user

After the report limitation is saved, it is available in the user account's Define Settings page.

1. Click Settings > All Settings > User Accounts.
2. Select the user and click Edit.
3. In the Report Limitation Category, select the limitation, and save your changes.

   The user can now access only reports in the selected limitation category and reports created by the user.

Enable an administrator to see reports from all limitation categories

When you create users with administrator rights, they have the Default report limitation category assigned. These administrators thus cannot see reports that belong to a custom, non-default report category, such as reports created by other users with administrator rights.

The built-in Orion Platform admin account has the No Limitation report category applied by default and can thus access all reports.

To see all reports, provide the user with the No Limitation category.

1. Click Settings > All Settings > User Accounts.
2. Select the user and click Edit.
3. In the Report Limitation Category, select the No Limitation category, and save your changes.

   The user can now see all reports, regardless of the limitation category they belong to.

Disable users from accessing all reports

To prevent a user from seeing all reports, specify the No Reports limitation category in the user account.

The No Reports limitation removes all access to reports when applied to a user account.

1. Click Settings > All Settings > User Accounts.
2. Select the user and click Edit.
3. In the Report Limitation Category, select the No reports category, and save your changes.

   The user can now only access the reports s/he created.
Configure a report you created to be available only for your user account

If you want to keep a report you created private, set its Report Limitation Category to No Reports.

Administrators with the No Limitation category can access private reports.

1. When creating or editing the report, go to the Properties tab.
2. In the Report Limitation drop-down, select No Reports.
3. Complete the wizard.

This way, the report will only be available to you.

Generate reports in the Orion Platform on a schedule

Schedules enable you to set up report actions to occur at specific times. These actions let you generate reports and print them, save them to disk, or email them to selected recipients. You can create schedules for single or multiple reports, or assign reports to existing schedules. In addition, you can add URLs to the schedules so that screen captures of specific websites at the time the reports were generated are included.

- Reports can be assigned to schedules when they are being edited, created, or in the Schedule Manager.
- Schedules can be created from the Report Manager, the Schedule Manager, or when you create or edit a report.

Schedule a report to run automatically while creating or editing a report in the Orion Platform

You can directly assign a report to a schedule while editing the report.

1. Navigate to the Schedule Report page.
2. Click Schedule this report to run regularly, and select Create new schedule.
3. Click Add Frequency, and then select when you want to run the report.
   - Click Add Time to select additional dates and times.
     - To delay when the report runs, select Specific Date in the Starting On field, and then select the date and time when you want the schedule to start.
     - To stop the report from running automatically, select Ending On, and then select the date and time when you want the schedule to end.
4. Click Add Frequency.
5. Click Add Action, and select the action (Email, Print, or Save to Disk) to be executed on the configured schedule.

6. Click Configure Action.
   - For email actions, enter the recipients, the message, and the SMTP server.
     Select Include Report's URL to allow recipients to access the report remotely.
   - For print actions, enter the Windows credentials necessary to access your printer, the printer, and print settings.
   - For save actions, enter the location you want to save the report to, the credentials in domain\username format, and the file type you want to save the report as. The location must be accessible from the Orion Web Console server.

7. Click Add Action.

The action is added to the Actions list. You can add multiple actions.

Create and assign report schedules for the Orion Platform in Report Manager

The Report Manager provides a list of all reports that have been set up for your SolarWinds Orion web-based reports. You can create schedules and assign reports to schedules.

Create a report schedule

1. Select a report.
2. Click on Schedule Report > Create New Schedule to display the Properties view.
3. Add additional reports to this schedule by clicking Assign another Report.
4. Click Assign Webpage to include a snapshot of the selected website, and enter the URL in the field displayed. You can assign multiple webpages.
   
   *Start each URL with http:// or https://.*

5. Expand Advanced Settings to specify a user account so that its limitations are applied to this schedule. Click Another User, and enter the User name or Account ID and Password.

6. Click Next to display the Frequency view.
7. Click Add Frequency, and then select when you want to run the report.
   
   *Click Add Time to select additional dates and times.*

   - To delay when the report runs, select Specific Date in the Starting On field, and then select the date and time when you want the schedule to start.
   - To stop the report from running automatically, select Ending On, and then select the date and time when you want the schedule to end.

8. Click Add Frequency, and then click Next to display the Actions view.
9. Click Add Action, and select the action (Email, Print, or Save to Disk) to be executed on the configured schedule.

10. Click Configure Action.
   - For email actions, enter the recipients, the message, and the SMTP server. Select Include Report's URL to allow recipients to access the report remotely.
   - For print actions, enter the Windows credentials necessary to access your printer, the printer, and print settings.
   - For save actions, enter the location you want to save the report to, the credentials in domain\username format, and the file type you want to save the report as. The location must be accessible from the Orion Web Console server.

11. Click Add Action.

12. Click Next to display the Summary view.

13. If the schedule summary is correct, click Create Schedule.

The schedule is displayed in the Schedule Manager.

Assign a report to a schedule or multiple schedules

1. Select one or more reports.
2. Click Schedule Report > Assign Existing Schedule.
3. Select the schedule or schedules in the Assign existing schedule list and clicking Assign Schedule(s) to confirm that you want to assign the report.

Schedule Orion Platform reports from the Schedule Manager

The Schedule Manager provides a list of all report schedules that have been set up for your SolarWinds Orion web-based reports. You can create, edit, run and delete schedules from this page, and assign reports to schedules.

1. Click Reports > All Reports in the menu bar, and then click Manage Reports in the upper right.
2. Click the Schedule Manager tab.
3. Click Create New Schedule to add a new schedule.
4. Select the schedule and click Run Now. The selected schedule runs, which includes the associated reports and report actions.
5. Select the schedule and click Assign to a Report.
Export and import reports in the Orion Platform

Select a supported export format based on how you want to use the exported file. The most common export formats have their own icons on the Orion Web Console report page.

<table>
<thead>
<tr>
<th>Supported Formats</th>
<th>Orion Web Console</th>
<th>Report Writer</th>
</tr>
</thead>
<tbody>
<tr>
<td>XML</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Excel</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HTML and MHTML</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Image (BMP, GIF, JPG, PNG, etc.)</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

💡 To export a report to PDF, click Print, and select your default PDF printer.

To share a custom report between two SolarWinds Sites, you can export it as XML and then import it at another site. You can also export a report as an Excel spreadsheet.

Export a report as XML to a different SolarWinds Site.

Export a report as XML to share it with another SolarWinds Site. You can also export a report to an Excel spreadsheet.

EOC can also import reports from connected SolarWinds Sites.

Export reports as XML

You can save reports from the Orion Web Console in XML format and import them back.

1. Click Reports > All Reports in the menu bar, and click Manage Reports in the upper right corner.
2. Display the web-based reports.
3. Click the report > Export/Import, and then click Export Report.
4. Click Save.

Import XML reports

💡 If you import a report with the same name as an existing report, it will be prefixed with "Copy of".

1. Click Reports > All Reports in the menu bar, and click Manage Reports in the upper-right corner.
2. Display the web-based reports.
3. Click Export/Import, and then click Import Report.
4. Navigate to the required XML file on a network drive, and then click Open.
5. The file will be imported and its name displayed at the top of the list of reports.
Export reports to Excel spreadsheets from the Orion Web Console

The Export to Excel button is only displayed if the report contains only custom table resources. Other resources cannot be converted to the Excel format.

1. Click Reports > All Reports in the menu bar, and click Manage Reports in the upper-right corner.
2. Open the report.
3. Click either Export as Excel.
Create custom monitors in the Orion Platform

With Orion Platform products, you can extend monitoring to non-standard devices, using object identifiers (OIDs) organized in management information bases (MIBs).

Orion Platform products provide the following advanced monitoring options:

- **Device Studio pollers**: Create pollers for certain technologies directly in the Orion Web Console.

> What is a poller?

Statistics monitored on your devices are specified by pollers. Pollers hold information about a monitored property, how to get the current value for the property, and where and how to display the retrieved data.

What do you need custom pollers for?
- To monitor a specific metric which is not monitored out-of-the-box.
- To monitor special equipment.
- To monitor objects although the number of monitored objects exceeds a poller's capacity limitation.

- **Universal Device Pollers**: If there is a specific metric that is not monitored out-of-the-box, or if you have special equipment you need to monitor, create a custom poller based on a specific object identifier (OID) and transform polled results into a resource in the Orion Web Console.

Review the comparison of UnDP and Device Studio pollers to determine which poller to use.

<table>
<thead>
<tr>
<th>UnDP</th>
<th>Device Studio poller</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can poll only one OID.</td>
<td>Can poll multiple OIDs for a given technology.</td>
</tr>
<tr>
<td>Cannot perform logical operations or transformations on the polled data.</td>
<td>Can perform logical operations or transformations on the polled data.</td>
</tr>
<tr>
<td>Polled values are displayed in dedicated resources.</td>
<td>Polled values are displayed in existing resources.</td>
</tr>
</tbody>
</table>
Management Information Base (MIB) in the Orion Platform

Management Information Base (MIB) is a structure that describes all objects a device can report on, such as CPU, fan, or temperature. MIB contains the name, datatype, and the object identifier (OID). MIB is a hierarchical structure, displayed as a navigation tree. Every entry in the MIB tree is a value for a specific component on a specific device.

Each entry in the tree is followed by a number in parenthesis. Each entry in the tree can be specified using the sequence of numbers, such as 1.3.6.1(iso.org.dod.internet). The unique numerical value is the OID.

For more information, see [Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)](https://www.solarwinds.com/support/article/KA00058).

Monitor custom statistics based on OIDs with Universal Device Pollers in the Orion Platform

SolarWinds Universal Device Poller (UnDP) is a customization feature of SolarWinds NPM. With UnDP, you can create custom monitors for almost any statistic provided by SNMP based on its Management Information Base (MIB) and object identifier (OID).

With Universal Device Poller, you can monitor:

- Interface traffic
- CPU temperature
- Addressing errors
- UPS battery status
- Current connections to a website

**Before you start configuring UnDPs**

- Consult your vendor documentation, and find out which OID you want to monitor.
- Create a list of nodes that you want to poll the custom statistic on.
UnDPs do not collect data from Orion Failover Engine or Hot Standby Engines. If a SolarWinds NPM server fails, data collection for any Universal Device Pollers stops on the server.

UnDPs are tied to the polling engine on which they are hosted. If you move a monitored node from one polling engine to another, you must also move the UnDP poller.

Define a custom statistic to monitor in the Orion Platform

Statistics monitored on your devices are specified by pollers. Pollers hold information about a monitored property, how to get the current value for the property, and where and how to display the retrieved data.

Defining a custom statistic for monitoring means creating a UnDP poller.

Before you begin, consult your vendor documentation, and find out which OID you want to monitor.

1. Start the Universal Device Poller application, for example by clicking Start > SolarWinds Orion > Universal Device Poller.
2. If prompted, download and install the MIB database.
3. Click New Universal Device Poller.
4. Specify the OID:
   a. Click Browse MIB Tree, and click Search MIBs in the upper-right corner.
   b. Select a Search By option, enter a string, and click Search.
   c. Select the OID, and click Select.

- If you know the OID, fill it in.
- If you know approximately where in the MIB tree you can find the OID, click Browse MIB Tree, navigate in the MIB tree to the OID, and click Select.
5. Test the selected OID against a device. Select a node, and click Test. See [Troubleshooting failed tests](#) if the test fails.

![Test Success]

6. On the Define Your UnDP screen, edit the suggested Name and Description. The poller name is populated automatically. The name is required and cannot contain spaces.

![Define Your UnDP]

7. To customize the value type, SNMP Get type, polling type or interval, click Advanced Options, and change the defaults:

   a. Select the expected format of values in MIB Value Type.
      
      - For Rate or Counter, provide a Unit and Time Frame.
      - For Raw Value, select a display Format for the polled raw values.
      - For Raw Value > Enumerated, click Map Values to provide strings corresponding to the values returned by the poller.

   b. Select SNMP Get Type, and decide whether the poller should poll nodes or interfaces.

   c. Specify the Polling Interval in minutes. Use values between 1 and 600.

   ![Warning]

   If you want to use the poller in a transformation, make sure that all pollers in the transformation have the same Polling Interval.

8. Keep default settings for Status (Enabled) and Keep Historical Data (Yes). With these options enabled, you can see the trend of polled values in Orion Web Console views.
9. Specify the Group to which you want to add the poller, and click Next.

   To create a new group, type a name for the group into the Group box.

10. Select devices to poll the statistic, click Test, and then click Next.

   Custom OIDs often work only for identical nodes.

11. If the selected OID is a table, specify labels for the rows in the table.

12. Select the Orion Web Console views that can display the poller as a chart, gauge, or table, and click Finish.

The new poller is added to All Defined Pollers and will be polled on the selected nodes or interfaces. You can now add Universal Device Poller resources showing the polled values to Orion Web Console views.

   - To view the poller status on maps, create a network map, add the poller into the map, and add the map on a view. See View UnDP status on Network Atlas maps in the Orion Platform.
   - To check that your UnDP pollers are properly configured, start Orion Diagnostics in your SolarWinds Orion > Documentation and Support program folder, right-click a UnDP, and select Run Tests.

Troubleshooting failed tests

If the test fails on a node or interface, make sure that the following settings are correct:

   - Verify that the test node is being polled using the correct community string. See Edit node properties.
   - Does the device support the polled MIB or OID? See the vendor documentation to confirm the MIBs supported by your device.
   - Can your SolarWinds NPM server access the device? Make sure that the device is responding to both ICMP and SNMP requests.
Select Orion Platform nodes or interfaces to poll a custom statistic

When you have created a UnDP poller, specify the devices (nodes or interfaces) to monitor the statistic. Before you begin, make sure the UnDP poller is created and enabled. See Define a custom statistic to monitor in the Orion Platform.

1. Start the Universal Device Poller application, for example by clicking Start > SolarWinds Orion > Universal Device Poller.
2. Click Assign Pollers.
3. Navigate the poller tree, select the pollers you want to assign, and click Next.
   
   By default, there are two poller groups:
   - Example - all predefined out-of-the-box UnDP pollers.
   - Default Group - all user-defined UnDPs if they are not assigned to any other group.

   Selecting a poller group selects all pollers in the group. If you do not want to assign all pollers, clear the pollers that you do not want to assign.

4. Expand the node tree down to the interface level, and select the elements to apply the pollers.
   
   Interfaces are not displayed unless you are assigning an interface poller.
   Selecting a node automatically assigns a selected interface poller to all interfaces on the node. Clear boxes for interfaces that should not be assigned to the poller.

5. Click Test to see current results of the selected pollers on the selected nodes or interfaces. If the test fails, see Troubleshooting failed tests.
6. After you have completed your poller assignments, click Finish.

Transform poller results in the Orion Platform

Values polled by a custom poller are often better understood after a calculation transforms the value to a different format.

For example, if a poller returns temperature values in Celsius, you might want to see the values in Fahrenheit.

Pollers that you use in a transformation must be assigned to the nodes to poll for values that will be transformed.

1. Start the Universal Device Poller application, for example by clicking Start > SolarWinds Orion > Universal Device Poller.
2. Click Transform Results, and click Next to acknowledge examples of transformations.
3. Type the name and description for the transformation, and click Next. Names must be unique. Names are required. Any spaces in the name are removed.
Descriptions are optional but might be helpful in identifying the type of information generated by the transformation.

You can also change other default settings:

a. Select Yes in the Keep Historical Data section. You will be able to view the transformed poller data in charts and gauges in the Orion Web Console.

b. Select Enabled as the Status if you want your transformation to begin calculating results immediately.

   If you select Disabled, the transformation will not transform polled data.

c. In the Group field, select a group where you want to add the transformation. To add a group, provide the new group name.

d. Optional: provide a polling interval.

   Make sure all pollers in the transformation use the same polling interval.
4. Provide the formula for calculating the transformation.
   a. Click Add Function, and select a function.

   ![Diagram of Add Function and Add Poller options]

   b. Click within the bracket, click Add Poller, and select the poller you want to transform.

   ![Formula: CtoF($nxOperatingTemp)]

   - Separate pollers with commas. The following example averages the results of three pollers:
     \[
     \text{avg}({\text{poller1}}, {\text{poller2}}, {\text{poller3}})
     \]
   - Use standard mathematical operations:
     \[
     {\text{poller1}} + {\text{poller2}}
     \]
   - Use the mathematical constants e and \( \pi \), as \( E() \) and \( \text{PI}() \), respectively.
   - Nest formulas. The following example returns the average of two poller comparisons:
     \[
     \text{avg}(\text{min}({\text{poller1}}, {\text{poller2}}), \text{max}({\text{poller3}}, {\text{poller4}}))
     \]

5. Test the transformation on a device, and click Next.

**Troubleshooting failed transformation tests**

If the test fails, verify the following items:

- Is your formula correct? Ensure that all braces are balanced, that there are no unnecessary spaces, and that all pollers return the same type of values.
- Are you using the correct community string for the node that is being polled for the test?
Does the device support the polled MIB or OID? See the documentation supplied by the device vendor to confirm supported MIBs for your device.

Can you access the device from the SolarWinds Network Performance Monitor server? Confirm that the device is responding to both ICMP and SNMP requests.

6. Select nodes for the transformation, and click Test.

- Interfaces are not displayed unless your poller transformation operates on an interface poller.

7. If the transformation output is a table, select labels for the rows in the table, and click Next.

8. Select Orion Web Console views where you want to include the transformed values as a chart or table, and click Finish.

- Click Preview to see how your poller resource will display in the selected Orion Web Console view.

The new transformation is added to All Defined Pollers and applied on the selected nodes or interfaces. You can add a Universal Device Poller resource to display transformed values in the Orion Web Console views.

- If the transformation combines data from other pollers, make sure that it is assigned to the same node or interface as the pollers used for the transformation and that it has the same polling interval.

Create pollers by duplicating and adjusting pollers in the Orion Platform

When creating similar pollers, consider copying a poller and modifying it.

1. Start the Universal Device Poller application, for example by clicking Start > SolarWinds Orion > Universal Device Poller.

2. In the All Defined Pollers pane, locate the poller that you want to duplicate.
1. To confirm that you have selected the appropriate poller, view the poller properties in the main Universal Device Poller window.

2. Right-click the poller, and select Duplicate Poller.

3. Change the Name of the poller.

4. Adjust the poller settings. See Define a custom statistic to monitor in the Orion Platform.

**Import UnDP pollers to the Orion Platform**

You can import custom UnDP pollers exported from UnDPs installed with earlier Orion Platform versions.

1. Start the Universal Device Poller application, for example by clicking Start > SolarWinds Orion > Universal Device Poller.
2. Click File > Import Universal Device Pollers.
3. For each poller you want to import, complete the following steps:
   a. Click Open, and locate the poller.
   b. Select the poller, and click Open.
4. Select the pollers to import from the list on the left, and click Import. Selected pollers will move to the pane on the right.
   - To select multiple pollers, hold down SHIFT or CTRL, and click the pollers you want.
   - To remove a poller from the Selected Pollers list, select the poller and click Remove.
   - To collapse all folders and see just the group names, hold down SHIFT, and then click – next to any of the group names.
5. Click OK.
6. To begin polling, enable the poller.
   a. Select the imported poller in the All Defined Pollers pane of the Universal Device Poller window.
   b. Click Edit Properties.
   c. Confirm that the poller Status is Enabled, and click Finish.

   If Disabled, the poller will not collect data until you enable it.

7. Specify nodes or interfaces to be polled by the imported poller. See Select Orion Platform nodes or interfaces to poll a custom statistic.

When the imported poller is enabled and assigned to the devices, the poller begins collecting statistics. To view the statistics, log in to the Orion Web Console, go to a view for the node or interface to which the poller is assigned, and consult the poller resource. See View Universal Device Poller statistics in the Orion Platform.

Export UnDP pollers from the Orion Platform

If you want to use your custom UnDPs in later SolarWinds NPM versions or on different polling engines, you need to export them first.

1. Start the Universal Device Poller application, for example by clicking Start > SolarWinds Orion > Universal Device Poller.
2. Click File > Export Universal Device Pollers.
3. In the Pollers pane on the left, navigate to the pollers that you want to export.

   To select all pollers in a group, select the group.
   To select multiple pollers, hold down SHIFT or CTRL and click the pollers to export.

4. Select the pollers, and click Export. Pollers will move to the Selected Pollers pane.

   To remove a poller from the list of pollers for export, select the poller and click Remove.

5. Click Save.
6. Navigate to the location where you want to export the selected pollers, provide a File name, and click Save.

Selected pollers will now be stored as a .UnDP file in the specified location. You can use the .UnDP file to import the pollers on another polling engine.
Temporarily suspend collecting statistics for pollers in the Orion Platform

When you assign a poller to nodes or interfaces, it starts collecting statistics on the selected elements. If you want to suspend data collection for a poller without deleting it, disable the poller.

1. Start the Universal Device Poller application, for example by clicking Start > SolarWinds Orion > Universal Device Poller.
2. In the All Defined Pollers pane, navigate to the poller you want to disable.
   To confirm that you have selected the appropriate poller, view the poller properties in the main Orion Universal Device Poller window.
3. Select the poller, and click Edit Properties.
4. Set Status to Disabled, and click Finish.

The poller will now still be available in the Universal Device Poller application, but will not collect any statistics.

Define UnDP Warning and Critical thresholds in the Orion Platform

If values polled by UnDPs on a device reach a certain level (critical or warning threshold), the UnDP on the device is highlighted in the Orion Web Console.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Thresholds & Polling grouping, click Custom Poller Thresholds.
4. Select a poller.
5. Select whether the expected polled value is a Text or a Number.

To get notified about exceeding a threshold in an email, configure an alert.

To see pollers with exceeded thresholds in a map, see View UnDP status on Network Atlas maps in the Orion Platform.

The Poller Value Type determines how the polled value will be interpreted. It also influences the set of possible comparison functions.

- For the Number type, available values include is greater than or less than.
- For the Text type, available values include for example contains.
6. Build conditions to define both Warning and Critical Thresholds:
   a. Select whether All Child Conditions Must Be Satisfied (AND) or if only At Least One Child Condition Must Be Satisfied (OR).
   b. Select a comparison relation, and provide a threshold value on which the comparison is based.
   c. Click + to add additional conditions, as required, to define the poller threshold.

7. After configuring all thresholds, click Submit.

If a value reported by the device belongs to the range defined by the Warning Threshold, pollers in maps will be yellow.

If a value reported by the device belongs to the range defined by the Critical Threshold, pollers in maps will be red.

View Universal Device Poller statistics in the Orion Platform

If you want to see a poller results in the Orion Web Console, you need to define which widgets, or resources, should be displayed on which views.

Prerequisites

The poller must be enabled, and assigned to the devices.

Set the poller to collect historical statistics. Without historical data, Orion Web Console widgets will only display the last polled value, and you cannot add charts with the poller results to the Orion Web Console.

Define widgets with UnDP results for Orion Web Console views

1. Start the Universal Device Poller application, for example by clicking Start > SolarWinds Orion > Universal Device Poller.
2. In the All Defined Pollers pane, select the poller whose results you want to add as a Orion Web Console resource.
3. Right-click the poller, and click Web Display.
4. Confirm that Yes is selected, and select the types of poller widgets that you want to display on individual Orion Web Console views.

   ▶ Click Preview to see what the poller widget will look like in the Orion Web Console view.

5. Make sure Do Not Show This Poller If It Is Not Assigned is selected. It ensures that the custom poller widget appears only on views for nodes or interfaces that have the custom poller assigned to them and enabled.

6. Click Finish.

When you log in to the Orion Web Console, the selected widgets with poller data will appear on selected views for nodes or interfaces that have the poller assigned to them and enabled.

See also View UnDP status on Network Atlas maps in the Orion Platform.

View UnDP status on Network Atlas maps in the Orion Platform

In the Orion Web Console network maps, you can see when a Universal Device Poller on a device returns values that exceed the warning and critical thresholds.

1. Create a Universal Device Poller in the UnDP application.
2. Assign the poller to nodes.
3. Define warning or critical thresholds specifying when you want the pollers to be highlighted.
4. Create a network map in the Network Atlas, drag the UnDPs into it, and save the map.

   To add a UnDP on a map, start the Network Atlas, navigate to a node on which the UnDP is enabled (Vendor > Node Name > Custom Node Poller), and drag the poller into the map.

5. Log into the Orion Web Console, go to the map view.
6. Locate the Map resource (or add it if not available), click Edit and select your map.

You can now see UnDPs for your nodes in the Orion Web Console map. When the polled UnDP values exceed the warning threshold, the UnDP icon turns yellow on the map. After reaching the critical threshold, the icon turns red.

Cannot find OIDs? Update the SolarWinds MIB Database for the Orion Platform

SolarWinds maintains a MIB database that serves as a repository for the OIDs used to monitor a wide variety of network devices. The MIB database is updated regularly.

When you are creating a UnDP poller and cannot find an OID in the MIB tree, update the MIB database.

2. On the left under Helpful Links, click Orion MIB Database.
3. If you are using Internet Explorer and it prompts you to add the SolarWinds downloads site http://solarwinds.s3.amazonaws.com, add the site to your trusted sites.

4. Specify a location where the file will download.

5. After the download completes, extract MIBs.zip to a temporary location.

6. Open the folder with the extracted MIBs.zip, and copy MIBs.cfg to the SolarWinds folder on your default install volume.
   The default location depends on the operating system. For example, on Windows Server 2012, MIBs.cfg is located in C:\ProgramData\Solarwinds.

   You may need to restart the Universal Device Poller after installing the MIB database.
Manage unique devices on the network with the Orion Platform

If you have devices on your network that SolarWinds does not recognize for polling, you can either edit an existing poller to suit your device needs, or create a poller specifically tailored to your device.

SolarWinds Orion polls values based on OIDs from the SolarWinds MIB database. There can be OIDs you might want to poll, which are not polled by SolarWinds Orion by default. If these OIDs are in the SolarWinds MIB database, you can create either an UnDP, or use Device Studio to poll for that value, and add support for vendors and technologies that are not natively supported by SolarWinds Orion.

| Orion Platform products poll devices based on OIDs according to the device vendor's MIB. These OIDs must be included in the SolarWinds MIB database. When you create custom pollers, you select OIDs from the SolarWinds MIB database. To poll an OID which is not in the SolarWinds MIB database, define it manually. See Define object identifiers (OIDs) that do not exist in the SolarWinds MIB database. |

With Device Studio pollers you can:

- Poll devices that do not support any of the OIDs polled for by SolarWinds pollers.
- Poll devices that return incorrect data when polled by SolarWinds pollers.
- Override polled values to display custom static values.

Device Studio technologies in the Orion Platform

Device Studio supports a number of technologies. Each technology has a defined set of properties that you can monitor on your devices. The technology you select defines how the polled data are processed, stored, and presented.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU &amp; Memory</td>
<td>CPU &amp; Memory is used for collecting data about the CPU and memory load of single processor systems. It provides data to resources related to CPU and memory, such as Average CPU Load &amp; Memory Utilization, Min/Max/Average of Average CPU Load, or Top CPUs by Percent Load. To use this technology, specify a single OID that reports a value from 0 to 100. For example, if a natively polled OID returns incorrect CPU load values, search for an OID that returns a possible value. In the case of CPU load, the load can vary between 0% and 100%, so you must look for an OID that returns a value between 0 and 100.</td>
</tr>
</tbody>
</table>

To determine the OID, consult your device vendor, or carry out a search for an OID that reports the correct value for your device.
### Technology & Usage

<table>
<thead>
<tr>
<th>Technology</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi CPU &amp; Memory</td>
<td>Multi CPU &amp; Memory provides data to the same resources for multiprocessor systems as the CPU &amp; Memory technology provides for single processor systems. For example, if a natively polled OID returns incorrect CPU load values, search for an OID that returns possible values. In the case of CPU load, the load can vary between 0% and 100% on each CPU core, so you must look for an OID that returns a table of values between 0 and 100, where each row corresponds to a CPU core.</td>
</tr>
<tr>
<td>Node Details</td>
<td>Node Details provides data for the Node Details resource, and can be used for devices that are not supported out of the box. To use this technology, specify custom OIDs to poll for Vendor, Machine Type, Software Version, and other data. You can also define custom text to be used instead of the polled value.</td>
</tr>
</tbody>
</table>

*Pollers using other polling technologies, such as VLAN and VRF, are also displayed in the Manage Pollers view. However, it is not possible to create pollers using these technologies in Device Studio.*

### Data sources used in Device Studio

By creating Device Studio pollers, you can define custom polling definitions in a way that allows you to view the defined set of pollers and the data polled by them as fully integrated entities in the Orion Web Console, including charts, alerts, and reports.

You can define a set of polled data, and then associate these data points with monitored nodes.

The data source you use for polling devices can be:

- A polled value or values reported by a device on an OID.
- A calculated value that results from the transformation of polled values.
- A fixed value in the form of a constant number or text. This value is not polled. For example, you can specify the software version of your device as 15.
Create pollers in Device Studio for the Orion Platform

To poll unique devices or technologies not supported by default, create a custom poller.

- Reduce the number of Unknown nodes by creating a custom poller.

1. Click Settings > All Settings, and in the Node & Group management grouping, click Manage Pollers.
2. Click Create New Poller.

3. Select a polling technology, type the Poller Package Name, select a test node, and click Next.

4. On the Specify Data Source tab, select a metric you want to define, and click Define Data Source.
5. On the Pick Object Identifier screen, type the OID, or search the MIB database.

6. If necessary, click Add Calculated Value to transform the multiple returned values into a single value, or select a different OID.

   Transforming multiple values to a single value is useful if, for example, the device returns CPU usage as a table of four values (with one value for each CPU core), but you want to use a single value for CPU usage. In this case, you can use the Average function to convert the table of values into a single value.

7. In the Create a Calculated Value screen, select a function, select an input from the lists, and click Test. You can also define a constant value, for example, if you are creating a CPU and memory poller, and the device you want to poll only supports CPU values.

   Continuing with the previous example, to create an average value out of the four reported values, select the Average function and specify the input values.

8. After testing whether the value is as expected, click Yes, the Data Source Is Reasonable.

9. To automatically test the poller on newly added nodes, select Automatically poll nodes during network discovery, and click Next. The test determines whether the Device Studio poller can be assigned to the newly added node.
10. On the Summary tab, review the poller package settings, and click Submit.

![Review Your Poller Package Settings](image)

The poller is now available in the list of pollers, and you can assign it to nodes.

**Define object identifiers (OIDs) that do not exist in the SolarWinds MIB database for the Orion Platform**

1. On the Pick Object Identifier screen, select the check box under Manually Define Object Identifier (OID).
2. Type the name and OID.
3. Select the SNMP get type. See [What is the SNMP Get Type?](#) for more information.
4. Click Poll Current Value From Test Node.

**What is the SNMP Get Type?**

The SNMP Get type defines the type of query you have to run to retrieve the appropriate information. You can retrieve scalar values by using either GET or GET NEXT, and you can retrieve values from a particular column in a table value by using GET TABLE.

> For table records, only the first five values are returned.

**What is a formula?**

Values polled by a custom poller are often better understood after a calculation transforms the value to a different format. For example, if a poller returns values in MB, you might want to work with the values presented in GB. The calculations and transformations that are used to manipulate poller results are called formulas.

Two types of values or data sources are available:

- Scalar: one value
- Tabular: column of values

When a new data source is created, the name is generated automatically according to the syntax:

<Property name>Formula<Number>

For example: *UsedMemoryFormula1*
Formulas used for transforming Device Studio poller results in the Orion Platform

<table>
<thead>
<tr>
<th>Formula</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KiloToByte</td>
<td>Multiplies input by 1024</td>
</tr>
<tr>
<td>MegaToByte</td>
<td>Multiplies input by 1024 x 1024</td>
</tr>
<tr>
<td>GigaToByte</td>
<td>Multiplies input by 1024 x 1024 x 1024</td>
</tr>
<tr>
<td>Average</td>
<td>Returns the average of values from the input columns</td>
</tr>
<tr>
<td>Sum</td>
<td>Returns the sum of values from the input columns</td>
</tr>
<tr>
<td>Count</td>
<td>Returns the total number of input columns</td>
</tr>
<tr>
<td>Condition</td>
<td>Creates an if/then statement</td>
</tr>
<tr>
<td>Truncate</td>
<td>Rounds the input decimal number up or down to an integer</td>
</tr>
<tr>
<td>Length</td>
<td>Returns the number of characters in the input string</td>
</tr>
<tr>
<td>Replace</td>
<td>Replaces the content in the string</td>
</tr>
<tr>
<td>IndexOf</td>
<td>Returns the position in the string</td>
</tr>
<tr>
<td>SubString</td>
<td>Defines the section of the string of interest</td>
</tr>
</tbody>
</table>

The formulas are divided into three main groups.

<table>
<thead>
<tr>
<th>Type of formula</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transformations</td>
<td>Transform data between different units. For example, transform megabytes to bytes.</td>
</tr>
<tr>
<td>Aggregations</td>
<td>Transform the values from the input table columns to scalar values. For example, transform the values from the input columns into the average of values.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Transform values according to a logical formula according to the following syntax: if(logical formula), (action to perform if formula is true), (action to perform if formula is false)</td>
</tr>
</tbody>
</table>

Example syntax

**SubString**

The SubString(,) calculation takes the following syntax:

SubString ([formula],index start,length)

For example, if your input is "test", the output will be "es" if you use the following calculation:

SubString ([UsedMemoryFormula],1,2)

As another example, if your input is "test", the output will be "st" if you use the following calculation:

SubString ([UsedMemoryFormula1],2,2)
Replace

The Replace(,) calculation takes the following syntax:
Replace([formula], search string, replacement string)

For example, if your input is "test", the output will be "resr" if you use the following calculation:
Replace([UsedMemoryFormula1], "t", "r")

Use Regex formulas for transforming poller results

When you define a Regex formula, use the following syntax:
Regex([variable], "regular expression")

Examples of correct formulas include:
- Regex([description], "^[a-zA-Z]*[^,]*")
- Regex([description], "V.[^,]*")
- Regex([description], "T.*")
- Regex([description], "C.[^ ]+")

Limitations of Regex formulas

When you define a Regex formula, the input string from the test device is interpreted up until the nearest \r (new line) character.

The following methods of defining Regex formulas are not supported:
- A backslash sequence for special characters such as the following: \\, \\, \\, \\.
- Grouping regular functions such as the following: \w, \W, \s, \S.
- Defining multiple conditions in square brackets such as the following: [^,^-].

Test Device Studio pollers in the Orion Platform

A Device Studio poller may not always be seamlessly supported by the device it is tested on. For example, errors occur if the OID the Device Studio poller polls for is not supported by the device, or if the returned value is not of the expected data type defined by the Device Studio poller.

To get the Device Studio poller working in your environment, try the following:
- Test the Device Studio poller on a different node.
- If the device you use for testing is not fully compatible with the Device Studio poller, upgrading the firmware of your test device might help.
- Modify the Device Studio poller to suit the devices you have. For example, you can modify the OID that is used to poll the device.

- Modifying Device Studio pollers this way requires familiarity with the MIB database structure.
- Some of the pollers provided by SolarWinds cannot be modified with Device Studio. You can only modify the poller definition of these pollers in a text editor.
Monitor devices with the Orion Platform using THWACK community pollers

Apart from creating your own Device Studio pollers, you can also import pollers provided by contributors of the THWACK community.

The THWACK community pollers are available in the Orion Web Console under Manage Pollers > THWACK Community Pollers. The list is updated automatically every 30 minutes, and it contains the device pollers that have been made available on THWACK, under Network Performance Monitor > NPM Content Exchange > Device Pollers > Documents.

You can group the available pollers according to tags, author, or technology. Click the name of a device poller to view the description of the poller.

To verify whether a poller suits your specific device, test the poller before importing it.

Test THWACK Device pollers

1. Select the THWACK community poller from the list, and click Test Device Poller.
2. Type your THWACK credentials, and click Submit.
3. Select an SNMP node for testing, and click Test Poller.

After the test is finished, you can directly assign the device poller to the test node.

Import Device pollers from THWACK

1. Select the THWACK community poller from the list, and click Import Device Poller.
2. Type your THWACK user credentials, and click Submit.
3. After the import is finished, the poller will be available in the Local Poller Library, and you can assign it to a device. For more information, see Assign Device Studio pollers to monitored devices in the Orion Platform.

If the poller was already imported earlier, you can either overwrite the existing poller, or create a new one.

Import THWACK community pollers to an environment without Internet connection

The THWACK community pollers are only updated automatically if you have a working Internet connection. To import THWACK community pollers to an environment that does not have an Internet connection, download the pollers from a computer which can access the Internet, save them to a portable drive or a USB drive, and import them manually.

Export Device Studio pollers to the THWACK community

1. On the Manage Pollers screen, click the Local Poller Library tab, and select a poller.

You can export Device Studio pollers that you created, but you cannot export pollers that are provided by SolarWinds.
2. Click Export, and select Export to Thwack.
3. Type your THWACK user credentials, and click Submit.

If you already logged in to THWACK from the Orion Web Console during the same session, you do not have to enter your credentials again, and the Device Studio poller will be exported immediately.

The Device Studio poller will be available on THWACK, in the Network Performance Monitor > NPM Content Exchange > Device Pollers > Documents section.

Why can’t I connect to THWACK from my Orion Platform?

Your Orion server must be able to open internet connections to connect to THWACK.

If the connection is blocked by a firewall or a proxy:

- The list of shared pollers cannot be retrieved from THWACK
- Any operation that relies on communication with THWACK, such as the upload or download of a poller, will fail.

Check your firewall and proxy settings to make sure that your Orion server can connect to the internet.

Assign Device Studio pollers to monitored devices in the Orion Platform

Specify devices on which you want to poll the statistics defined by the poller.

1. On the Manage Pollers page, select a poller, and click Assign.
2. Select the node you want to assign the poller to.
3. If the node has not been scanned yet, click Scan Now.
4. If the scan result is a match or a multiple match, select the node, and click Enable Poller.

You can only scan SNMP nodes whose status is Up.

Scan monitored objects in the Orion Platform to verify if the OIDs match

When a monitored node is scanned, the OIDs of the monitored node and the OIDs specified in the poller are compared to see if they match.

These scenarios are possible:

- If the OIDs do not match, the scan returns a result indicating the mismatch, and the poller cannot be assigned to the monitored node.
- If the OIDs match, and there is no other poller supporting the specific technology, then the poller is automatically enabled on the node.
If the OIDs match, but there is already another poller for the technology, the new poller is not enabled. You can enable the poller manually. See Assign Device Studio pollers to monitored devices in the Orion Platform.
Access remote nodes in the Orion Platform

You can access nodes through RDP, SSH, and telnet directly from the Orion Web Console.

Use Integrated Remote Desktop in the Orion Platform

Sometimes it is necessary to console into a remote server to troubleshoot an issue. This can be accomplished within the Orion Web Console.

To enable this feature:

1. In the Orion Web Console, select Settings > All Settings and click Manage Accounts under User Accounts.
2. Select your Orion account and click Edit.
3. Under the ALERTS section, select Yes for Allow Browser Integration.
4. Click Submit.

The Node Details page will have an extra set of icons in the upper right, including one that links to the Remote Desktop page.

This feature requires Internet Explorer 9 and earlier.

Press Ctrl+Alt+Break to enter/exit full screen mode.

1. Open the Node Details view for the server you want to view remotely.
   
   The easiest way to open the Node Details view is to click the remote server you want to view in any All Nodes resource.

2. Click ☁, located at the of the Node Details view.
   
   Depending on the security settings of your browser, you may be asked to install an ActiveX control for remote desktop viewing. Follow all prompts to install this required control.

3. Verify the Server IP address or hostname, select an appropriate Screen Size, and then click Connect.

Access nodes using HTTP, SSH, and Telnet in the Orion Platform

To access nodes using protocols for remote device access, you can use in-product browser links to external third party tools using URIs, or use the built-in SSH client in the Orion Web Console.
Access nodes with third-party tools

The Orion Web Console supports the use of HTTP, SSH, and Telnet protocols for remote device access if associated applications like PuTTy and FiSSH on your Orion server are properly registered.

For more information, search the MSDN online help for "Registering an Application to a URI Scheme."

To use the remote access applications, web browser integration for the user account must be enabled. Navigate to the user account, and ensure Allow Browser Integration is set to Yes.

Launch remote access applications from Node Details widgets. These applications are launched on the client, and so the network communication is initiated from the client that launched the tool.

Web-based SSH

You can access network devices and servers using SSH through a web-based feature. On the Node Details page, locate the Management resource, and click SSH. A web-based terminal launches providing an SSH direct terminal connection. You can use SSH commands to modify device settings and troubleshoot server issues.

The SSH session opens from the server that polls the node. If a node is managed by an additional polling engine, the session is opened from the additional polling engine to the device.

The web-based SSH supports all servers with configured SSH access, including Linux hosts, virtual machines, switches, routers, and firewalls.

- The server or network device must be reachable by the Orion server.
- Web-based SSH supports SSH2.
- SSH requires that you open port 22.

Need an SSH client? Try the free tool SolarWinds® Solar-PuTTY.
High Availability in SolarWinds products

SolarWinds High Availability (HA) provides failover protection for your Orion server and additional polling engines to reduce data loss when your primary server goes down. If your primary server fails, the HA feature allows your secondary server to take over all services, such as polling and alerting, with minimal downtime. SolarWinds HA protects your main server, also known as your main polling engine, and additional polling engines. It does not protect your databases or your additional web servers.

SolarWinds supports physical-to-physical, physical-to-virtual, virtual-to-physical, and virtual-to-virtual failover in an IPv4 single subnet (High Availability) or multi-subnet (Disaster Recovery) environment. You can deploy High Availability on both a single subnet and multiple subnets using the same SolarWinds installation.

How does SolarWinds High Availability work?

Single subnet (LAN)

When you configure your environment for SolarWinds High Availability on a single subnet, place your secondary server on the same subnet as the primary server. Configure the secondary server to use the same network and database resources as the primary server. In the Orion Web Console, add both servers to an HA pool, which is accessed through a single Virtual IP (VIP) address or virtual hostname to route incoming requests and messages to the current, active server.

The SolarWinds HA software monitors the health of both servers in the pool, and both servers keep open communication channels over TCP port 5671 to exchange information. When a critical service goes down, such as the SolarWinds Information Service, the software starts the service. If the service goes down a second time within an hour, the software initiates a failover to the standby server.

After a failover to the secondary server is complete, the secondary server becomes the active server and continues to act as the active server until another failover event occurs. The secondary server assumes all of the responsibilities of the primary server, including receiving syslogs, SNMP traps, and NetFlow information through the VIP or virtual hostname. You can manually failover to your primary server to return it to active service.

If you have deployed Orion agents, agents that report to the primary server are updated with the IP addresses of the HA pool members. When the server fails over, the agents send data to the active HA pool member's IP address.
Multiple subnets (WAN)

When you configure your environment for SolarWinds High Availability over a WAN (Disaster Recovery), place your secondary server in the same DNS zone as your primary server. Configure the secondary server to use the same database resources as the primary server. In the Orion Web Console, add both servers to an HA pool, which is accessed through a single virtual hostname to route incoming requests and messages to the current, active server. You can have only two servers in a pool.

The SolarWinds HA software monitors the health of both servers in the pool, and both servers keep open communication channels over TCP port 5671 to exchange information. When a critical service goes down, such as the SolarWinds Information Service, the software starts the service. If the service goes down a second time within an hour, the software initiates a failover to the standby server and edits the DNS host entry to point to the standby server.

After a failover to the secondary server is complete, the secondary server becomes the active server and continues to act as the active server until another failover event occurs. The secondary server assumes all of the responsibilities of primary server, including receiving syslogs, SNMP traps, and NetFlow information through the virtual hostname. You can manually failover to your primary server to return it to active service.

If you have deployed Orion agents, agents that report to the primary server are updated with the IP addresses of the HA pool members. When the server fails over, the agents send data to the active HA pool member's IP address.

How failovers work

After High Availability is enabled and you have set up a pool, each pool monitors itself for failover conditions such as:

- Inability to connect to the network
- Stopped SolarWinds services
  
  Stopped Agent services is not a failover condition.
- Power loss
- Network connection loss to the primary server

When a monitored service is down, the Orion server tries to allow the service to recover before failing over to the secondary server. If the same service fails within the default self-recovery period, a failover occurs.

When a failover condition is met and failover occurs in a pool, a failover event is logged and can be viewed in the Event Summary resource or the Events view. An email is also sent to your default recipients.
For example, if the job engine service is down, the High Availability software attempts to start it. If the job engine fails again within 1 hour, then a failover occurs and the event is logged. If the job engine fails in 61 minutes, a failover does not occur.

Failovers with virtual hostnames

When your HA pool uses a virtual hostname, failovers may not appear to work due to caching issues. The client DNS cache can take up to one minute to redirect traffic to the new active pool member.

However, your browser's DNS cache does not respect the DNS Time to Live (TTL) value, and the DNS cache retention varies between browsers from 60 seconds to 24 hours. You must flush your browser's cache be successfully redirected to the new active pool member.

When do I use a VIP or a virtual hostname?

Use a virtual IP address (VIP) to reference your protected servers when you are protecting a server on a single subnet. Use a virtual hostname either on a single subnet or across multiple subnets.

<table>
<thead>
<tr>
<th></th>
<th>Single Subnet</th>
<th>Multiple Subnets</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>virtual hostname</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

What is a Virtual IP address?

A Virtual IP (VIP) address is an IP address that is shared by both members of a HA server pool on the same subnet. When a member of the pool goes down, the other pool member takes over the VIP address and responds to requests sent to the VIP. The VIP and each pool member must be part of the same subnet.

- The VIP option is only available for HA pools on a single subnet and HA pool members must use static IPv4 IP addresses.
- SolarWinds High Availability does not support IPv6 addresses.
- The VIP option is not available when running HA in the cloud. Instead, you must use a virtual hostname.

How do I choose a VIP address?

You have two options when choosing a VIP address.

- Use your original Orion server's IP as your VIP, and add a new IP address to your manually configured network adapter for your Orion server. This allows devices that you have configured for limited access to a set number of IP addresses to continue to send information to the same IP address. This option requires no device configuration change if your devices can only send information to specific IP addresses.
- Use a new IP address as your VIP when you have no device restrictions.
If you lock down the IP addresses you send information to and receive information from, you must make configuration changes to your devices because the HA pool may send polling requests from one of three IP addresses.

You can use SolarWinds Network Configuration Manager to update your router and switch configurations.

**What is a virtual hostname?**

A virtual hostname is shared by both members of the HA pool. Only the active member of the HA pool responds to the virtual hostname. Use a virtual hostname to connect to your Orion server or additional polling engine HA pools when they span two different subnets or are deployed in the cloud.

You can use a virtual hostname when configuring an HA pool on a single subnet or over two subnets.

**How do I create a virtual hostname?**

You can create a new virtual hostname on the fly when you create an HA pool or create a virtual hostname before creating your HA pool.

SolarWinds strongly discourages you from using your original Orion server's host name as the virtual hostname. You must modify your reverse lookup zones manually in this scenario.

**Which IP address is used as the source when using a VIP?**

Outbound communication from the HA pool, such as WMI or SNMP polling requests, may be sent by the primary or secondary server's IP address or the VIP address. All inbound communication goes through the VIP address.

The active pool member has a minimum of two IP addresses available: the IP address of the server and the VIP address for the pool.

Because there are multiple IP addresses bound to a single NIC, Windows chooses which IP address is used as the originating IP address. The IP address with the most high order bits that match the destination of the next hop is used as the source IP address for all outbound polling activity.

You can determine the source IP address by doing the following:

1. Convert the IP addresses to binary.
2. From left to right, compare how many bits in the IP addresses match the default gateway's IP address.

The IP address with the most consecutive, matching bits is used for the HA pool's source IP address.

In general, choose an IP address that is close to the default gateway's IP address so outbound communication comes from the VIP address, like in the first example. While this VIP selection method is not guaranteed to work, most environments are able to use this method.

All local (same subnet as the Orion server) traffic will source from the "first" address or native.
Examples of matching the binary bits

The following is an example where the VIP is used as the outbound IP address.

<table>
<thead>
<tr>
<th>IP address</th>
<th>IP address converted to binary</th>
<th># of matching bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Gateway (first hop)</td>
<td>10.199.15.1</td>
<td>00001010-11000111-00001111-00000001</td>
</tr>
<tr>
<td>VIP</td>
<td>10.199.15.20</td>
<td>00001010-11000111-00001111-00101000</td>
</tr>
<tr>
<td>Primary pool member</td>
<td>10.199.15.61</td>
<td>00001010-11000111-00001111-00111101</td>
</tr>
<tr>
<td>Secondary pool member</td>
<td>10.199.15.62</td>
<td>00001010-11000111-00001111-00111110</td>
</tr>
</tbody>
</table>

The longest match in the example above is the VIP. It has 27 consecutive matching high order bits to the default gateway.

The following is an example where pool members' IP addresses are used as the outbound IP address.

<table>
<thead>
<tr>
<th>IP address</th>
<th>IP address converted to binary</th>
<th># of matching bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Gateway (first hop)</td>
<td>10.199.15.1</td>
<td>00001010-11000111-00001111-00000001</td>
</tr>
<tr>
<td>VIP</td>
<td>10.199.15.82</td>
<td>00001010-11000111-00001111-01010010</td>
</tr>
<tr>
<td>Primary pool member</td>
<td>10.199.15.61</td>
<td>00001010-11000111-00001111-00111101</td>
</tr>
<tr>
<td>Secondary pool member</td>
<td>10.199.15.62</td>
<td>00001010-11000111-00001111-00111110</td>
</tr>
</tbody>
</table>

In this example, the longest match is the pool members' IP addresses. When a failover occurs, the IP address of the active Orion server is used as the source IP for all polling requests. The VIP address is only used for inbound traffic, such as syslog, SNMP traps, NetFlow, and accessing the Orion Web Console.

SolarWinds High Availability requirements

High Availability on a single subnet is provided for SolarWinds products released on Orion Platform version 2016.2 and later.

High Availability over multiple subnets is provided for SolarWinds products released on Orion Platform version 2017.3 and later.

The products and product versions must match between your primary and secondary pool members.
### Supported products for HA

<table>
<thead>
<tr>
<th>Single subnet</th>
<th>Multiple subnets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Products running on Orion Platform 2016.2 and later</td>
<td>Products running on Orion Platform 2017.3 and later</td>
</tr>
<tr>
<td>Enterprise Operations Console 2.0 and later</td>
<td>Enterprise Operations Console 2.0 and later</td>
</tr>
<tr>
<td>IP Address Manager 4.3.2 and later</td>
<td>IP Address Manager 4.5 and later</td>
</tr>
<tr>
<td>Log Analyzer 1.0 and later</td>
<td>Log Analyzer 1.0 and later</td>
</tr>
<tr>
<td>NetFlow Traffic Analyzer 4.2.1 and later</td>
<td>NetFlow Traffic Analyzer 4.2.2 and later</td>
</tr>
<tr>
<td>Network Configuration Manager 7.5.1 and later</td>
<td>Network Configuration Manager 7.7 and later</td>
</tr>
<tr>
<td>Network Performance Monitor 12.0.1 and later</td>
<td>Network Performance Monitor 12.2 and later</td>
</tr>
<tr>
<td>Server &amp; Application Monitor 6.3 and later</td>
<td>Server &amp; Application Monitor 6.4 hotfix 1 and later</td>
</tr>
<tr>
<td>Server Configuration Monitor 1.0 and later</td>
<td>Server Configuration Monitor 1.0 and later</td>
</tr>
<tr>
<td>Storage Resource Monitor 6.3 and later</td>
<td>Storage Resource Monitor 6.5 and later</td>
</tr>
<tr>
<td>User Device Tracker 3.2.4 and later</td>
<td>User Device Tracker 3.2.4 and later when installed on Orion Platform 2017.3 and later</td>
</tr>
<tr>
<td>Virtualization Manager 8.0 and later</td>
<td>Virtualization Manager 8.0 and later</td>
</tr>
<tr>
<td>VoIP &amp; Network Quality Manager 4.2.4 and later</td>
<td>VoIP &amp; Network Quality Manager 4.2.4 and later when installed on Orion Platform 2017.3 and later</td>
</tr>
<tr>
<td>Web Performance Monitor 2.2.1 and later</td>
<td>Web Performance Monitor 2.2.1 and later when installed on Orion Platform 2017.3 and later</td>
</tr>
</tbody>
</table>

The following products can be integrated with your Orion Platform-based product. The integration module between products is supported under SolarWinds High Availability, but the stand-alone product is not supported.

- Storage Manager 6.2.3
- Virtualization Manager appliance 6.3.2 and later
- Engineers Toolset 11.0.3 and later
- Database Performance Analyzer on Orion 10.2 and later
- Patch Manager 2.1.3 and later
Software and Hardware requirements for HA

SolarWinds strongly recommends that the hardware and software of the standby server matches the primary server. Using matching system specifications and installed software ensures the same performance in the event of a failover.

- SolarWinds does not provide failover support for any database.
- Some SNMP trap, syslog message, and flow data is lost while waiting for the secondary server to become active.

### Hardware/Software Requirements for both servers

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Windows Server 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Windows Server 2019</td>
</tr>
<tr>
<td>Hardware</td>
<td>Must meet the minimum hardware requirements for the products you have installed on the primary server or closely match the primary server</td>
</tr>
<tr>
<td>Software</td>
<td>Must meet the minimum software requirements for the products you have installed on the primary server or closely match the primary server</td>
</tr>
<tr>
<td>IP address version</td>
<td>IPv4</td>
</tr>
<tr>
<td>Database connection</td>
<td>Connection to the SolarWinds Orion database</td>
</tr>
<tr>
<td></td>
<td>If protecting an NTA environment, both servers must be able to connect to the separate NTA Flow Storage database.</td>
</tr>
<tr>
<td>Other (for virtual hostnames)</td>
<td>Windows or BIND DNS administrative server credentials</td>
</tr>
<tr>
<td></td>
<td>BIND version 9.3 and later or Windows DNS on Windows Server 2008 and later</td>
</tr>
</tbody>
</table>

- You can use other DNS servers using your own scripts.
- The primary and secondary server can be joined to a Windows domain

### HA port requirements

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Service/Process</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>UDP</td>
<td>SolarWinds High Availability Service</td>
<td>outbound</td>
<td>Used when failing over with a virtual hostname to update the virtual hostname's DNS entry and for periodic monitoring.</td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Service/Process</td>
<td>Direction</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>----------------------------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>4369</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>bidirectional</td>
<td>TCP ports 4369 and 25672 must be open between the main and secondary servers to allow RabbitMQ clustering between the two servers. These ports exchange EPMD and Erlang distribution protocol messages for RabbitMQ. They do not need to be open in additional polling engine pools.</td>
</tr>
<tr>
<td>5671</td>
<td>TCP</td>
<td>SolarWinds High Availability</td>
<td>bidirectional</td>
<td>Port 5671 must be open into the HA pool with the main Orion server from all Orion servers.</td>
</tr>
<tr>
<td>17777</td>
<td>TCP</td>
<td>SolarWinds installer</td>
<td>bidirectional</td>
<td>Used when installing the standby server software. You can close this port after installation.</td>
</tr>
<tr>
<td>25672</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>bidirectional</td>
<td>TCP ports 4369 and 25672 must be open between the main and secondary servers to allow RabbitMQ clustering between the two servers. These ports exchange EPMD and Erlang distribution protocol messages for RabbitMQ. They do not need to be open in additional polling engine pools.</td>
</tr>
</tbody>
</table>

**Networking requirements for HA**

- Members of the HA pool that includes your main Orion server must be able to resolve the short names of all the other servers.
- All additional polling engines must be able to resolve the host names of each member of the HA pool that includes your main Orion server.
- Additional web servers must be able to resolve the host names of all Orion servers.
- Pool members must be able to resolve each other's host name.
- Devices sending syslogs, SNMP traps, and NetFlow information to your Orion server must be configured to send the information to the VIP address or virtual hostname and receive requests from the pool.
- Devices must be able to accept inbound connections from the source IP addresses.

⚠️ SolarWinds High Availability does not support IPv6 addresses.
Additional requirements for single subnet deployments

- Both your primary and secondary servers must be on the same subnet.
- Both pool members must have static IPv4 addresses set on the network adapter. You do not need dedicated NICs.
- A virtual IP address must be available on the same subnet as the primary and secondary servers.
- Devices must be able to accept inbound connections from the VIP address.
- The maximum supported latency between servers in a pool is 200 ms. SolarWinds recommends that the latency remains under 100 ms.

Depending on your network, you may have additional requirements for single subnet deployments. Up to three IP addresses per pool may be in use among the VIP, primary, and secondary servers because of how Windows calculates the source IP address from the HA pool. You can modify your devices to receive requests from all IP addresses or determine which IP address is used as the source IP address.

Additional requirements for multiple subnet deployments

- Both your primary and secondary servers must be able to communicate with each other using the host names.
- Your primary and secondary servers must use different host names and IP addresses.
- The latency between each HA member can be up to 500 ms. Each member of the pool should have a geographical copy of the SQL database from the SQL Availability Group accessible with a latency under 200 ms, preferably under 100 ms.

You may need to modify firewall rules to allow traffic from pool members and to the VIP address or virtual hostname. For example, you may need to modify the NetFlow firewall rules to allow incoming TCP traffic on port 2055 to go to the VIP address.

High Availability deployment walk-through

The following provides a high-level walk-through of how to set up high availability protection on your main server or additional polling engines.

Before you begin, review the requirements and how to choose a VIP address or virtual hostname.

1. Build a standby server. SolarWinds recommends that your standby server has similar or the same specifications as the primary server.
2. Open port 5671 (TCP) on the primary (incoming) and standby (outgoing) servers.
3. Open ports 4369 and 25672 (TCP) on the main Orion server and its standby server. These ports are not required when protecting additional polling engines.
4. Download and install the secondary server software.
5. Activate your HA pool licenses.
6. Create your HA pool using either a VIP or virtual hostname.
Optional deployment steps

Depending on your network and device configuration, you may need to perform some of the following steps.

- Modify the firewall settings to allow communication to and from the VIP address or virtual hostname and the primary and secondary servers.
- For single subnet deployment, modify your DNS to point your Orion Web Console's host name to the VIP.
- Modify where devices send data to and receive data from.
  - Route all traffic to and from the VIP or virtual hostname. You cannot use a VIP in multi-subnet deployments.
    
      Depending on your network setup, you may be able to change your primary server's IP address to another address in the subnet and use the already established SolarWinds IP address as the VIP address. See When do I use a VIP or a virtual hostname? for more information.
    
  - Route all traffic to and from the IP addresses of the primary and secondary IP addresses. This can be done for both single and multi-subnet deployments.
- Modify additional SolarWinds components to communicate to the HA pool.

Set up the standby server

Your secondary, or backup, server takes over all tasks in case of a failover. Download or move the backup server installer to the secondary server. The installer uses the information on the main server or polling engine to install the correct products and product versions.

If you upgrade an HA pool member, the SolarWinds products installed on the secondary server must match your primary server, including the version numbers and any hotfixes.

You can open the main server’s Orion Web Console while logged in to the secondary server to download the server software instead of moving the installer to the secondary server. You may need to install hotfixes manually on pool members.

Before you begin, you need the credentials for your SolarWinds Orion SQL database.

1. Open the Orion Web Console.
2. Click Settings > All Settings > High Availability Deployment Summary.
3. Click Setup a new HA server.

4. Click Get started setting up a server.

5. **Activate** your HA pool license.

6. On the Setup a High Availability Server dialog, click Download installer now.

7. Move the downloaded installer to your secondary server and run it.
   - Select which type of backup server you want to install under High Availability.
   - Enter your credentials for your Orion SQL database when prompted.

You can now [add the backup server to a pool](#) with your main server or additional polling engine.

**Activate High Availability pool licenses**

High Availability is licensed per pool, which is an internal grouping of a primary and secondary server. You receive a 30-day evaluation license for an unlimited number of HA pools.

You do not need to purchase a second additional polling engine license or additional product licenses for the secondary servers and polling engines in your HA pools.

> **Tip:** If you are setting up multiple pools, activate all of your HA pool licenses. When you set up your HA pools, each pool automatically consumes one HA pool license until no licenses are available.

1. Click Settings > All Settings > License Manager.
2. Select a license.
3. Click activate.
4. Enter your license information.

Licenses are automatically assigned to the pool with the Main poller and then to pools without licenses.

**Set up an HA pool**

An HA pool is a group of two servers that have access to the same network and database resources. The pool includes one main server or additional polling engine and one secondary server or secondary polling engine. Each server is called a pool member and can take over all responsibilities of the other server.
When a pool member is sending and receiving data, it is the active pool member. When a pool member is waiting to take over, it is the standby pool member.

⚠️ If you use a virtual hostname, the browser and computer may cache the host name of the active server. If you are testing using the host names, you may need to flush your DNS cache.

Before you begin, you need the following:

- A VIP address (for single subnet installations)
- A virtual hostname (for multiple subnet installations)
- A secondary HA server
- An available HA pool license

ℹ️ - The software automatically detects if you are installing on a single subnet or multiple subnets.
- Virtual hostnames cannot use punctuation.

**Single subnet**

1. In the Orion Web Console, click Settings > All Settings > High Availability Deployment Summary.
2. Click Setup High Availability pool next to your standby server. If a HA pool license is not available, you are prompted to activate an HA pool license.
3. Choose the server you want to make highly available.
4. Enter the pool name.
5. Enter your VIP or virtual hostname. You can use both VIP and virtual hostname at the same time or neither. If you use a virtual hostname, do not include the domain name.
   *The VIP must be unassigned and on the same subnet as the primary and secondary servers.*
6. Click Next, and review your selections.
7. Click Create Pool to complete the pool setup.

Your main server or additional polling engine is now highly available and can failover to the standby server on the same subnet. An audit event is logged when you create the pool.

When the pool is created, the High Availability Deployment Summary displays the active and standby servers grouped under the pool name. Failover events are logged and you can receive email notifications.

⚠️ You may need to refresh the page to see the correct pool and server status.
SolarWinds recommends that you perform a manual failover after you create your pool and observe the data collected to ensure that all network and device changes are correct.

Multi-subnet

The servers must be able to resolve the host name of the other server in the pool. You may need to update the hosts file on each server.

1. In the Orion Web Console, click Settings > All Settings > High Availability Deployment Summary.
2. Click Setup High Availability pool next to your standby server. If a HA pool license is not available, you are prompted to activate an HA pool license.
3. Choose the server you want to make highly available.
4. Enter the pool name and the virtual hostname. Do not include the domain name in the virtual hostname.
5. Click Next.
6. Select the DNS type.
   - **Microsoft DNS**
     a. Enter the IP address of the DNS server that manages the pool members' DNS Zone.
     b. Enter the DNS Zone.
     c. Enter administrative credentials for the DNS server.

   ! We recommend a local administrator account configured for WMI access. For non-local administrator accounts, we recommend an administrator account with full DACL and remote WMI management enabled.

   - **BIND DNS**

     ! The BIND server must allow the virtual hostname to update dynamically. The operating system must also allow for dynamic updates to the DNS.

     a. Enter the IP address of the DNS server that manages the pool members' DNS Zone.
     b. Enter the DNS Zone.
     c. Enter the TSIG secret key name and the TSIG shared secret key value.

   - **Other**

     ! Use this option if you can use scripts to update the DNS entry for the host name.

     a. Enter the IP address of the DNS server that manages the pool members' DNS Zone.
     b. Enter the DNS Zone.

7. Click Test to validate your Microsoft or BIND credentials and permissions.
8. Click Next to complete the pool setup. The software validates the virtual hostname against the selected DNS server. If the host entry already exists, you are prompted to overwrite the entry or change the virtual hostname.
Your main server or additional polling engine is now highly available and can failover to the standby server across subnets. An audit event is logged when you create the pool and the DNS entry points to the active server.

When the pool is created, the High Availability Deployment Summary displays the active and standby servers grouped under the pool name. Failover events are logged and you can receive email notifications.

SolarWinds recommends that you perform a manual failover after you create your pool and observe the data collected to ensure that all network and device changes are correct.

- You may need to refresh the page to see the correct pool and server status.
- You may set the DNS Time to Live of your virtual hostname record in your script. SolarWinds recommends setting your DNS Time to Live to a shorter time period, such as a minute. You may also need to flush your browser's DNS cache by closing and reopening your browser after manual switchover.

What is a DNS Zone?

All pool members must be managed in the same DNS zone when creating pools that span multiple subnets.

A DNS zone is where you store name information about one or more domains you manage. You can divide your network into multiple subordinate DNS zones to aid in management, organization, or speed. The DNS zone you use for HA pools can be your organization-wide DNS zone but is more likely to be a subspace.

For example, solarwinds.com is our organization-wide DNS zone, but we could decide to manage all North American subnetworks on a separate DNS zone and use the na.solarwinds.com subdomain to access them. While the DNS server for solarwinds.com will have some records for na.solarwinds.com, the DNS server in the na.solarwinds.com DNS zone is the authoritative name server and all management activities for that subdomain occur in that DNS zone.

What are Transaction Signatures?

We require transaction signatures (TSIG) when interacting with BIND DNS instead of administrator credentials. TSIG grants greater security when updating the DNS server.

The **TSIG shared secret key name** is the name you gave the key in the configuration file.

The **TSIG shared key value** is the value contained in the .private file created when you generate the TSIG secret. Use the string after `Key:` in the file.

You must configure your BIND DNS name server in the DNS zone to use the TSIG key you use when creating the HA pool. The key must use the HMAC-MD5 message authentication code with a key size between 1 and 512 bytes. You can use the `dnssec-keygen` utility included in your BIND installation to generate a new key.

If you have never used transaction signatures with BIND DNS before, you must also modify the BIND configuration file to allow DNS updates signed by newly registered TSIG.
Modify BIND DNS to use TSIG example

⚠️ The following is provided as an example only. SolarWinds does not guarantee that this example will work as expected, nor do we support issues regarding BIND DNS. Create backups of your configuration file before beginning, and consult with your vendor's documentation.

1. Log on to your BIND DNS server as an administrator.
2. Open a command prompt and run the following command:
   
   ```
   # dnssec-keygen -a HMAC-MD5 -b <keysiz> -n HOST <keyname>
   ```
   
   The command returns information similar to the following and saves the output to pair of text files having suffix .key and .private:
   
   ```
   K<keyname>+.157+08924
   ```
   
   - A keyname must be a valid domain name without any space and it cannot begin with DHCP_UPDATER.

3. Run the following command to display the generated key:
   
   ```
   # cat K<keyname>+.157+08924.key
   ```
   
   For example, it returns a response similar to the following:
   
   ```
   <keyname>. IN KEY 512 3 157 <secret value>
   ```

4. Register the key in BIND by adding the following code to the configuration file (usually located in /etc/named.conf or /etc/bind/named.conf):

   ```
   key "<keyname>" {
   algorithm hmac-md5;
   secret "<secret value>";
   }
   ```

5. Recofigure BIND using the following command:

   ```
   rndc reconfig
   ```

6. Verify that the new key is registered in your BIND server by running the following command:

   ```
   # rndc tsig-list
   ```

   This command returns information similar to the following:

   ```
   view "_default"; type "static"; key "bindupdate";
   view "_default"; type "static"; key "local-ddns";
   view "_default"; type "static"; key "<keyname>";
   view "_default"; type "static"; key "rndc-key";
   view "_bind"; type "static"; key "bindupdate";
   view "_bind"; type "static"; key "local-ddns";
   view "_bind"; type "static"; key "<keyname>";
   view "_bind"; type "static"; key "rndc-key";
   ```
7. Modify the zone section in the BIND configuration file to allow DDNS updates signed by the registered TSIG.

8. Recofigure BIND using the following command:
   ```
   rndc reconfig
   ```

Choose the server you want to be active in the Orion Platform

If you want a server in your HA pool to be the active server as much as possible, for example, if one server has better hardware specifications, you can choose it as your preferred active server. When a preferred active server fails over, manually or automatically, to the standby server, it will failback to the preferred server when the preferred active server's status is UP.

By default, no preferred server is selected and automatic failback is not enabled.

You cannot select a passive pool member when you create your pool.

1. Select your pool.
2. In the Commands menu, click Edit Pool.
3. Expand Preferred Server Settings.
4. Select the server you want to failback to in the case of a failover.

When a failover occurs, the active server fails back to the preferred server when the preferred server is healthy again.

If the standby server is selected, the server fails over to the preferred server as soon as you save your changes.

Configure High Availability settings

Click Settings > All Settings > High Availability Settings to access these options.

By default, High Availability is enabled and an email is sent when a failover occurs. You can change the default interval and modify your default email settings.

Default interval to consider a member as down in a pool

Define how long the active pool member can be down before a failover occurs. Provide the interval in seconds.

Email me when server status is changed

Choose to receive email messages when a failover occurs. This is enabled by default and uses the default email settings to send notifications. High Availability notifications do not depend on the SolarWinds alerting service or the Orion database, so you still receive High Availability alerts when the service or database is down.
Email me when facility status is changed

Receive email messages when the status of a low-level component changes, such as the percent used of the CPU or RAM. Facilities are used to gauge the health of the system and may trigger a failover condition. For example, the computer may restart and failover if the CPU stays over 100% for a significant amount of time.

SolarWinds recommends disabling this setting due to a potentially large message volume.

Email me when resource status is changed

Receive email messages when a SolarWinds Orion component changes, such as the polling or job engines. Resources are generally SolarWinds-specific processes or services that are monitored by the High Availability software that can trigger a failover condition. For example, if the job engine is down and does not restart successfully, the active server fails over to the standby server.

SolarWinds recommends disabling this setting due to a potentially large message volume.

Set up the default High Availability email for Orion Platform products

The information you provide in the default email action is used to send email messages when there is a status change in an HA pool member, facility, or resource. This is also used as the default information for the Send an Email/Page alert action.

While the information in the default email action is used by default for all SolarWinds email notifications, High Availability-specific notifications are sent independent of the SolarWinds alerting service. When the SolarWinds alerting service or the database is down, you can still receive email notifications for failover events as long as there is a network connection available and your SMTP server is up.

1. Click Settings > All Settings in the menu bar.
2. Click Configure Default Send Email Action.
3. Under the Default Recipients heading, provide the email addresses of all default recipients for any email alert action. For example:
   email@company.com; email2@company.com; distrolist@company.com
   - Separate email addresses with a semicolon.
4. Provide the default sender and reply address.
5. Enter the default SMTP server information.
   - Selecting SSL encryption automatically changes the SMTP port number to 465.

Configure alerts for other DNS types

If you use a non-supported DNS server, you can use alerts, alert actions, and scripts to automatically update the DNS entry for your HA pool when a failover occurs. Your devices must be able to resolve host names managed by the DNS zone you want to use.
SolarWinds does not support other DNS server options. However, we have provided an out-of-the-box alert, Update High Availability Active Member DNS Record on AWS Route53 When Failover Occurs, that you can use as an example.

The following are general steps that you should follow when creating an alert to update DNS entries on non-supported DNS servers. You may need to download other tools to run your scripts successfully.

1. Create a new alert.

   We recommend duplicating Update High Availability Active Member DNS Record on AWS Route53 When Failover Occurs as a base.

2. Trigger the alert when your High Availability Pool Members' Pool ID is not empty. You must also specify a Pool Member Type. For example, the following conditions monitor both your main pool and your additional polling engines.

3. Reset the alert automatically after a period of time, such as one to five minutes.

4. Add an Execute an External Program or External VB Script alert action.

5. Create a DNS host entry update script. You can use following values in your alert actions to pass as parameters to your script.
   - Active member primary IP address = ${N=SwisEntity;M=PrimaryIpAddress}
   - DNS server IP Address = ${N=SwisEntity;M=Pool.DnsIpAddress}
   - DNS Zone = ${N=SwisEntity;M=Pool.DnsZone}
   - Virtual HostName = ${N=SwisEntity;M=Pool.VirtualHostName}

6. Do not add a reset action.

After you create and enable the alert, further test your script by initiating a manual failover.

You may set the DNS Time to Live of your virtual hostname record in your script. SolarWinds recommends setting your DNS Time to Live to a shorter time period, such as a minute. You may also need to flush your browser's DNS cache by closing and reopening your browser after manual switchover.
Modify additional SolarWinds components when using High Availability

The following SolarWinds components must be modified to successfully connect to your HA pool members:

- Network Atlas
- WPM Recorder
- WPM Player (active player mode)
- Desktop Notification Tool
- SWQL Studio

Use the VIP or virtual hostname to connect these components to your SolarWinds installation.

SolarWinds Orion agents and the WPM player (passive player mode) do not need to be modified to communicate with your HA pool members.

Disable or delete HA pools, force a failover, or update an HA pool for Orion Platform products

Use the High Availability Deployment Summary page to view and manage your pools and to view the pool member type.

Disable HA pools

During an upgrade or maintenance procedures on your HA pool members, you must disable your pool. HA pools can also be disabled when you no longer have sufficient HA pool licenses for the number of enabled pools.

1. In the Orion Web Console, click Settings > All Settings > High Availability Deployment Summary.
2. Select the pool you want to disable.
3. Toggle High Availability to Off.

You can also disable the entire feature on the [High Availability Settings] page.
Force a manual failover

When testing SolarWinds High Availability and network configuration changes or when upgrading, you can failover to the standby pool member manually.

- Failover can only occur when both pool members are up, the pool is enabled, and High Availability is enabled.
- If the HA pool uses a virtual hostname, you may need to flush your browser's DNS cache by closing and reopening your browser.

1. In the Orion Web Console, click Settings > All Settings > High Availability Deployment Summary.
2. Select the pool you want to failover manually.
3. Click Commands on the pool details section of the pool you want to failover.
4. Click Force Failover.

The pool fails over to the secondary server and a failover audit event is logged that records who forced the failover and when it occurred.

Update your credentials, VIP address, virtual hostname, or active server

1. In the Orion Web Console, click Settings > All Settings > High Availability Deployment Summary.
2. Select the pool to update.
3. Click Commands on the pool details section.
4. Click Edit Pool.
5. Update your credentials, (including TSIG certificates), VIP address, virtual hostname, or preferred active server.

The pool is saved with the changes you made.

View the pool member type

In addition to polling metrics, individual pool members list a Server Type and an HA Run Type. Select a pool member to view the pool member type and other polling information.

- The Server Type displays the type of Orion server, such as Additional or Main Polling Engine.
- The HA Run Type indicates if the server is currently the active or standby server.

Remove HA pools

You may need to remove one or more HA pools to free an HA pool license or to change pool members.

When you remove a pool in a single subnet pool, the VIP is still reserved in the database and is not recycled so you can re-establish the pool without modifying your network or device settings.
When you remove a pool in a multiple subnet pool, the DNS entry for the virtual host is still in your DNS server and associated with the server that is active when you remove the pool.

1. In the Orion Web Console, click Settings > All Settings > High Availability Deployment Summary.
2. Select the pool you want to remove.
3. Click Commands on the Pool Details section.
4. Click Remove Pool.

An audit event is logged when you remove a pool.