© 2018 SolarWinds Worldwide, LLC. All rights reserved.

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

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, 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 and other SolarWinds marks, identified on the SolarWinds website, as updated from SolarWinds from time to time and incorporated herein, are registered with the U.S. Patent and Trademark Office and may be registered or pending registration in other countries. All other SolarWinds trademarks may be common law marks or registered or pending registration in the United States or in other countries. All other trademarks or registered trademarks contained and/or mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective companies.
# Table of Contents

**Server & Application Monitor Administrator Guide**

- How Orion Platform products work ................................................................. 31
- Introduction to SolarWinds SAM ........................................................................ 32
  - Applications defined and monitored in SAM .................................................... 32
  - How SAM works .................................................................................................. 36
- License Orion Platform products .......................................................................... 38
  - SAM licensing model detailed ........................................................................... 39
    - License consumption ....................................................................................... 40
    - Verify the component monitors consumed per template ............................... 41
    - Manage and activate your SAM license ............................................................ 42
- Evaluate Orion Platform products ......................................................................... 43
  - What happens after an evaluation license expires? .............................................. 44
  - Evaluate performance improvements achieved with Additional Polling Engines and Additional Web Servers ................................................................. 44
  - Evaluate High Availability .................................................................................. 44
- Activate licenses .................................................................................................... 45
  - Activate licenses with Internet access ................................................................. 45
  - Activate licenses offline ..................................................................................... 46
- Upgrade licenses .................................................................................................... 47
  - Update a license .................................................................................................. 47
- Assign licenses to a server .................................................................................... 47
  - Stack licenses (Additional Polling Engines) ....................................................... 47
  - Assign licenses to a polling engine ..................................................................... 48
- Migrate licenses from one server to another ......................................................... 48
  - Migrate licenses with Internet access ................................................................. 48
  - Migrate licenses offline ..................................................................................... 49
Synchronize licenses .................................................................................................................. 50
Security enhancements and exceptions for SolarWinds Orion Platform products .......... 50
Configure the Orion Web Console to use SSL .................................................................. 50
Use a previously installed SSL certificate ........................................................................ 51
Generate a self-signed certificate ....................................................................................... 51
Use SSL after you install an Orion product ....................................................................... 52
Certificate categories .......................................................................................................... 53
What is the Skip website bindings option? ...................................................................... 53
Enable FIPS .......................................................................................................................... 53
Run SolarWinds SAM .......................................................................................................... 55
Uninstall SAM ...................................................................................................................... 55
Upgrade and migrate SAM .................................................................................................. 58
Troubleshooting .................................................................................................................. 58

**Discover and add network devices** .................................................................................. 59

Discover your network with the Discovery Wizard .......................................................... 59
  SNMP credentials ............................................................................................................. 63
    Add SNMP credentials ................................................................................................. 64
Add nodes using Active Directory .................................................................................... 64
Credentials for Active Directory discovery ...................................................................... 65
Automatically add discovered nodes ................................................................................. 65
Add discovered devices to SolarWinds .............................................................................. 67
Add a single node for monitoring .................................................................................... 70
Choose the polling method to use .................................................................................... 72
  External Node (No Status) ............................................................................................ 72
  Status Only: ICMP .......................................................................................................... 72
  Most Devices: SNMP & ICMP . ...................................................................................... 72
  Windows Servers: WMI and ICMP ............................................................................... 72
  Windows and Linux Servers: Agent ............................................................................... 73
Meraki Wireless: API ........................................................................................................... 73
Import nodes from a list of IP addresses ........................................................................ 73
Manage scheduled discovery results .............................................................................. 74
Minimize SNMP processing load during discoveries using the Discovery Ignore List ........ 74
Add ignored devices back to discovery ............................................................................ 74
Manage devices in the Orion Web Console ..................................................................... 75
Delete devices from monitoring ..................................................................................... 75
View node data in tooltips .............................................................................................. 75
Edit node properties ........................................................................................................ 76
  Edit the node name, web address, and the default node view ....................................... 76
  Edit polling settings ....................................................................................................... 77
  Edit dependencies or custom properties ....................................................................... 77
Add data to poll on the node ............................................................................................ 78
  Customize alert thresholds ............................................................................................. 78
Change the polling method for a node ............................................................................ 79
Promote a node from ICMP to SNMP monitoring .......................................................... 79
Promote a Node to WMI Monitoring ............................................................................... 80
Change polling engine node assignments ...................................................................... 80
View the resources and statistics monitored on a node .................................................. 81
Suspend data collection or alerts for nodes in Maintenance Mode .................................... 81
  Mute alerts ..................................................................................................................... 82
  Resume alerts .................................................................................................................. 82
  Stop collecting statistics ............................................................................................... 82
  Start collecting statistics ............................................................................................... 82
Schedule a maintenance period ....................................................................................... 83
Change scheduled maintenance ...................................................................................... 83
Cancel scheduled maintenance from the Node Details resource .................................... 83
Cancel scheduled maintenance from Manage Entities page .......................................... 84
Poll and rediscover devices immediately ................................................................. 84
Group objects and mirror network dependencies in the Orion Web Console ............ 84
Group monitored objects ......................................................................................... 85
Create groups ........................................................................................................... 85
Edit group properties or change the group members .............................................. 86
Delete groups ........................................................................................................... 86
Set the group status based on the status of the group members ............................ 86
Mirror network object dependencies in the Orion Web Console ........................... 87
Create a dependency between network objects ..................................................... 88
Edit a dependency between network objects ....................................................... 89
Delete a dependency between network objects .................................................... 89
Create dependencies between network objects automatically .............................. 89
View active alerts on child objects when the parent object is down ....................... 91

Discover applications in your environment .......................................................... 92
Application Discovery ............................................................................................. 92
Add application monitors to nodes ......................................................................... 94
Customize the application details view .................................................................... 95
  Custom application details view ............................................................................ 95
  Select a view for a template .................................................................................. 95
  Select a view for an application .......................................................................... 96
Customize SAM Application Summary views ....................................................... 97
Create, delete, modify, or restrict views ................................................................... 99
Add resources and columns to views, and define subviews ..................................... 99
  Add widgets to the view from the Customize Page ................................................. 99
  Add resources to the view from the Customize Views page .................................. 100
Divide content into subviews from the Customize Page ......................................... 101
  Divide content into subviews from the Customize Views page ............................ 102
Add subviews using Enable Navigation .................................................................. 103
Optimize views for TV screens or mobile devices .................................................. 103
Enable NOC Views ...................................................................................................... 103
Customize NOC Views ............................................................................................... 104
Exit NOC Views ........................................................................................................... 104
Manage NOC Views .................................................................................................... 104
Display subviews ......................................................................................................... 104
Move resources in NOC Views .................................................................................... 104
Change the NOC view logo .......................................................................................... 105
Viewing node and application data in tooltips ......................................................... 106
Node tooltips ............................................................................................................... 106
Application tooltips .................................................................................................... 107
Add SolarWinds SAM data to the Node Details view ............................................... 108
View events, alerts, traps, and syslogs in the Orion Web Console Message Center ... 109
View network events in the Web Console .................................................................... 109
View notifications ....................................................................................................... 110
Troubleshooting environmental issues with Performance Analysis dashboards .... 111
Compatible SolarWinds products .................................................................................. 111
Create analysis projects ............................................................................................... 112
Create analysis projects from the Performance Analysis dashboard ...................... 112
Create analysis projects from the entity details page ................................................ 113
Update charts in real-time (Real-Time Polling) ......................................................... 114
View the polled data for a plotted metric .................................................................... 114
Modify the time range for all charts .......................................................................... 115
View more information for an entity ........................................................................... 116
Share analysis projects ............................................................................................... 116
View your saved analysis projects .............................................................................. 116
Delete analysis projects .............................................................................................. 116
Add a Performance Analysis Project to the menu ..................................................... 116
Monitor with Orion agents in SAM .................................................................................................................. 118
Overriding agent and agentless monitoring ........................................................................................................ 118
Communication type ............................................................................................................................................. 118
Templates and component monitors ...................................................................................................................... 119
Reports .................................................................................................................................................................. 120
Poll devices with SolarWinds Orion agents ......................................................................................................... 121
SolarWinds Orion agent requirements ................................................................................................................ 121
  Account Privileges ............................................................................................................................................... 123
  Agent port requirements ..................................................................................................................................... 123
  Agent resource consumption .............................................................................................................................. 126
Modify global agent deployment and update settings ........................................................................................ 126
  Navigate to the Agent Settings page .................................................................................................................. 126
Agent communication modes .................................................................................................................................. 127
  Server-initiated communication .......................................................................................................................... 127
  Agent-initiated communication .......................................................................................................................... 127
Configure SNMP for agents .................................................................................................................................... 128
  Configure SNMP .................................................................................................................................................. 129
  Configure SNMP v3 ........................................................................................................................................... 129
  Enable SNMP daemon on AIX computers ........................................................................................................... 131
Credentials and privileges used on Linux-based computers ................................................................................ 133
  SSH credentials .................................................................................................................................................. 133
  Credentials with elevated privileges .................................................................................................................... 134
  SNMP credentials ............................................................................................................................................... 134
  Service account privileges ................................................................................................................................ 134
Certificates and the agent ....................................................................................................................................... 134
Deploy agents to nodes ......................................................................................................................................... 135
  Deploy an agent with the Add Node wizard ......................................................................................................... 135
  Deploy agents to monitored nodes ...................................................................................................................... 136
Deploy the agent manually to a Windows computer .......................................................... 137
Deploy an agent manually to a Linux-based computer ......................................................... 138
Mass deploy an agent on Windows using MST files and a Group Policy ............................... 139
Deploy agents on Linux-based computers through a repository .......................................... 141
Deploy with a Gold Master Image ..................................................................................... 142
Deploy on Windows Core Servers .................................................................................... 143

View agent connections and status, update agents, or manage agents ................................ 146
Choose a list of resources and statistics to monitor .............................................................. 146
Manage the agent as a new node ....................................................................................... 147
View installed agents details .............................................................................................. 147
Reboot the node the agent is installed on ........................................................................... 147
Update the agent manually ................................................................................................ 147
Re-establish a connection to a agent using server-initiated communication ..................... 148
Edit agent settings ............................................................................................................ 149
Track your polling method ................................................................................................ 150
View the status of agent plug-ins ...................................................................................... 151
Edit agent connection settings or reprovision the agent once deployed ............................ 152
Connect to or register a previously installed agent to modify connection or update settings .... 153
Change the agent port to match the open port on the Orion server .................................... 154
Change the agent communication mode on the remote node ............................................ 155

Migrate agents from one Orion instance to another ............................................................ 156
Redeploy agents from the Orion Web Console to a monitored node .................................... 156
Edit agent connection settings or reprovision the agent once deployed ............................ 157
Use a group policy to migrate agents on Windows .............................................................. 158

Troubleshooting agents ...................................................................................................... 159
Troubleshooting agent installation, deployment, and connections ........................................ 159
Troubleshooting agent configuration .................................................................................. 160
Troubleshooting agent connections ................................................................................... 161
Monitor your environment using AppStack ................................................................. 162
Troubleshooting with AppStack .................................................................................. 163
AppStack categories and data ..................................................................................... 164
Supported categories and data .................................................................................... 165
AppStack data overview .............................................................................................. 168
Object status and colors ............................................................................................... 169
Using quick links ......................................................................................................... 170
Using the overview bar ................................................................................................. 171
Customize the AppStack view ...................................................................................... 172
Use filters for AppStack ............................................................................................... 173
Filter options ................................................................................................................. 173
Creating filters ............................................................................................................. 174
AppStack filter options .............................................................................................. 174
Create an AppStack layout ......................................................................................... 175
Monitor cloud instances and VMs ............................................................................... 176
Cloud monitoring recommendations ........................................................................... 177
Cloud monitoring requirements .................................................................................. 178
Cloud metrics vs. OS metrics ...................................................................................... 178
Add the first cloud account to the Orion Platform ...................................................... 179
  Working in the Cloud Summary page ...................................................................... 180
Explore cloud instances and VMs on the Cloud Summary page ............................. 182
Configure cloud accounts for the Orion Platform ..................................................... 184
  Configure AWS accounts for cloud monitoring ...................................................... 184
  Configure Microsoft Azure for cloud monitoring ................................................... 188
Cloud service polling overview .................................................................................. 189
Cloud metrics vs. OS metrics ...................................................................................... 189
AWS polling ................................................................................................................ 190
Azure polling ............................................................................................................... 196
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throttling overview</td>
<td>200</td>
</tr>
<tr>
<td>AWS throttling</td>
<td>200</td>
</tr>
<tr>
<td>Azure throttling</td>
<td>201</td>
</tr>
<tr>
<td>Manage your cloud infrastructure</td>
<td>202</td>
</tr>
<tr>
<td>Find cloud account credentials</td>
<td>202</td>
</tr>
<tr>
<td>Configure cloud monitoring settings</td>
<td>203</td>
</tr>
<tr>
<td>Stop an AWS cloud instance/VM</td>
<td>209</td>
</tr>
<tr>
<td>Stop an Azure cloud VM</td>
<td>209</td>
</tr>
<tr>
<td>Reboot a cloud instance/VM</td>
<td>210</td>
</tr>
<tr>
<td>Delete a cloud instance/VM</td>
<td>210</td>
</tr>
<tr>
<td>Unmanage and manage a cloud instance/VM</td>
<td>211</td>
</tr>
<tr>
<td>Poll a cloud instance/VM immediately</td>
<td>211</td>
</tr>
<tr>
<td>Manage monitoring for cloud service accounts</td>
<td>212</td>
</tr>
<tr>
<td>Configure a cloud instance/VM as a managed node</td>
<td>213</td>
</tr>
<tr>
<td>Configure a VM for use as a managed node in the Orion Platform</td>
<td>215</td>
</tr>
<tr>
<td>Create cloud application monitors and templates</td>
<td>217</td>
</tr>
<tr>
<td>Manage cloud monitoring alerts</td>
<td>218</td>
</tr>
<tr>
<td>Troubleshoot cloud monitoring</td>
<td>220</td>
</tr>
<tr>
<td>Monitor application dependencies</td>
<td>227</td>
</tr>
<tr>
<td>Application Dependencies polling overview</td>
<td>228</td>
</tr>
<tr>
<td>How SAM uses Orion agents to find and monitor application dependencies</td>
<td>229</td>
</tr>
<tr>
<td>Agent plug-in overview</td>
<td>229</td>
</tr>
<tr>
<td>Configure the Application Dependencies feature</td>
<td>231</td>
</tr>
<tr>
<td>Before you begin</td>
<td>231</td>
</tr>
<tr>
<td>Deploy Orion agents to nodes that host applications you want to monitor</td>
<td>232</td>
</tr>
<tr>
<td>Assign application monitors to nodes</td>
<td>233</td>
</tr>
<tr>
<td>Customize polling settings</td>
<td>233</td>
</tr>
<tr>
<td>Access application dependencies data</td>
<td>234</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Incoming Connections resource</td>
<td>234</td>
</tr>
<tr>
<td>Connection Details page</td>
<td>237</td>
</tr>
<tr>
<td>Manage polling for application dependencies</td>
<td>239</td>
</tr>
<tr>
<td>Manage Application Dependency polling</td>
<td>240</td>
</tr>
<tr>
<td>Manage Connection Quality polling</td>
<td>242</td>
</tr>
<tr>
<td>Troubleshoot application dependency issues</td>
<td>243</td>
</tr>
<tr>
<td>Agent-related issues</td>
<td>244</td>
</tr>
<tr>
<td>Data-related issues</td>
<td>246</td>
</tr>
<tr>
<td>Application Dependencies log files</td>
<td>248</td>
</tr>
<tr>
<td>Check Application Dependencies services</td>
<td>249</td>
</tr>
<tr>
<td>Handle HTTP listeners port sharing in Windows</td>
<td>249</td>
</tr>
<tr>
<td>Monitor application dependencies for Windows Failover Clusters (WFCs)</td>
<td>250</td>
</tr>
<tr>
<td>Monitor hardware health</td>
<td>251</td>
</tr>
<tr>
<td>Monitored Hardware Sensors</td>
<td>252</td>
</tr>
<tr>
<td>Enable hardware health monitoring</td>
<td>252</td>
</tr>
<tr>
<td>Enable monitoring from the Add Node wizard</td>
<td>252</td>
</tr>
<tr>
<td>Enable hardware health monitoring on a node</td>
<td>253</td>
</tr>
<tr>
<td>Enable, disable, or adjust hardware health sensors</td>
<td>253</td>
</tr>
<tr>
<td>Update hardware health statistics</td>
<td>254</td>
</tr>
<tr>
<td>Enable hardware sensors</td>
<td>254</td>
</tr>
<tr>
<td>Disable hardware sensors</td>
<td>254</td>
</tr>
<tr>
<td>Edit hardware health thresholds</td>
<td>255</td>
</tr>
<tr>
<td>Change the MIB used for polling hardware health statistics</td>
<td>255</td>
</tr>
<tr>
<td>Change the MIB tree used for polling hardware health globally</td>
<td>256</td>
</tr>
<tr>
<td>Change the MIB for polling hardware health statistics on a specific node</td>
<td>256</td>
</tr>
<tr>
<td>Change hardware health temperature units</td>
<td>256</td>
</tr>
<tr>
<td>Monitor Syslog messages</td>
<td>256</td>
</tr>
<tr>
<td>Before you begin</td>
<td>257</td>
</tr>
</tbody>
</table>
Configure the SolarWinds Orion server to use the correct syslog port ...................................... 257
Syslog message priorities ........................................................................................................... 257
  Syslog facilities ....................................................................................................................... 258
  Syslog severities ...................................................................................................................... 258
  Syslog facilities ....................................................................................................................... 259
  Syslog severities ...................................................................................................................... 260
View Syslog messages in the Orion Web Console ................................................................. 261
Clear Syslog messages in the Orion Web Console ................................................................. 262
View and clear Syslog messages in the Syslog Viewer ........................................................... 262
Search for Syslog messages in the Syslog Viewer ................................................................. 262
Define the number of messages displayed, message retention, and the displayed columns in the Syslog Viewer ................................................................. 263
Trigger alerts when receiving specific Syslog messages ....................................................... 263
Forward syslog messages ......................................................................................................... 265
Monitor SNMP traps .............................................................................................................. 266
Before you begin ...................................................................................................................... 266
View SNMP traps in the Orion Web Console ........................................................................ 266
View current traps in the Trap Viewer .................................................................................. 267
Search for traps in the Trap Viewer ...................................................................................... 267
Define how many traps to display, if you want to refresh the traps view, trap retention, and the information displayed in the Trap Viewer .................................................. 268
Configure Trap Viewer filters and alerts ................................................................................ 268
What is a Trap Template? ........................................................................................................ 269
Monitor Quality of Experience metrics ................................................................................ 271
How SolarWinds Packet Analysis Sensors work ................................................................. 272
  Network Packet Analysis Sensor (NPAS) .............................................................................. 272
  Server Packet Analysis Sensor (SPAS) .................................................................................. 272
Limitations to Packet Analysis Sensors .................................................................................. 272
Common Packet Analysis Sensor deployment scenarios ...................................................... 273
Aggregation per application ................................................................. 274
Aggregation per site ......................................................................... 276
Aggregation per computer ................................................................. 278
Monitor traffic to and from a port mirror, SPAN, or network tap .......... 280
Monitor traffic to and from a specific node ........................................ 282
Remove a sensor ............................................................................. 283
Monitor QoE applications and nodes .................................................. 284
Manage global QoE settings ............................................................... 284
Monitor applications for QoE ............................................................. 285
Monitor nodes with a network sensor .................................................. 287
Ignore traffic from applications or nodes ............................................ 288
Define custom HTTP applications ..................................................... 289
Advanced sensor configuration ......................................................... 289
Configure which interface to monitor for traffic ................................. 290
Set the number of CPU cores and the amount of memory QoE can use 290
Configure QoE thresholds ................................................................. 291
Packet Analysis Sensor agents .......................................................... 291
Integrate an Orion Platform product with ServiceNow .................... 291
Before you begin ............................................................................. 292
Install and configure the SolarWinds Alert Integration application in ServiceNow .... 292
Create a ServiceNow integration user with Web service access only .... 292
Configure an Orion Platform product with ServiceNow .................... 293

Manage Asset Inventory ..................................................................... 294
Enable and disable the Asset Inventory dashboard ............................. 295
Asset Inventory data collection ........................................................... 296
Add server hardware monitoring ....................................................... 296

Manage processes, services, tasks, and events in real time ................. 298
Real-Time Process Explorer ............................................................... 299
Monitor unmonitored processes .......................................................................................... 300
Use the Real-Time Process Explorer .................................................................................. 301
Real-Time Process Explorer alerts ...................................................................................... 303
Real-Time Process information in top 10 alerts .................................................................. 304
Real-Time Event Log Viewer ............................................................................................... 306
Service Control Manager ..................................................................................................... 310
Windows Scheduled Task Monitor ....................................................................................... 313
  Windows Scheduled Task Monitor returned status codes .................................................... 316
  WTSM status ....................................................................................................................... 319

AppInsight Applications ...................................................................................................... 321

AppInsight for Exchange ..................................................................................................... 322
  Navigating AppInsight for Exchange .................................................................................. 322
  Recommendations for AppInsight for Exchange ................................................................. 324
  Configure AppInsight for Exchange on nodes ................................................................. 325
  AppInsight for Exchange requirements and permissions .................................................. 328
    Microsoft Exchange Versions Supported: ....................................................................... 328
    AppInsight for Exchange Requirements and Permissions .............................................. 329
    PowerShell Requirements ............................................................................................... 329
  Edit the AppInsight for Exchange template ...................................................................... 330
  Advanced Manual Configuration of AppInsight for Exchange .......................................... 331
    Configuration changes to enable AppInsight for Exchange ........................................... 331
    Verify Microsoft Exchange credentials ........................................................................ 332
  Manually configure the Microsoft Exchange server .......................................................... 333
    Define Exchange credentials ......................................................................................... 333
    Grant Exchange Access .................................................................................................. 334
    Set Mailbox Search Access ............................................................................................. 335
    Install PowerShell 2.0 ...................................................................................................... 335
    Set PSLanguageMode to FullLanguage for the PowerShell website ................................ 335
Create a self-signed certificate ................................................................................. 335
Configure WinRM 2.0 on an Exchange server ....................................................... 336
Create a firewall rule .............................................................................................. 337
Configure IIS ........................................................................................................ 338
Test the application ............................................................................................... 339
Set PowerShell permissions for Exchange ........................................................... 341
Resolving errors after a reinstall ......................................................................... 341
Find Exchange URL settings ................................................................................ 342
Attachment extensions acknowledged by AppInsight for Exchange .................... 345

**AppInsight for IIS** .............................................................................................. 346

Navigate the AppInsight for IIS details view ......................................................... 346
Configure AppInsight for IIS on nodes .................................................................. 348
Add through the Discovery Wizard ........................................................................ 348
Add via manual configuration ............................................................................... 349
AppInsight for IIS requirements and permissions ............................................... 350
AppInsight for IIS requirements and permissions ............................................... 350
AppInsight for IIS technologies and ports ......................................................... 351

Edit the AppInsight for IIS template .................................................................... 353
Manually configure AppInsight for IIS ................................................................. 354
Install PowerShell 2.0 and the WebAdministration snapin ................................ 355
Download PowerShell 2.0 .................................................................................... 355
Install PowerShell 2.0 on Windows Server 2008 and 2008 R2 .......................... 355
Set execution policy on the target computer ....................................................... 357
Create a self-signed certificate ............................................................................. 358
Create a firewall rule ............................................................................................ 359
Update WsMan limits ............................................................................................ 360
Create a WinRM listener ....................................................................................... 361
Find IIS URL settings ........................................................................................... 362
Verify a server's WinRM PowerShell instance ............................................................. 362

**AppInsight for SQL** .................................................................................................. 364

Add AppInsight for SQL to a node ............................................................................. 369

AppInsight for SQL requirements and permissions ................................................. 371

AppInsight for SQL permissions ............................................................................... 372

Monitor an SQL named instance with AppInsight for SQL ..................................... 374

Monitor clusters with AppInsight for SQL ............................................................... 376

Edit the AppInsight for SQL template .................................................................... 379

**Manage application monitor templates and component monitors** ....................... 381

Manage templates .................................................................................................... 385

Create a template ..................................................................................................... 385

Create a custom template (Example) ....................................................................... 386

Create a SolarWinds Windows service application template ..................................... 386

Assign a template to a node ..................................................................................... 387

Edit a template ......................................................................................................... 387

Copy a template ........................................................................................................ 388

Export and import templates ..................................................................................... 388

Delete templates ........................................................................................................ 391

Tag a template ........................................................................................................... 391

Change between 32-bit and 64-bit polling ................................................................ 391

Modify and customize monitors ............................................................................... 393

Multi-edit components ............................................................................................. 393

Delete or Disable a monitor ....................................................................................... 394

Linux/Unix system configurations for component monitors .................................... 394

Apache configurations ............................................................................................. 394

Tomcat configurations ............................................................................................. 395

JMX ............................................................................................................................. 396

Squid ............................................................................................................................ 397
Nagios ......................................................................................................................... 397
ODBC configurations ............................................................................................... 398
PostgreSQL configurations ....................................................................................... 398
MySQL configurations .............................................................................................. 400
IBM DB2 with ODBC configurations ................................................................. 402
  Linux-based computers ....................................................................................... 402
  Configure DB2 on AIX devices ............................................................................. 404
Monitors and templates using WMI ................................................................. 407
  Component monitors using WMI ........................................................................ 407
  Templates using WMI .......................................................................................... 407
Assign and edit application monitors to nodes ................................................. 412
Create component monitors from the Component Monitor Wizard ............... 412
Scan nodes for applications .................................................................................. 414
Unmanage and manage assigned application monitors ................................... 416
Manage templates and groups ............................................................................. 417
  Assign an application template to a group .......................................................... 417
  Unassign application monitors from a group ...................................................... 420
  Assign an application template to a group .......................................................... 421
  Unassign application monitors from a group ...................................................... 424
Script custom component monitors ................................................................. 425
  Linux/Unix Script monitor ................................................................................ 426
    Field Descriptions ............................................................................................ 427
    Create a Linux or Unix script monitor ............................................................. 428
    Nagios scripting ............................................................................................... 432
  Windows Script monitor ..................................................................................... 433
    Field Descriptions ............................................................................................ 433
    Create a Windows Script Monitor ................................................................... 435
    Nagios Script monitor ....................................................................................... 439
Field Descriptions ........................................................................................................ 440
Scripts must report status through return codes ......................................................... 441
Test script output ........................................................................................................ 442
Windows PowerShell monitor ....................................................................................... 444
Field Descriptions ........................................................................................................ 444
Create a Windows PowerShell monitor ........................................................................ 446
Application Monitor Thresholds ................................................................................... 449
Inheriting Thresholds .................................................................................................... 450
Threshold Adjustments at the Template Level ............................................................... 450
Threshold Adjustments at the Component Monitor Level ............................................ 450
Multi-Value scripts and thresholds .............................................................................. 451
Apply baseline thresholds at the template level .......................................................... 452
Apply baseline thresholds at the application level ....................................................... 454
Adjust threshold settings and apply baseline data ....................................................... 456
How SAM calculates the baseline ............................................................................... 456
Change the amount of data used in baseline calculations ............................................ 457
Apply baseline thresholds at the template level .......................................................... 457
Apply baseline thresholds at the application level ....................................................... 458
Use latest baseline details .......................................................................................... 459
Edit capacity planning thresholds .............................................................................. 459
View latest baseline details .......................................................................................... 461
View the Latest Baseline Details Page ......................................................................... 461
Example tasks for application monitors ..................................................................... 462
Create your first application and alert ......................................................................... 463
Create a WMI monitor .................................................................................................. 463
Apply the WMI monitor template ............................................................................... 463
Alert on the WMI application via email ........................................................................ 463
Scan for applications to monitor ................................................................................ 465
Monitor a specific URL .............................................................................................................. 466
Monitor VMware performance counters using an application monitor ........................................ 467
Add components to the application monitor .............................................................................. 467
Monitor and restart stopped Windows services ......................................................................... 469
Create the monitor ..................................................................................................................... 469
Create an alert that restarts any stopped Windows services and sends an email ...................... 469
Monitor large directories ............................................................................................................ 470
Monitor IIS application pools ...................................................................................................... 472
Use the JMX component monitor wizard .................................................................................... 473
Add a JMX component monitor .................................................................................................. 473
Configure the SOAP monitor ....................................................................................................... 474
Load WSDL Files ........................................................................................................................ 474
Manually Enter XML ................................................................................................................... 475
Assign an application template to a group .................................................................................... 477

**Use alerts to monitor your environment** .................................................................................. 480
Alert preconfiguration tasks ........................................................................................................ 480
Configure the default information in the email action ................................................................. 481
Best practices and tips for alerting ............................................................................................... 481
Navigate to the Alert Manager ..................................................................................................... 482
Add an SMTP server .................................................................................................................... 482
SAM alert variables ...................................................................................................................... 483
  Component Monitor properties for alerts ................................................................................. 483
  Component Monitor variables for alerts .................................................................................... 486
Application Monitor properties for alerts .................................................................................... 494
Application Monitor variables for alerts ...................................................................................... 494
Create new alerts to monitor your environment .......................................................................... 500
Set alert properties ...................................................................................................................... 501
Define the conditions that must exist to trigger an alert ............................................................. 502
Define the conditions that must exist to reset an alert ................................................................. 504
Schedule when an alert monitors your environment ............................................................................ 505
Define what happens when an alert is triggered ................................................................................. 506
   Add actions to alerts ......................................................................................................................... 507
   Add what happens when an alert is not acknowledged ................................................................. 508
Define what happens when the alert is reset ....................................................................................... 508
Review the alert's configuration ............................................................................................................ 509
Commonly created alerts ..................................................................................................................... 509
   Alert me when a server goes down ................................................................................................. 510
   Alert on custom properties ............................................................................................................. 511
View triggered alerts in the Orion Web Console ................................................................................ 512
Remove alerts from the Active Alerts list .......................................................................................... 512
Test alert triggers and actions ............................................................................................................ 513
   Test trigger conditions ................................................................................................................... 513
   Test alert actions while creating or editing an alert .................................................................... 513
   Test alert actions in the Action Manager .................................................................................... 514
Modify multiple alerts or share alerts ................................................................................................ 514
   Add actions to alerts without opening the Alert Wizard ............................................................. 514
   Share alerts with others ................................................................................................................ 514
Build complex conditions .................................................................................................................. 515
   How conditions are evaluated ...................................................................................................... 515
   Wait for multiple objects to meet the trigger condition .............................................................. 516
Evaluate multiple condition blocks .................................................................................................... 517
   How condition blocks are evaluated ............................................................................................. 517
Evaluate multiple object types ............................................................................................................ 518
Manage alert actions .......................................................................................................................... 518
   Assign an action to an alert ............................................................................................................ 518
   Enable and Disable Alerts ........................................................................................................... 518
Available alert actions .......................................................................................................................... 518
Change a custom property ..................................................................................................................... 518
Create a ServiceNow incident .............................................................................................................. 519
Use reference fields .............................................................................................................................. 519
Filter expression examples .................................................................................................................... 520
Configure a ServiceNow incident ......................................................................................................... 520
Dial a paging or SMS service .................................................................................................................. 521
Email a web page to users ..................................................................................................................... 521
Create a dynamic URL ........................................................................................................................... 522
Execute an external batch file ................................................................................................................ 522
Execute an external Visual Basic script .................................................................................................. 523
Log the alert message to a file ............................................................................................................... 523
Log the alert to the NPM event log ....................................................................................................... 524
Change the resource allocation of a virtual machine ............................................................................ 525
Delete a snapshot of a virtual machine .................................................................................................. 526
Move a virtual machine to a different host ........................................................................................... 526
Move a virtual machine to a different storage ....................................................................................... 527
Pause a virtual machine ........................................................................................................................ 528
Power off a virtual machine .................................................................................................................. 529
Power on a virtual machine ................................................................................................................... 529
Restart a virtual machine ....................................................................................................................... 530
Suspend a virtual machine ..................................................................................................................... 530
Take a snapshot of a virtual machine ..................................................................................................... 531
Play a sound when an alert is triggered ................................................................................................. 532
Send a Windows Net message ............................................................................................................. 533
Restart IIS sites or application pools .................................................................................................... 533
Send an SNMP trap ............................................................................................................................... 534
Send a GET or POST request through HTTP or HTTPS ..................................................................... 535
Send a syslog message ................................................................. 535
Send an email or page ................................................................. 536
Manually set a custom status ..................................................... 537
Use the speech synthesizer to read alerts .................................. 538
Log an alert to the Windows Event Log on a specific server ........ 538
Changes in the alerting engine .................................................... 539
Changed or removed functionality ............................................. 539
Database changes ..................................................................... 539
Macro or variable changes ......................................................... 540
Alert migration to the web ......................................................... 540
Migration issues ....................................................................... 540
Limitations to migrated alerts ................................................... 541
General alert variables ............................................................. 541
Defunct alert variables ............................................................ 542
Share alerts with other SolarWinds products ............................. 542

**Manage reports in the Orion Web Console** ................................ 544
Predefined reports .................................................................... 544
Modify an existing web-based report ....................................... 544
Create a web-based report ....................................................... 545
Customize a web-based report layout ...................................... 547
Add content to a web-based report ......................................... 548
Add a custom chart or table to a web-based report .................. 548
  Add a data series and customize a chart ............................... 549
  Add a data series and customize a table .............................. 550
Build conditions ...................................................................... 551
Restrict who can access reports .............................................. 552
Create or add a report limitation category ............................... 553
Restrict user access to the report ............................................ 553
Generate reports on a schedule ................................................................. 553
Schedule a report to run automatically while creating or editing a report ................................................. 553
Create and assign report schedules in Report Manager ................................................................. 554
Create a report schedule ........................................................................ 554
Assign a report to a schedule or multiple schedules ............................................................. 555
Schedule reports from the Schedule Manager ........................................................................... 555
Export and import reports ...................................................................................... 555
Export reports as XML .................................................................................. 556
Import XML reports ...................................................................................... 556
Export reports to Excel spreadsheets from the Orion Web Console ........................................... 556

**Manage the Orion Web Console** .................................................................................. 557

Log in to the Orion Web Console ................................................................................ 557
Manage Orion Polling Engines ................................................................................. 557
Use additional polling engines to balance polling ......................................................... 557
Pre-flight checklist ............................................................................................... 558
Port requirements for Additional Polling Engines ......................................................... 558
Install an Additional Polling Engine .......................................................................... 559
Activate Additional Polling Engine licenses .................................................................. 560
View a polling engine status .................................................................................. 560
Update polling settings .......................................................................................... 560
Configure polling interval settings ........................................................................... 560
Configure polling statistics intervals .......................................................................... 561
Configure the dynamic IP address and hostname resolution .......................................... 562
Configure Database Settings ................................................................................... 562
Configure network settings ..................................................................................... 564
Configure calculations and threshold settings .............................................................. 565
Calculate node availability ...................................................................................... 566
Node Status ........................................................................................................... 566
Percent Packet Loss .................................................................................................................. 566
Define baselines for nodes ........................................................................................................ 567
Define a baseline for an individual node .................................................................................. 567
Define a baseline for multiple nodes ...................................................................................... 567
Assign credentials to virtual servers ....................................................................................... 567
Assign credentials to Hyper-V servers .................................................................................... 568
Assign credentials to VMware servers .................................................................................... 568
Set general thresholds ............................................................................................................ 568
Set how many retries are necessary before packet loss is reported ...................................... 568
Set the node warning level ....................................................................................................... 569
Delete polling engines ............................................................................................................ 570

Thresholds ................................................................................................................................. 570
Set general thresholds ............................................................................................................ 571
Customize thresholds for single objects .................................................................................. 571
General threshold types ........................................................................................................... 572
Baselines and baseline calculations ....................................................................................... 573
What data is subject to statistical baseline calculation? ........................................................... 573
Use mean and standard deviations as thresholds .................................................................... 574
Customize how the baseline is calculated ............................................................................... 574

Manage Orion Web Console user accounts ........................................................................... 575
Create users .............................................................................................................................. 575
Create users based on existing Active Directory or local domain accounts ............................ 576
Change account passwords ....................................................................................................... 578
Enable users to authenticate through LDAP ............................................................................ 578
Define what users can access and do ....................................................................................... 579
Set default menu bars and views for users ............................................................................... 582
Limit users to specific network areas ....................................................................................... 583
Restrict user access to network areas by applying limitations ............................................... 583
Patterns for limitations ................................................................. 584
Create limitations based on custom properties ................................ 584
Delete account limitations ............................................................. 585
Configure automatic login ............................................................ 585
Enable Windows Authentication with Active Directory ..................... 586
Log in with Windows pass-through security .................................... 588
Share views with non-Orion Web Console users ............................... 589
Automatically login by passing your credentials through the URL ....... 590
Administrative functions of the Orion Web Console ......................... 590
View secure data ......................................................................... 590
Handle counter rollovers ................................................................ 590
Configure web proxy settings ......................................................... 591
Orion Web Console and chart settings .......................................... 592
Auditing Settings ....................................................................... 594
Chart Settings ........................................................................... 594
Discovery Settings ..................................................................... 595
Worldwide Map Settings .............................................................. 595
Active Alert Settings .................................................................. 595
Web Console settings .................................................................. 595
Auditing settings ...................................................................... 597
Chart settings ........................................................................ 597
Discovery, Worldwide Map, and Active Alerts settings ................... 598
Active Alerts settings .................................................................. 598
Custom properties ...................................................................... 598
Create a custom property .............................................................. 599
Remove a custom property ............................................................ 601
Import custom property values ....................................................... 602
Export custom property data ......................................................... 603
Change custom properties values ................................................................. 603
Edit values for custom properties ................................................................. 603
Filter objects when assigning custom properties ........................................... 604

**Customize the Orion Web Console look, views, settings, charts, and maps** 605

My Dashboards ................................................................................................. 605
Customize My Dashboards .............................................................................. 606
Specify My Dashboards and Alerts & Activity items for users ....................... 606
Add items to My Dashboards .......................................................................... 608
Add menu bars ................................................................................................. 609
Change the Orion Web Console color scheme ............................................... 609
Change the Orion Web Console logo .............................................................. 609
Use Orion Web Console breadcrumbs ............................................................ 610
Customize breadcrumbs .................................................................................. 610

Customize resources in the Orion Web Console ............................................. 610
Filter nodes in resources using SQL queries .................................................. 611
SQL query examples ....................................................................................... 611
Specify what a Custom Object resource displays ........................................... 611

Widget configuration examples ....................................................................... 612
Display a Network Atlas map in the Orion Web Console ............................... 612
Display a list of objects on a network map ....................................................... 613
Display a custom list of available maps .......................................................... 613
Display the Worldwide Map ............................................................................ 613
Display events received during a given time period ......................................... 614

Specify user-defined links .............................................................................. 614
Specify Custom HTML ..................................................................................... 615
Filter nodes ...................................................................................................... 615
Group nodes within a view ............................................................................... 616
Add a Service Level Agreement Line to charts (SolarWinds NPM) .................. 616
Customize views .................................................................................................................. 617
Create, delete, modify, or restrict views ............................................................................. 617
Create new views .................................................................................................................. 617
Add resources and columns to views, and define subviews ................................................ 618
Create custom summary views ............................................................................................ 622
Enable NOC View Mode ........................................................................................................ 624
Optimize views for TV screens or mobile devices ................................................................. 624
Limit objects on a view .......................................................................................................... 626
Use a view as a template ........................................................................................................ 627
Delete views .......................................................................................................................... 627
Specify views for device types .............................................................................................. 627
Widget configuration examples ............................................................................................. 627
Add external websites ............................................................................................................ 632

Maintain the SolarWinds Orion database ............................................................................ 633
Additional resources ............................................................................................................. 633
Database maintenance ........................................................................................................... 633
Check the database size ........................................................................................................ 634
Specify the time to run database maintenance ...................................................................... 634
Adjust retention periods ........................................................................................................ 635
Launch database maintenance manually ................................................................................ 635
Back up and restore the database .......................................................................................... 635
View database details and data in the Database Manager ...................................................... 636
Add a server to Database Manager ....................................................................................... 636
View database details ............................................................................................................ 636
View table details ................................................................................................................... 637
Update Orion Platform products to use the new database .................................................... 637

High Availability in SolarWinds products ........................................................................... 639
How does SolarWinds High Availability work? ..................................................................... 639
View the pool member type ................................................................. 653
Remove HA pools ............................................................................. 653
How failovers work ............................................................................ 654
Failovers with virtual hostnames ...................................................... 654
Which IP address is used as the source? ............................................ 654
Examples of matching the binary bits .............................................. 655
What is a DNS Zone? ........................................................................... 656
What are Transaction Signatures? .................................................... 656
  Modify BIND DNS to use TSIG example ........................................... 657
Configure alerts for other DNS types .............................................. 658
Modify additional SolarWinds components when using High Availability ......................................................... 659
Welcome to the SolarWinds Server & Application Monitor SAM Administrator Guide. This guide provides an overview of product features and related technologies. In addition, it contains recommendations on best practices, and troubleshooting information for common situations. To learn about planning, installing, and getting started with SAM, see the SAM Getting Started Guide.

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:

- Primary 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 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.

**Introduction to SolarWinds SAM**

SolarWinds Server & Application Monitor (SAM) gives you the tools to monitor your applications and environment through a single web console. SAM includes custom collections of templates, application monitors, and alerts to intelligently monitor application status and issues. Monitor over 200 application types including application servers, operating systems, authentication servers, database servers, and more.

SAM monitors applications in public, private, and hybrid environments using:

- **AppStack**: provides an interactive visual mapping within Orion with an in-depth perspective through the entire environment to help identify the root cause of performance and availability issues.
- **AppInsight**: monitors every aspect for Microsoft Exchange, IIS, and SQL servers in an environment, displaying metrics, status, and issues to manage and maintain applications and servers.
- **Cloud monitoring**: provides visibility into cloud environments through the Orion Web Console.
- **PerfStack**: troubleshoot issues in your environment from data collected by your SolarWinds Orion solution.

Integrated with the Orion Platform, leverage SAM monitored data and nodes with Orion features including automated application discovery, agent monitoring, High Availability (HA), web-based license management, and much more.

This guide provides Information about configuring and using SolarWinds SAM. For installation information, review the SAM 6.6 Recommended Requirements and the SAM Release Notes, and then use the SolarWinds Orion Installer. If you are new to SAM, see the SAM Getting Started Guide. The SolarWinds Customer Portal and the SolarWinds online IT community, THWACK, also contain product information.

**Applications defined and monitored in SAM**

In SolarWinds SAM, an application is a collection of component monitors inherited from a template. A component monitor queries for values returned by a process, counter, status, or script. SAM uses the data received to display vital statistics concerning the health of the system.

**Node**

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

A template is the blueprint for an application. It is a collection of component monitors designed to monitor a server or application. You can customize numerous templates using only the component monitors you need for a specific environment.

The type of information returned by the component monitor is based upon the type of monitor being utilized. For example, one type of monitor can report the up or down status of a service or process, another monitor can return the percentage of free space of a volume. Another type of component monitor can return up to ten values. Each monitor type, along with its parameters and returned values and/or states, is unique.

SolarWinds SAM provides the following types of templates:

- **AppInsight application templates** are preconfigured templates that provide detailed information. If you have business-critical Exchange, Microsoft IIS, or Microsoft SQL instances, use the AppInsight templates to monitor these applications. These templates have their own mechanism of discovering elements of an application dynamically. They also have special licensing.

- If you have other business-critical applications, apply one of the many preconfigured application templates that ship with SolarWinds SAM. SolarWinds recommends deploying a single template, making necessary edits to customize it to your environment, and then deploying the edited template on all similar applications. You can also obtain a template from the thwack community for an application not shipped with SAM.

- If you have a custom, homegrown application that you need to monitor, you can build a custom template.

For a list of out-of-the-box templates, see the [SAM Template Reference](#).

**Application**

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

**Component Monitor**

A component monitor is the fundamental element of an application. Component monitors return the current status or value of a monitored service or process. All component monitors return at least one value or one status condition.

For a full list of component monitors, see [SAM Component Monitor Types](#).
Every application template includes a number of component monitors per application or service to monitor. You can include multiple versions of component monitors for specific system monitoring or for customized scripts.
Each node, along with its applications and component monitors, can be viewed through the Orion Web Console as shown in the diagram below.

If you make a change at the template level, the applications based on that template are affected. If you make a change at the application level, only the individual application is affected. This inheritance relationship is beneficial if you need to make a lot of changes. For example, rather than making one change to 100 applications (and therefore 100 changes), you can change one item that affects all 100 applications based on that template.
The following illustration explains the template and application relationship.

How SAM works

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

1. **Orion Database**: Statistics are written to and requested from the Orion database by the Orion Server.
2. **Orion Server or Additional Poller**: Last poll time, statistics, and state, requested and returned for display.
3. **Network Engineer viewing Web Console**: SAM requests performance data based on defined monitors and targets respond.
4. **Monitored Nodes**:
Installed as a module in your family of SolarWinds products, SAM can be visualized with the following flowchart:

License Orion Platform products

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.
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.

SAM licensing model detailed

The SolarWinds SAM license you purchase is based on the number of allowed assigned component monitors. A component monitor provides a statistic that you want to monitor in SolarWinds SAM. You can have as many application templates and assigned monitors as needed, as long as the number of assigned component monitors does not exceed the license count.

If assigned component monitors exceed the license limit, monitors beyond the license limit are not activated and statuses change to Not Licensed. Either disable assigned component monitors to reduce your total assigned monitor count, or contact SolarWinds to upgrade your SolarWinds SAM license.

SAM has the following available license tiers:

<table>
<thead>
<tr>
<th>AVAILABLE LICENSE TIERS</th>
<th>NUMBER OF COMPONENTS TO MONITOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>AL150</td>
<td>150</td>
</tr>
<tr>
<td>AL300</td>
<td>300</td>
</tr>
<tr>
<td>AL700</td>
<td>700</td>
</tr>
<tr>
<td>AL1100</td>
<td>1100</td>
</tr>
<tr>
<td>ALX</td>
<td>Unlimited amount of items to monitor standard polling throughput.</td>
</tr>
</tbody>
</table>
License consumption

SolarWinds SAM licenses do not have to mirror the license count of other installed SolarWinds products. For example, you can install SolarWinds SAM with a 150-component license on a SolarWinds NPM server with an unlimited node license.

The number of component licenses are consumed by a specific amount by component and feature:

- **Asset Inventory data collection**: Asset Inventory data collection does not count against your SAM component monitor license.
- **Windows Scheduled Task Monitor**: The WSTM consumes five license units per node.
- **Agents**: Agent software is free. You remain bound by license limits regardless of whether you poll information via an agent or another protocol.
- **AppInsight for SQL**: 50 component monitors count against your licensed number of component monitors per SQL instance.
- **AppInsight for Exchange**: 50 component monitors count against your licensed number of component monitors, per Exchange Server.
- **AppInsight for IIS**: 30 component monitors count against your licensed number of component monitors per monitored IIS server.

To verify the number of consumed and available component monitors in your license, access the SAM License Summary.

1. Log in to the SolarWinds Web Console with an administrator account.
2. Click Applications.
3. Click SAM Settings.
4. Click SAM License Summary.

### SAM License Summary

<table>
<thead>
<tr>
<th>Allowance</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed number of component monitors</td>
<td>unlimited</td>
</tr>
<tr>
<td>Total number of component monitors</td>
<td>50</td>
</tr>
<tr>
<td>Licensed component monitors</td>
<td>50</td>
</tr>
<tr>
<td>Unlicensed component monitors</td>
<td>0</td>
</tr>
<tr>
<td>Available component monitors</td>
<td>unlimited</td>
</tr>
</tbody>
</table>
Alternatively, click License Details in the Settings page to view the used and available component monitors.

Verify the component monitors consumed per template

SolarWinds SAM licenses do not have to mirror the license count of any other installed SolarWinds products. For example, you can install SolarWinds SAM with a 150 component license on a SolarWinds NPM server with an unlimited node license.

**Example:** The Apache template has eight available licensed component monitors. If you have an AL150 license and assign all eight component monitors in this template to a node, the balance of remaining licenses is 142 (150-8 = 142). If only five of the eight component monitors are assigned to a node, the balance of remaining licenses is 145 (150-5=145).

To view the number of licensed component monitors per template in SAM, click Settings > All Settings > SAM Settings > Manage Templates. Review the Licensed Components column amount per template. Component monitors are consumed from the license only when the template is assigned to a node.
Manage and activate your SAM license

During installation, the web-based License manager will prompt you activate your SAM license; note these details:

- When using your Customer ID and password, use your individual profile information.
- If you do not know your Customer ID or password, enter a Support ticket.
- To get an activation key, navigate to the SolarWinds Customer Portal, click License Management, then click the plus sign [+].
- Your SAM license interacts additively with your other SolarWinds licenses. For example, if you have an NPM SL500 (500 nodes and 500 volumes) installed with SAM AL50, you can monitor a total of 550 nodes (500 NPM nodes + 50 SAM nodes), 550 interfaces, 550 volumes (matching the node count), and 50 application monitors.

The web-based License Manager replaces the stand-alone License Manager in Orion Platform products. If you upgraded from a previous version of SAM, 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 upgraded to the new web-based License Manager, SolarWinds recommends that you uninstall the standalone version.

To manage SAM and other licenses:

1. Click Settings > All Settings in the Orion Web Console.
2. Click License Details in the Details section.
3. Click License Manager.

You can sort licenses by product name, product version, license type, or expiration date. You can also add a license, upgrade a current license to a new tier, and activate licenses on new servers. The License Manager on the Main Polling Engine controls all licenses for your SAM environment, including scalability engines and High Availability.

💡 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.

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

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.
   a. Click Customer Portal, and log in using your Customer ID and password or your individual user account information.

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

![Note]
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. Log in to the Customer Portal, and click Licenses > Manage Licenses.
5. In the Customer Portal License Management, expand the product license to activate, and click Activate License Manually.
6. Paste the unique machine id from clipboard, and click Generate License File. Save the .lic file locally and transfer it to the offline computer.
7. 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

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 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 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.
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.
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.
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.
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

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.

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 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.
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

Yellow ⚠️

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

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.
Run SolarWinds SAM

SAM is part of the Orion Web Console, accessed through a web browser. You can access the page through a shortcut added to your programs. When opened, bookmark the page for ease of returning.

1. Launch the Orion Web Console using either of the following methods:
   - Start the 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.

After logging in, SolarWinds highly recommends setting up users to ensure your data and network remain in your control. SAM and all Orion products support different permissions for users, including administrator level for access to all key features and configurations.

Some features available in SAM and multi-module Orion products will require administrator access.

Uninstall SAM

Due to moving servers, installing a fresh copy, or other reasons, you may need to uninstall SAM from your environment. To remove SAM from a server, remove the product through the Windows Control Panel. Repeat these instructions on all servers including Additional Polling Engines, Additional Web Server, and HA pairs.

Uninstalling products may require uninstalling files and editing registries. For technical assistance, contact Support.

Prior to uninstalling, SolarWinds recommends the following preparation:

- **Backup the existing database**
  - To preserve your data, back up your database(s). If you need help with backups, check your vendor’s site for documentation and instructions.
  - If you have your database on a VM, create a snapshot or copy of your VM.
  - If you need software to perform backups and maintenance for Microsoft SQL databases, you can install SQL Management Studio Express for your specific version of Microsoft SQL on your database server.
Use one of the following links to download the installation:

- [SQL Management Studio Express 2008](#)
- [SQL Management Studio Express 2012](#)
- [SQL Management Studio Express 2014](#)

| Backup product folders | Create copies and backups of your product folders. You may have customizations in these folders specific to your installations. For example, you may have custom code or Report Writer reports to save. |

To remove SAM from a server, complete the following steps:

1. **Remove product licenses**
   1. In the Orion Web Console, select Settings > All Settings > and click License Manager.
   2. In the web-based License Manager, select the SAM license to remove.
   3. Click Deactivate. This removes the SAM license activation and server assignment.
      With the license deactivated, it is parked, or available but unused. Depending on the amount of products you need to uninstall, you may want to deactivate licenses for additional SolarWinds products: Additional Polling Engines, Additional Web Server, Scalability Engines, or High Availability.

2. **Uninstall SolarWinds products**
   1. Open Programs and Features in the Windows Control Panel.
   2. Select the product(s) to remove one at a time and click Uninstall.
      First, uninstall SolarWinds Server & Application Monitor.

   **Warning:** When you have multiple Orion Platform products installed and are not uninstalling all of them, continue with step 5 to restart the server. Deleting SolarWinds folders and registries affects the operation of all Orion Platform products.

   You may also need to uninstall the SolarWinds Job Engine and SolarWinds Orion Information Service.

3. **Delete or rename SolarWinds folders**
   Delete files from the following locations to fully clear all files. If you installed to a different domain, look on that location instead of C:\.

   - C:\Program Files (x86)\SolarWinds
   - C:\Program Files (x86)\Common Files\SolarWinds
   - C:\inetpub\SolarWinds
   - C:\ProgramData\SolarWinds
   - C:\ProgramData\SolarWindsAgentInstall
### 4. Remove specific Registry keys

**Important:** These steps affect your Registry settings. For assistance, [contact Support](#).

1. Open the command line interface on the server.
2. Type `regedit`, and click OK.
3. Expand `HKEY_LOCAL_MACHINE > Software`.
4. Delete both the SolarWinds and the SolarWinds.net folders.
5. If uninstalling from a 64-bit computer, expand `HKEY_LOCAL_MACHINE > Software > Wow6432Node`, and delete both the SolarWinds and the SolarWinds.net folders.

### 5. Restart and reinstall

Restart the server. To install SAM 6.5 or later, use the [SolarWinds Orion Installer](#). To install SAM 6.4 or earlier, see the [SAM Installation Guide](#).

For further information and assistance uninstalling your product, [contact Support](#).
Upgrade and migrate SAM

For upgrade information, use the SAM upgrade guide. For environments with multiple SolarWinds modules, use the Multiple Product Upgrade Guide. Learn how to upgrade like the geeks with preparation lists, gotchas and need to know information, changed requirements, instruction checklists, and troubleshooting.

The SolarWinds Migration Guide includes preparation, checklists, instructions, and troubleshooting for migrations.

- Migrating products to a new server with the same IP and hostname
- Migrating products to a new server with a new IP and hostname
- Migrating the Orion SQL database

Troubleshooting

If you experience issues and are not on the latest product versions, we recommend completing a full upgrade. Use the Product Upgrade Advisor to create the upgrade path. Many of these updates solve issues you may experience part way through your upgrade.

Check the SolarWinds Success Center for troubleshooting information. We recommend searching the name of the product, the version number, any error codes or messages displayed, and the general issue you found.

If an issue occurs you need additional help with, contact Support. We recommend gathering logs and diagnostics, a screenshot of the issue, and any error codes you receive. Attach and add this information to your ticket. You may also want to gather additional diagnostics on your additional pollers and web servers.

You can also visit the SolarWinds online IT community, THWACK, for product information.
Discover and add network devices

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 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><strong>IP Ranges</strong></td>
<td>Use this option when you want Orion to scan one or more IP ranges. If you have many IP ranges to scan, consider adding multiple discovery jobs rather than including all ranges in a single job.</td>
</tr>
<tr>
<td><strong>Subnets</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>IP Addresses</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Active Directory</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

![Network Sonar Wizard](image)
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.

   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](image)

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

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

![Network Sonar Wizard](image)
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.

SNMP credentials

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.

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

Add nodes 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**

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**

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.

![Select types of volumes]

- **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.

![Select applications]

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.

**Add discovered devices to SolarWinds**

After the Network Sonar Wizard discovers your network, the Network Sonar Results Wizard opens, allowing you to import network elements into. 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**

<table>
<thead>
<tr>
<th>Device Types to Import</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the device types to monitor.</td>
</tr>
<tr>
<td>Count</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>1</td>
</tr>
</tbody>
</table>

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

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

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.

**Network Sonar Results Wizard**

**Volume Types to Import**
Select the volume types to monitor.

<table>
<thead>
<tr>
<th>Count</th>
<th>Volume Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>RAM</td>
</tr>
<tr>
<td>✔</td>
<td>Virtual Memory</td>
</tr>
<tr>
<td>✔</td>
<td>Other</td>
</tr>
<tr>
<td>✔</td>
<td>Fixed Disk</td>
</tr>
<tr>
<td>✔</td>
<td>RAM Disk</td>
</tr>
</tbody>
</table>

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

**Network Sonar Results Wizard**

**Import Preview - LABORION03**
Select devices, interfaces, and volumes that you wish to ignore or import. All ignored items will be removed from future network discovery, manual or scheduled. If you wish to ignore items, do so before importing.

<table>
<thead>
<tr>
<th>Polling IP Address</th>
<th>Name</th>
<th>Machine Type</th>
<th>Volumes</th>
<th>Polling Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔ 10.196.100.250</td>
<td>HQDC-3750-CORE.demo.lab</td>
<td>Catalyst 37xx Stack</td>
<td></td>
<td>SNMP</td>
</tr>
<tr>
<td>✔ 10.196.200.250</td>
<td>BROF-3750-CORE.demo.lab</td>
<td>Catalyst 37xx Stack</td>
<td></td>
<td>SNMP</td>
</tr>
<tr>
<td>✔ 10.196.202.1</td>
<td>BROF-2821-WAN.demo.lab</td>
<td>Cisco 2821</td>
<td></td>
<td>SNMP</td>
</tr>
<tr>
<td>✔ 10.196.204.11</td>
<td>BOHYV01</td>
<td>Hyper-V Server</td>
<td>RAM, Virtual Memory, Fixed Disk</td>
<td>SNMP</td>
</tr>
<tr>
<td>✔ 10.196.204.12</td>
<td>BOESX01.demo.lab</td>
<td>VMware ESX Server</td>
<td>RAM Disk (4), Fixed Disk</td>
<td>SNMP</td>
</tr>
</tbody>
</table>

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

## Add a single node for monitoring

To add a single node for monitoring:

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

- **Polling Method:**
  - **External Node: No Status**
  - **Status Only: ICMP**
  - **Most Devices: SNMP and ICMP**
  - **Windows Servers: WMI and ICMP**

- **Choose credential:**
  - Credential name:
  - User name:
  - Password:
  - Confirm password:
  - Test

- **Windows Servers: Agent**
  - Optional agent useful for monitoring Windows hosts in remote or distributed environments, such as the old agent?
4. Select the statistics and resources to monitor on the node, and click Next.

5. 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 Configuration]

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

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

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

   ![Alerting Thresholds]

6. Click OK, Add Node.

   The node will be monitored according to the options you set.
Choose the polling method to use

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

External Node (No Status)

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

Status Only: ICMP

Limited information is gathered using Internet Control Message Protocol (ICMP) or ping. This polling method is used to monitor status and measure the average response time and packet loss percentage for managed devices.

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

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

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

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

Windows Servers: WMI and ICMP

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

When used as an alternative to SNMP, WMI can provide much of the same monitoring and management data currently available with SNMP-based polling with the addition of Windows specific communications and security features.
Your devices must have WMI and 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 Servers: Agent

An agent is software that provides a communication channel between the Orion server and a Windows or Linux-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.

Import nodes from a list of IP addresses

Import devices from a seed file in the Network Sonar Discovery wizard.

Enter one IP address or host name per line.

1. Open the seed file.
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 seed file into the field.
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

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 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.

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.

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>
</table>
**Node Data in Tooltips**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</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.

   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 Manager and you want to poll for UCS data, select Poll for UCS, provide the Port on which the UCS manager listens and credentials.
  - Click Test to verify that the credentials are valid for the selected UCS Manager.

- 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.

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. If you want 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.

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.
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.

Promote a Node to WMI Monitoring

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

   1. On the web console, navigate to Settings > Manage Nodes.
   2. Check the node you want to promote, click Edit Properties, and then select Windows Servers: WMI and ICMP.
   3. Enter the appropriate WMI credentials.
   4. Click Test to confirm your settings. When done, click Submit, then click OK.

Change polling engine node assignments

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 server
- 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. Locate the node using either of the following methods:
      - Use the search tool above the node list to search your SolarWinds Orion database for the device you want to manage.
      - Select a Group by criteria, and expand the group including the node to manage.
   4. Select the node for which you want to change the polling engine.
5. 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.

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

The node will now be polled 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. Locate the node to view:
   - Use the search tool above the node list.
   - Select a Group By option.
   - Expand the group to display more options.
3. Select a node
4. Click List Resources on the Node Management toolbar to display instances and volumes, along with monitoring status.

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 Administrator and Node Management rights.

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.
- **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.

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.
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.](image)

5. To add or remove the group members, click Add & Remove Objects.
   
   ![You can also change group members directly on the Manage Groups page.](image)

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.](image)

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><strong>Object States</strong></th>
<th><strong>Group Status</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Up, Warning, Down" /></td>
<td><img src="image" alt="Up" /></td>
</tr>
</tbody>
</table>

page 86
The Show Worst Status selection ensures that the worst status in a group of objects is displayed for the whole group.

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.

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, when a parent object, such as a switch, goes down or becomes unresponsive all interfaces on the switch will also be unresponsive, even though they may be working.

To account for this situation, the Unreachable status is used for the interfaces, because their parent node reports as down, and their own status cannot be determined.
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.

![Manage Dependencies](image)

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

![Show only](image)

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

![Dependency name](image)

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.

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.

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.
Discover applications in your environment

SolarWinds SAM can scan nodes and automatically assign the Application Monitors suitable for each scanned node. You control the nodes to be scanned, the application templates used in the scan, and the scanning parameters that determine a match.

In larger environments, adding many applications at once can take a great deal of time. You may need to log in with an administrator account to perform this action.

- **Application Discovery** - Discover and add applications through discovery. Set up application monitoring with application monitors and templates.
- **Add application monitors to nodes** - Learn how to add application monitors to currently monitored nodes.
- **Customize the application details view** - Learn how to customize the application and template views.
- **Customize SAM Application Summary views** - Modify resources displayed in the Application Summary page.
- **Add SolarWinds SAM data to the Node Details view** - Modify Node Details to display SAM resources.
- **Viewing node and application data in tooltips** - You can view node and application data directly through hover-over tooltips.

**Application Discovery**

SolarWinds SAM can scan nodes and automatically assign the Application Monitors it deems suitable for each scanned node. You control the nodes to be scanned, the application templates used in the scan, and the scanning parameters that determine a match.

In larger environments, adding many applications at once can take a great deal of time. You may need to log in with an administrator account to perform this action.

1. On the Web Console, click Settings > All Settings > Discovery Central > Discover Applications. To use the wizard, click Discover Applications. You can also access this through the Settings > All Settings > SAM Settings > Scan Nodes for Applications.
2. Click [+*] to expand the node groups, and then select the nodes you want to scan, then click Next.
3. Select the applications to locate in the scan. You can use the Show only drop-down list to filter the application template list. As you select templates across the filter groups, they display in the selected applications section. To adjust the template assignment criteria, expand Advanced Scan Settings and move the slider to the desired setting:
   - Minimal Match - At least one component must match to assign the template.
   - Partial Match - Some of the components must match to assign the template.
   - Strong Match - Most of the components must match to assign the template.
   - Exact Match - All of the components must match to assign the template.
4. When you are finished selecting applications, click Next.
5. Some application templates require credentials either to access restricted resources, or to run within the context of a specific user. To scan for these templates, add the necessary credentials to the list. If a template you are scanning for requires credentials, the credentials in this list are tried in the order in which they appear.
6. If you have domains sharing user names with different passwords, SolarWinds recommends that you run separate application discoveries for each domain. When you are finished entering credentials, click Next.
   
   Warning: Credentials are tried several times over the course of a scan, so an incorrect password is likely to lock out an account. To avoid potential account lockouts that affect actual users, SolarWinds recommends that you create and use service accounts. A service account is an account created specifically for the purpose of providing credentials to use for SolarWinds monitoring. With service accounts, no actual user is affected by an account lockout if a password should be entered incorrectly.
7. Review the summary for the scan. If the automatic discovery matches templates that are already assigned to the node, by default the template is not assigned a second time. If you want to assign duplicate templates, select Yes, Assign Anyway from the Do you want to assign duplicates list.
8. Click Start Scan to begin the scan, running in the background. A banner message appears near the top of the screen, SAM scan in progress. To view the progress of the scan, click More Details in the banner message. From this screen you can see the progress of the scan, cancel the scan, or go to the Application Summary screen.

You are notified by a message near the top of the screen when scanning is complete. Click More Details to see the results of the scan. Click Application Summary to display the summary page.
Add application monitors to nodes

After adding individual nodes, you are prompted to add applications for monitoring the desired application(s) on the new node.

1. Add a node from the web console by clicking Settings > All Settings > Add a Node.
2. On the Add Application Monitors step, use the Show Only drop-down to select a category of Application Monitors. A list of monitors displays. For a list of monitors, see Component Monitor Types.

3. Select the Application Monitor(s) you want to assign.
4. Select or enter the appropriate credentials, and then click Next.
5. On the Change Properties page, modify any of the information as needed, such as the Node Status Polling interval (in seconds) and the Collect Statistics Every frequency (in minutes).
6. Click OK and complete adding the node.

You can modify the assigned application monitors for the node at any time.
**Customize the application details view**

Applications inherit the custom view setting from their templates in the same way as other template settings. You can customize the templates through overrides or creating a copy of the template and editing that content.

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

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Application Monitors.
2. Find an assigned Application Monitor without a Custom View.
3. Return to Applications > SAM Summary then click the Application Monitor to view its application details page.
4. Click Customize Page, then proceed with your customizations.

**Custom application details view**

You can select and create a custom application details view. This custom view is applied at the template level. Applications inherit the custom view setting from their templates in the same way as other template settings.

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

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Application Monitors.
2. Select an Application Monitor and then click Edit Properties.
3. Click Modify Template Settings in the field Custom Application Details View.
4. Select Yes, use <TemplateName> Details View in the field Custom Application Details View.
5. Click Submit, then click the name of the assigned Application Monitor to view its application details page.
6. Click Customize Page and proceed with your customizations.

After creating a customized application details view for a template, you can change the Custom Application Details View setting in the template properties to switch between the default view and the custom view.

**Select a view for a template**

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

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Select a template and then click Edit.
3. If you want applications based on this template to use the default view, set Custom Application Details View to No, use Default Application Details View.
4. If you want applications based on this template to use the custom view, set Custom Application Details View Yes, use <TemplateName> Details View, where TemplateName is the name of the selected template.

5. Click Submit.

**Select a view for an application**

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

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Application Monitors.
2. Select an Application Monitor and then click Edit Properties.
3. Click Modify Template Settings in the field Custom Application Details View.
4. If you want this application to use the default view, set Custom Application Details View to No, use Default Application Details View.
5. If you want this application to use the custom view, set Custom Application Details View to Yes, use <TemplateName> Details View, where <TemplateName> is the name of the selected template.
6. Click Submit.
Customize SAM Application Summary views

You can edit the current SAM Application Summary, or create a copy to refine with filters and resources for your own summary. The SAM Application Summary page is called Application Summary in the Manage Views list.

You can create a copy of the Applications Summary view simply by selecting and copying through the Manage Views page.

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

1. On the Web Console, click Settings > All Settings > Manage Views, locate and select Application Summary, and click Copy.
2. Select the Copy of the Application Summary and click Edit.
3. You can change the name of the view, add and remove resources, modify column layouts, and more.
4. Click [+ ] in a column you want to display SAM resources. The Add Resource page opens to select one or more resources to add. To list SAM specific resources, you can Group By Classic Category and select Sam Application Summary Resources. These options include resources like All Applications Tree, Top XX Monitored Processes, AppStack Environment, ApplnSight resources, and many other application/component monitors.

![Add Resource](image)

5. A NOC mode view is also available to enable. You can also create and modify NOC views for cycling through network monitoring resources.

6. You can add Limitations for access and content through the View Limitations section.

7. When done, click Preview to verify the data and layout. If satisfied, click Done to save.

For details on how to modify and enhance the view, see Create, delete, modify, or restrict views.
Create, delete, modify, or restrict views

Orion Web Console views are configurable presentations of network information that can include maps, charts, summary lists, reports, events, and links to other resources. Edit views directly or through the Manage Views page.

Customized views can be assigned to menu bars. With NOC View Mode enabled, views may be optimized for display in Network Operations Centers.

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

Add resources and columns to views, and define subviews

Administrators can edit views directly on the page by clicking the pencil icon or through the Customize Views page.

1. Click Settings > All Settings in the menu bar.
2. In the Views grouping, click Manage Views.
3. Select the view, and click Edit.

Add widgets to the view from the Customize Page

Widgets are a new way to refer to resources in your SolarWinds installation.

1. Go to the view you created.
2. Click the pencil icon on the upper left.
3. Click the Add Widgets button in the upper right.
4. Search for widgets, or resources, and drag and drop widgets directly on the page where you want them to be, including in new columns.
   - You can limit offered resources by criteria in the Group by list, or search for a resource or widget in the Search box.
5. When complete, click Done adding widgets, and then Done editing.

The view is populated with the widgets you selected.
Add resources to the view from the Customize Views page

1. On the Customize page, click + next to the column that you want to add the resources, also known as widgets.

To open the Customize view page, click Settings > All Settings > Manage Views. Select the view, and click Edit.

2. Select resources in the middle pane, and click Add Selected Resources.

You can limit offered resources by criteria in the Group by list, or search for a resource, or widget, in the Search box.
3. Use the arrow icons next to the columns to move resources between columns.

4. Click Done.

The view is now populated with the widgets you selected.

- Resources already in your view are not marked in the list. You can add a resource on a view more than once.
- Some resources may require additional configuration.
- Several options on the Add Resources page are added to the list of resources for a page, but the actual configuration of a given map, link, or code is not added until the page is previewed.

Divide content into subviews from the Customize Page

1. Hover over the side menu and click Add tab.
2. Type a name for the new tab, and click Update.
3. Select an icon.
4. Click Done.
5. Add resources by opening the Customize Page.
Divide content into subviews from the Customize Views page

1. On the view, click the Customize Page icon.
2. Click Add tab.

```
<table>
<thead>
<tr>
<th>Customize Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAGE SETTINGS</td>
</tr>
<tr>
<td>+ Add tab</td>
</tr>
</tbody>
</table>
```

3. Enter the tab name, and click Update.
4. Select an icon, add resources, and click Done.

To drag and drop widgets, click Preview, and then add the widgets.

You can access the subview with the resources from the view menu.
Add subviews using Enable Navigation

1. On the Customize view, select Enable Left Navigation.

To open the Customize view page, click Settings > All Settings > Manage Views. Select the view, and click Edit. You can also click Customize Page > Page Settings on the view.

2. Click Add Tab.
3. Type a name for the new tab, and click Update.
4. Select an icon, and add resources.
5. Click Done.

You can access the subview with the resources from the view menu.

When you are done with your changes, click Preview, and then click Submit.

Optimize 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 resources.

Enable NOC Views

You can configure any Orion Web Console view to appear in the NOC view form.
1. Log in to the Orion Web Console as an administrator.
2. Open a view, and click Customize Page in the top right 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.
   You have created a NOC version of your view with a compressed header and footer, and without the left navigation area.

Customize NOC Views

To add resources, remove resources, or add subviews on a NOC view, click the top-right icon, and select Customize Page.

Exit NOC Views

Click the NOC Settings icon, and select Exit NOC Mode.

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

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.

Display subviews

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

To display a subview, click the circle.

Move resources in NOC Views

If you want to move resources within a NOC view, you turn on the drag&drop mode.
1. Click the Settings icon in the top right corner of the NOC view, and select Pause Rotation.
2. Drag and drop resources within the selected pane.
3. When you have finished repositioning the resources, click the Settings icon again, and select Resume Rotation.

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.
**Viewing node and application data in tooltips**

You can hover over objects such as nodes and groups to view additional information. These tooltips also include SAM specific data, providing at-a-glance updates and data for quick responses. You can click the objects to access details pages for deeper data or to manage alerts and use management options.

### Node tooltips

<table>
<thead>
<tr>
<th>TOOLTIP DATA</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Status</td>
<td>Current status of the node: up, down, warning, unplugged, or unmanaged</td>
</tr>
<tr>
<td><strong>i</strong> SolarWinds SAM now supports the ability to include applications in calculation of node child status. So if node is up, but application on that device is down, you will see a child status icon indicating there is a problem.</td>
<td></td>
</tr>
<tr>
<td>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>
<tr>
<td># of Running VMS</td>
<td>Number of running VMS and total VMS</td>
</tr>
<tr>
<td>ESX Host Status</td>
<td>Status of the ESX Host</td>
</tr>
</tbody>
</table>
### Application tooltips

<table>
<thead>
<tr>
<th>TOOLTip DATA</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Name</td>
<td>The name of the application</td>
</tr>
<tr>
<td>App Status</td>
<td>The status of the application: up, down, unknown, warning, or critical</td>
</tr>
<tr>
<td>Server Status</td>
<td>Operational status of the server: up, down, warning, unplugged, or unmanaged</td>
</tr>
<tr>
<td>Components with Problems</td>
<td>List of the components with problems and their statuses</td>
</tr>
</tbody>
</table>
Add SolarWinds SAM data to the Node Details view

To view SAM data including application and component monitor information, you may need to edit the Node Details - Summary view. You can modify the content of the view through the layout and resources included. For more details on modifying a view, see Add resources and columns to views, and define subviews.

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

1. On the web console, click Settings > All Settings > Manage Views. Select the Node Detail summary and click Edit.

2. Click [+] in a column you want to display SAM resources. The Add Resource page opens to select one or more resources to add. To list SAM specific resources, you can Group By Classic Category and select Sam Application Summary Resources. These options include resources like All Applications Tree, Top XX Monitored Processes, AppStack Environment, ApplInsight resources, and many other application/component monitors.

3. Click Add Selected Resources to save all selections to the column.
You can move these resources to other columns or click [+ ] to add resources to those columns.

4. Click Done to update the view.

To check the view, navigate to a node you edited to see the added resources and layout. You can edit the view again to further modify the content.

**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.

**View network events in the Web Console**

All events that occur to monitored devices on your network are automatically logged and displayed in the Orion Web Console. You can view and remove them as your network management policies require.

**Filter events**

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.
Clear or remove events

Clearing an event removes the event from the Events view.

![Info icon with text: 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.

View notifications

Click the bell icon in the top-right corner to display unread notifications.

![Notification screen with four notifications: 20 new blog post(s), Evaluation is ending! Purchase licenses to continue using key functionality, Configure your default send email action, Discovery import completed successfully.]

Notifications include the following messages:

- If you configured the Orion Web Console to check for product updates, an announcement displays when an update, such as any upgrade, service pack, or hotfix becomes available.
- If you configured the Orion Web Console to store blog posts, new and unread posts to the Orion Product Team Blog are announced in the notification bar.
- If you configured a scheduled discovery, results display in the notification bar when the discovery completes.
- If you are monitoring any VMware ESX or ESXi Servers, the notification bar displays the number of ESX nodes found during any discovery, and inform you if any discovered ESX nodes require credentials.
- If you are monitoring Hyper-V nodes, the notification bar informs you when Hyper-V servers were found during a discovery.
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
- VIM 7.1 or later (VMAN integrated with the Orion Platform)
- NTA 4.2.2 or later
- SRM 6.4 or later
- WPM 2.2.1 or later
- EOC 2.0 or later
- NCM 7.7 or later (Configuration changes)
- VNQM 4.4.1 or later (IPSLA operations)
- DPAIM 11.1 or later (DPA integrated with the Orion Platform)

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

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

- NetPath™

For a more complete list, see SolarWinds KB MT85165.

Create analysis projects

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

- Metrics marked with a rocket ship can collect real-time metrics.
- 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.
   
   ![Entity in metric palette]

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

Open an analysis project directly from the manage resource on your details page. This opens a project with relevant metrics from the entity already charted. For example, key metrics for node entities include:

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

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

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

![Management section]

You can add more metrics or metrics from related entities.

This is supported for nodes, interfaces, IPSLA operations, clusters, datastores, hosts, VMs, LUNs, SRM pools, storage arrays, volumes, cloud instances, and SAM applications.
Update charts in real-time (Real-Time Polling)

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

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

Click Start Real-Time Polling in the toolbar.

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

View the polled data for a plotted metric

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

Click and drag a selection on a chart, and click on the icon with the magnifying glass.
The Data Explorer tab opens with the data that for the chart within the time frame you select. Use the Filters menu or the search bar to further reduce the visible data.

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.

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.
Monitor with Orion agents in SAM

When using the Orion agent, SAM collects all data from application monitors for that server. SAM can deploy and consume collected data using Orion agents for Windows and Linux. For full details on Orion agents, see:

- Poll devices with SolarWinds Orion agents
- Modify global agent deployment and update settings
- Agent communication modes
- Configure SNMP for agents
- Credentials and privileges used on Linux-based computers
- Certificates and the agent
- Deploy agents to nodes
- View agent connections and status, update agents, or manage agents
- Migrate agents from one Orion instance to another

Overriding agent and agentless monitoring

You can override data collection behavior in specific instances per application monitor or template. You can configure an application or template to collect data through a preferred polling method as agent or agentless. For example, for the User Experience Monitor template you may not want to measure response time locally from the server where the application is installed. If this is the case, you can switch the application to poll without using an agent.

![Advanced settings for polling method](image)

Communication type

Agent Communication can be deployed as either Active or Passive:

- Agent initiated Communication (Active): The Agent initiates communication with the server on the default port of 17778 (this can be changed if needed). This port must be opened on the server firewall so the Agent can connect. No change to the Agent firewall is required.

For more information, see:
Orion Server initiated Communication (Passive): The Agent waits for requests from the server on the default port of 17790 (this can be changed if needed). This port must be opened on the Agent computer’s firewall so the server can connect. No change to the server firewall is required.

Templates and component monitors

Application templates provide collections of application monitors with configurable settings to collect and monitor data for Orion managed nodes. These templates include a variety of options based on operating systems, applications, and services.

For details, prerequisites, and configuration requirements for application templates and monitors, see SAM Component Monitor Types and SAM Template Reference. To use component monitors in Linux environments with the Orion agent for Linux, you need complete additional configurations. This information is added to the component monitors and available in this section.

The following component monitors supported for Orion Agent for Windows:

- Process Monitor - Windows
- DNS Monitor - TCP
- DNS Monitor - UDP
- Exchange Web Services User Experience Monitor
- HTTP Monitor
- Performance Counter Monitor
- SMTP Monitor
- TCP Port Monitor
- ODBC User Experience Monitor
- Oracle User Experience Monitor
- Windows Event Log Monitor
- Windows PowerShell Monitor
- Windows Service Monitor
- WMI Monitor

The following component monitors are supported for Orion Agent for Linux:

- Directory Size Monitor
- File Age Monitor
- File Change Monitor
- File Count Monitor
- File Existence Monitor
- File Size Monitor
- HTTP User Experience Monitor
- HTTPS User Experience Monitor
• JMX Monitor
• Linux/Unix Script Monitor
• Nagios Script Monitor
• ODBC User Experience Monitor
• Process Monitor
• Oracle User Experience Monitor
• SNMP Monitor
• TCP Port Monitor
• TomCat Server Monitor

The following component monitors are supported for Orion Agent for AIX:

• Directory Size Monitor
• File Age Monitor
• File Change Monitor
• File Count Monitor
• File Existence Monitor
• File Size Monitor
• HTTP User Experience Monitor
• HTTPS User Experience Monitor
• JMX Monitor
• Linux/Unix Script Monitor
• Nagios Script Monitor
• ODBC User Experience Monitor
• Process Monitor
• SNMP Monitor

ℹ️ SNMPv3 with encrypted mode is not supported.
ℹ️ To poll SNMP details correctly, you need to manually enable the SNMP daemon.

• TCP Port Monitor
• TomCat Server Monitor

Reports

The following reports are installed for use with the Orion Agent:

• Agent Inventory
• Agent Plugin Version
Poll devices with SolarWinds Orion agents

An agent is software that provides a communication channel between the Orion server and a Windows or Linux computer. Products install plugins on agents to collect the data that the agents send back. 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 2048-bit TLS encryption. The agent protocol supports NAT traversal and passing through proxy servers that require authentication.

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 2016</td>
<td>AIX 7.1</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008</td>
<td>AIX 7.2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2</td>
<td>Amazon AMI, 64-bit only</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2 SP1</td>
<td>CentOS 5</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012</td>
<td>CentOS 6</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2</td>
<td>CentOS 7</td>
</tr>
<tr>
<td></td>
<td>Windows 7</td>
<td>Red Hat Enterprise Linux 5</td>
</tr>
<tr>
<td></td>
<td>Windows 7 SP1</td>
<td>Red Hat Enterprise Linux 6</td>
</tr>
<tr>
<td></td>
<td>Windows 8</td>
<td>Red Hat Enterprise Linux 7</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td><strong>Windows</strong></td>
<td><strong>Linux/Unix</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
|  | · Windows 8.1  
· Windows 10 | · Raspbian 8.0 on ARMv6 or ARMv7 processors, 32-bit only  
· SUSE Linux Enterprise Server 10  
· SUSE Linux Enterprise Server 11  
· SUSE Linux Enterprise Server 12  
· Ubuntu 14  
· Ubuntu 15  
· Ubuntu 16 |
| Hard drive space | Approximately 100 MB of hard drive space on the target computer. |  |
| Other software | 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 4.0 (You must install this manually if you are installing an agent on Windows Server 2008 R2 or earlier or Windows Core)  
· .NET Framework 4.5 (Required for Windows Server 2008 R2 SP1 and later) | For Linux, you may need to install the following manually:  
· Python 2, versions 2.4.3 and later  
  
  **Python 3 is not supported**  
· The bash shell  
For AIX:  
· You don't need to install Python manually. Required packages are distributed and deployed automatically with the agent plug-ins.  
· 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](#).  
After the agent is installed, it runs as a Local System account and does not require administrative permissions to function. |  |
| Latency | Agents can tolerate up to 500 ms of latency between the remote computer and the Orion server. |  |
Account Privileges

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

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.

Agent port requirements

<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>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</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>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>
<tr>
<td>17791</td>
<td>TCP</td>
<td>SolarWinds Agent</td>
<td>Outbound</td>
<td>Agent-initiated</td>
<td>Windows 2008 R2</td>
<td>Used continuously by the agent to communicate back to the Orion server. Also used to deploy the agent.</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>17778</td>
<td>TCP</td>
<td>Orion Module Engine SolarWinds Agent</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>17790</td>
<td>TCP</td>
<td>Orion Module Engine SolarWinds Agent</td>
<td>Outbound</td>
<td>Server-initiated</td>
<td>All</td>
<td>Used to communicate with the Orion server.</td>
</tr>
<tr>
<td>17791</td>
<td>TCP</td>
<td>Orion Module Engine SolarWinds Agent</td>
<td>Inbound</td>
<td>Agent-initiated</td>
<td>Windows 2008 R2</td>
<td>Used continuously by the agent to communicate back to the Orion server. Also used to deploy the agent.</td>
</tr>
</tbody>
</table>
Agent resource consumption

<table>
<thead>
<tr>
<th>RESOURCE</th>
<th>CONSUMPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Less than 1% on average under normal operating conditions (0.24% on average)</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</td>
</tr>
<tr>
<td></td>
<td>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.

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 a 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.

**Configure SNMP for agents**

SNMP is a polling method used by Orion agents and as default to collect for monitors and resources. Review this information to locate and resolve any issues when troubleshooting connectivity, access, and data polled in SAM.

The following components and resources depend on SNMP connections:

- Location, Contact, and SysObjectID of the Node Details resource
- SAM SNMP component monitor
- Hardware Health data and resources
- Asset Inventory page and resources

⚠️ Hardware Health and Asset Inventory are not supported on AIX devices.
Configure SNMP

To configure SNMP, you need to install the SNMP daemon if missing. The Orion agent configures SNMP for you during deployment. You can manually configure SNMP. If settings need to be modified for Orion agent, the configurations are verified and updated during agent deployment.

On AIX computers, the auto-configuration is not supported. Make sure that SNMP daemon is running.

If you need to install the SNMP daemon, you can install the daemon using a command according to your Linux/Unix distribution. Deploying the agent automatically configures SNMP. If the SNMP daemon is not installed, SNMP cannot be configured.

To install SNMP daemon on Linux:

- **Install on Ubuntu:** `sudo apt-get -y install snmpd`
- **Install on Red Hat / CentOS:** `yum -y install net-snmp`
- **Install on SUSE:** `zypper -y install net-snmp`

Auto-configuration of SNMP on Linux executes on the following actions:

- The first step during a Discovery
- Anytime you initiate a List resource on any node managed by the Orion agent for Linux

SAM completes the following changes during auto-configuration:

- Checks the snmpd service is configured to start automatically after system reboots.
- Checks the snmpd.conf file for the configuration of an agent owned community string. If the string is missing, SAM adds the community string. The string is "agent owned" = with an SNMP v2 community string in form of an agent guid (randomly generated value that is unique for each agent).
  
  For example:

  ```
  ### BEGIN SolarWinds Agent SNMP auto config
  rocommunity 36343901-D61F-4C72-B860-A8E18DD892E4 localhost
  ### END SolarWinds Agent SNMP auto config
  ```

  If SAM adds the community string, SNMP is restarted.

Configure SNMP v3

If you have SNMP v3 configurations detecting users through the configuration file without an SNMP v2 community string, SAM will not modify the configuration file. SNMP v3 will not be auto-configured on deployment. You can provide SNMP credentials manually at the node level to configure access.
Prerequisites

To add SNMP credentials, you can enter the credentials through the Add Node Wizard or edit an existing node. You cannot test the credentials until the agent is deployed.

For encryption, you also need to install a common python extension `pycrypto` on the target machine to make polling possible. To install:

```
PyCrypto installation on ubuntu
apt-get install python-pip
pip install pycrypto
```

Test Credentials

You can test any manually entered credentials by editing the Node. To test, you need a properly connected agent deployed to the target node. Review the credentials and click Test.
Enable SNMP daemon on AIX computers

SNMP Monitor on AIX devices requires that the SNMP daemon be enabled.

Without enabling the SNMP daemon, the following information will not be available in the Node Details widget:

- Location
- Contact
- SysobjectID
To enable the SNMP daemon, add the following lines to the configuration file in /etc/snmpdv3.conf which configures snmpv1, v2c, and v3 access.

Use the following configuration example as a reference:

```plaintext
# 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
```
Test the SNMP configuration

- To test the configuration for v1 requests, use `snmpdinfo`.
- To test v2c and v3 requests, use `clsnmp` for v2c and v3 requests and configure `/etc/clsnmp.conf`.

```
v2cstring localhost snmpv2c
v3user_noauth localhost snmpv3 user1 - - - - - -
```

This configuration matches the examples above.

**Credentials and privileges used on Linux-based computers**

Agents installed on Linux-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-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-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 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.

When this is selected, we connect to the Linux-based computer using the provided SSH credentials and then switch users to the account with elevate privileges to install and configure the agent.

Verify your privileges by opening an SSH connection to the remote computer, switching to the elevated credentials, and entering `sudo -i`.

SNMP credentials

Select Include SNMP Credentials in order 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.

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.

Certificates and the agent

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

For more information, search for "Add the Certificates Snap-in to an MMC" at [technet.microsoft.com](http://technet.microsoft.com).
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.

- Agents do not work with AppInsight for SQL in a clustered environment.
- 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-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-based computers through a repository
- Deploy with a Gold Master Image
- Deploy 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 & Linux Servers: Agent as the Polling Method.
6. Select the operating system type of the remote computer.

![Windows & Linux Servers: Agent](image)

7. Choose a credential from the list, or enter new credentials, and then click Next.

   - These credentials are only used to connect to the remote computer and install the agent software. After the agent is deployed, the credentials may change with no impact to the deployed agent.
   - The credentials must have administrator or root-level privileges. On Linux-based devices you can connect with one credential set and then use another credential to use `su` or `sudo` for package installation. Most Linux distributions require the user’s password when using `sudo`. Other distributions, such as SUSE, may require the root password. Depending on your Linux distribution, enter the required credential for the Include Credentials with Elevated Privileges to install the package.
   - For Linux-based nodes, you can choose to add SNMP credentials to collect SNMP data for Asset Inventory and Hardware Health from the remote node.

8. Click Start Install on the Install Agent Software window.
9. Choose the resources to monitor on the agent, and click Next.
10. Add application monitors on the agent, and click Next.
11. Change properties or keep the defaults, and click OK, Add Node.

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

**Deploy agents to monitored nodes**

![Warning](image)

The Orion server must be able to communicate with the remote nodes. To monitor Linux-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-based computers 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.
   - You can assign credentials to multiple locations or nodes by selecting multiple entries.
8. Click Deploy Agent.

When 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 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 is successful, the agent is listed on the Manage Agents page.

**Deploy an agent manually to a Linux-based computer**

Use this method to install agents if you cannot use push deployment to Linux-based devices over SSH. For example, when the device is behind a NAT or is hosted in the cloud. This approach uses `wget` or `curl` to download the installation files from your chosen polling engine. This agent installation method is known as a pull deployment.

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings > Download Agent Software.
3. Click 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 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 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 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 computer manually and then install it instead of using `wget` or `curl`.

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 computer and extract it.
4. Follow the instructions in the `readme.txt` file.

Select your distribution

Agents are supported on the following Linux operating systems.

- AIX 7.1
- AIX 7.2
- Amazon AMI, 64-bit only
- CentOS 5
- CentOS 6
- CentOS 7
- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- Raspbian 8.0 on ARMv6 or ARMv7 processors, 32-bit only
- SUSE Linux Enterprise Server 10
- SUSE Linux Enterprise Server 11
- SUSE Linux Enterprise Server 12
- Ubuntu 14
- Ubuntu 15
- Ubuntu 16

If your operating system is not listed, select the closest match to your Linux 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.

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.
     a. To use an existing polling engine, select Use Connection Details from Polling Engine, and then select a polling engine from the list.
     b. To manually enter the polling engine IP address, select Enter Connection Details Manually, and then enter the host name and IP address. The IP address is required. Use the host name and IP address of the polling engine that you can access from the client.
   - 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.

₁ 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 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-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-based computers. The Orion server and Additional Web Servers are Linux repositories for the agent. This method allows you to use automation tools to mass deploy agents on your Linux-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 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 in a terminal open to the Linux-based computer.
7. You may be prompted for the root password to add the repository.
8. After the repository is registered with the computer, copy and run the install command. The agent software is downloaded from the repository and installed on the computer.
9. In the terminal, type service swiagentd 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 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. You must add the location of the repository to every Linux-based computer that you want to install the agent software from the repository. 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.

! Important: 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.
     a. To use an existing polling engine, select Use Connection Details from Polling Engine, and then select a polling engine from the list.
     b. To manually enter the polling engine IP address, select Enter Connection Details Manually, and then enter the host name and IP address. The IP address is required. Use the host name and IP address of the polling engine that you can access from the client.
   - 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 double-click setup.bat.
8. Follow the instructions in the Installation wizard.
When 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, take the following steps 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, and the port number for the agent. The default port is 17790.
6. Click Submit.

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

Deploy on Windows Core Servers

If you are installing the agent on a Windows Core Server, you must install .NET Framework 4.5 and 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.

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 to the host server and operate normally.

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. Also open port 17791 if the device is running Windows 2008 R2.
- **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 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 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 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 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 a 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>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.</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>COLUMN</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• Invalid Response: The status displayed if the agent responds in an</td>
</tr>
<tr>
<td></td>
<td>unexpected manner.</td>
</tr>
<tr>
<td></td>
<td>• Waiting for Connection: The agent was approved, but has yet to connect to</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>system.</td>
</tr>
<tr>
<td></td>
<td>• Server-initiated: The agent listens on its designated port for connections</td>
</tr>
<tr>
<td></td>
<td>from the Orion server.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the agent software. This is helpful in determining which agents</td>
</tr>
<tr>
<td></td>
<td>should be updated.</td>
</tr>
</tbody>
</table>

When viewing Linux-based nodes monitored by Orion agents for Linux, 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 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...
     1. Click More > Edit Row Properties.
     2. In the Available Properties panel, select System Properties > Polling Method.
     3. Click Save Changes at the top of the screen.
   - If you use the legacy Manage Nodes page...
     1. 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.
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-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:
service 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.
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.

   ![Note] 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.

**Change the agent port to match the open port on the Orion server**

![Note] 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:
   
   `<agentManagementServiceConfiguration messagingPort="1778" />`

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.

   ![Note] If you installed the agent manually, you can change the port number during installation through the wizard in the web console.

   ![Note] If you deployed the agent from the server, the port number is set automatically.

   ![Note] 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 in 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 in the terminal.
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.

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.
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. Also open port 17791 if the agent is on Windows 2008 R2. 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.
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 have 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.

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-based computers 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.
- 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.

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.
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-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:
   ```bash
   service 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.

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.
### Troubleshooting agents

The most common issues with agents occur during installation or configuration. The agent may be unable to connect to the Orion server, or the server may be unable to connect to the agent.

For information about what a plug-in status means, see [View the status of agent plug-ins](#).

### Troubleshooting agent installation, deployment, and connections

If your agent does not deploy correctly, use the following questions to help you troubleshoot the issue. You can also install the agent manually on the target computer.

**Are you installing other software on the target computer?**

- Some software installations, such as Windows Updates, prevent other installations from finishing successfully.
- Install the agent when the other installations have completed.

**Is the target computer waiting to be restarted?**

- Deployment can fail when the computer is waiting to be restarted after installing software.
- Restart the computer and try again.

**Is the SolarWinds agent service installed and running on the target computer?**

- The agent may have connectivity issues. Ping the Orion server.
- Restart the agent service and try again.

**Can you ping the Orion server or connect to the web console from the target computer?**

- The SolarWinds agent requires [port 17778](#) to be open on the server (server-initiated communication).
- Verify that the Orion server can ping the computer that has the agent installed (agent-initiated communication).
- Ensure that you are using the correct Orion administrator credentials.
Do you use group policies in your organization?

- You may have a network policy that interferes with deploying agents.

Are your credentials correct?

- (Windows only) - Ensure that the account can access and create a folder at the following location: `\<hostname_or_ip>\admin$\temp` on the remote computer.
- Ensure that Remote Procedure Call (RPC), a Windows service, is running.
- Ensure the required ports are open. See the Orion Agent requirements.
  - Windows - 135, 445, 17778, and 17791
  - Linux/Unix - 22
- If you are using a domain account, use the complete name when entering credentials. For example: `domain\username`.

Can you resolve the host name or IP address?

- If a host name or Fully Qualified Domain Name was used, ensure that it can be resolved from the client computer.
- If the Orion server or the additional poller is behind a NAT, ensure that the IP address specified when creating the MST file is the correctly routed IP address the client uses to access the Orion server.

Troubleshooting agent configuration

Connection refused for a passive agent

- Specify an agent shared secret to connect an agent running in server-initiated communication mode, or specify a proxy.
- Verify that the agent port is accessible.

Agent is not running in passive mode

- The agent is running in the agent-initiated communication mode and you cannot connect to it.
- Change the communication mode to server-initiated. You can uninstall and install the agent from the server, or manually install it.
- You can change the communication mode on the remote host through the Control Panel > Orion Agent Settings.

Agent is not running in passive mode

- The agent version is empty or zero. This indicates that something is wrong with the agent.
- Install the agent again.
Agent GUID is different than the request ID

- The agent may be connected to another Orion server, or is broken.
- Install the agent again.

Troubleshooting agent connections

If your agent and your Orion server cannot communicate, the agent cannot respond to queries or the Orion server cannot receive data from the agent.

ℹ️ You must have access to the remote host for most troubleshooting steps.

Is the agent service running?

- You can check the Manage Agents page for the agent status, or log in to the remote host with the agent installed to check the status.
- If the agent is not running or has stopped, start the SolarWinds Agent service.

Are all plug-ins installed correctly?

- Select the agent in the Manage Agents page and click More Actions > View installed agent plug-ins.
- If there is a problem with a plug-in, ensure that all prerequisites are installed, such as python, and then reinstall the agent.

Do the communication modes match between the agent and the server?

- On the remote host, open the Control Panel > Orion Agent Settings. The communication mode must match the communication mode in the Manage Agents page on the Orion server.
- If the modes do not match, change one to match the other.

Does the server initiate communication?

- Log in to the server host and ping the remote host.
- Server-initiated communication requires port 17790 to be open on the remote host.

Does the agent initiate communication?

- Log in to the remote host and ping the server.
- Agent-initiated communication requires port 17778 to be open on the server.

Is the remote host running on a Linux distribution?

- Ensure that **Python 2**, versions 2.4.3 and later, is installed. Check the python version by typing `python -v` in the command line.
Monitor your environment using AppStack

The Application Stack, or AppStack, refers to the various layers that make up a complex application delivery infrastructure. The AppStack Environment view is an interactive visual mapping within the Orion Platform that provides an in-depth perspective through an entire environment to help identify the root cause of performance and availability issues.

AppStack automatically gathers information about objects in an environment, as well as their respective relationships, and displays them in a customizable view. Some relationships, such as groups and dependencies, can be customized.

| The AppStack environment supports only server and virtual server node types. |

| To display relationship data about AWS and/or Azure cloud-based instances and VMs in AppStack, manage them as nodes in the Orion Platform so relationship data is retrieved during monitoring. |

To access the AppStack, click My Dashboards > Environment. Filter the application view with filter options and filter properties. You can also save and reuse these filters as layouts to display specific views of the AppStack.

In the AppStack view, you can hover-over each node and application to see a tooltip of data and status. This view provides quick insight into issues in the stack and overall statistics. Select each item on the view to load related items throughout the environment. See AppStack data overview for details on icons and colors of icons for at-a-glance monitoring.

| You can further understand, monitor, and customize the AppStack with the following: |

| AppStack categories and data |
| Customize the AppStack view |
Troubleshooting with AppStack

Using AppStack as a troubleshooting tool is fairly straightforward. Simply navigate to the AppStack Environment view, and click on an object to see related objects. To investigate further, navigate to the Details page of the object or any related object.

For example, the illustration below displays all objects in the current environment. The application, MSSQLSERVER, is in a Critical state, as indicated by its icon. To see what this application is related to, click the MSSQLSERVER icon.

As you select objects in the AppStack, the system automatically updates the view to select and highlight related objects. In this example, MSSQLSERVER is selected. Once it is selected, related objects are highlighted by the fading of unrelated objects, as shown:
If you want to completely hide unrelated objects from the view, you can click the Spotlight. Select an object then click Spotlight in the upper right-hand corner to hide them.

To navigate to the details page of a selected object, click the icon of the selected object next to the chart at top or double-click the larger icon in the main view. You can review and managed the critical and warning issues per node.

AppStack categories and data

By default, the following AppStack Environment categories are available in the Orion Platform:

- Groups
- Applications
- Database Instances (with Orion Integrated DPA)
- Servers
- Hosts
- Virtual Clusters
- Virtual DataCenters
- Virtual Centers
- Volumes

Other Orion Platform products offer additional categories. Empty categories can be hidden through the Change Layout Settings option in the drop down menu.
The Category Status Summary (located to the right of each category) parses, enumerates, and displays the number of objects in a given category, emphasizing the status as indicated by the colors. The Category Status Summary can be toggled to either display at all times, or only when categories are collapsed.

You can manage the setting through the Change Layout Settingsoption.

Supported categories and data

The following matrix outlines categories associated with the AppStack Environment view, which vary by SolarWinds product.

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>SRM</th>
<th>SAM</th>
<th>VMAN</th>
<th>WPM</th>
<th>DPA</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>Use Groups more effectively manage your environment by organizing monitored objects logically, regardless of device type or location.</td>
</tr>
<tr>
<td>Applications</td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
<td>In SAM, an application is a collection of component monitors grouped together to collect specific metrics concerning the application as a whole.</td>
</tr>
<tr>
<td>Database Instances</td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
<td>A database is an organized collection of data. The displayed database instances including Microsoft SQL, MySQL, and Oracle.</td>
</tr>
<tr>
<td>Transactions</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td>A transaction is a recording of web browser steps assigned to a specific location.</td>
</tr>
<tr>
<td>Steps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td>A step is a collection of actions. For example, the actions required to navigate to a specific URL make up one step.</td>
</tr>
<tr>
<td>Servers</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
<td>A server is a computer capable of accepting requests from the client and giving responses accordingly. The server makes services, as access to data files, programs, and peripheral devices, available to workstations on a network.</td>
</tr>
<tr>
<td>Hosts</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
<td>A Host is defined as a server running a Hypervisor for virtualization that can host multiple VM.</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>SRM</td>
<td>SAM</td>
<td>VMAN</td>
<td>WPM</td>
<td>DPA</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
<td>-----</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Virtual Clusters</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td>Virtual clusters are built with VMs installed at distributed servers from one or more physical clusters. VMs in a virtual cluster are logically connected by a virtual network across several physical networks. Each virtual cluster is formed with physical machines or a VM hosted by multiple physical clusters.</td>
</tr>
<tr>
<td>Virtual Datacenters</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td>A virtual datacenter is a centralized virtual repository to store, manage, and disseminate data related to a particular body of knowledge or pertaining to a particular business.</td>
</tr>
<tr>
<td>Virtual Centers</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td>A VMware virtual center (vCenter) server is a centralized management application that manages VMs and ESXi hosts centrally. Use a vSphere client to access vCenter Server and manage ESXi servers.</td>
</tr>
<tr>
<td>Data Stores</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td>A data store is a repository of a set of data objects. These objects are modeled using classes defined in a database schema. A data store is a general concept that includes not just repositories like databases, but also simpler store types such as flat files. Some data stores represent data in only one schema, while other data stores use several schemas for this task.</td>
</tr>
<tr>
<td>Volumes</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td>A volume, or logical drive, is a single accessible storage area with a single file system, typically resident on a single partition of a hard disk.</td>
</tr>
<tr>
<td>LUNS</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A Logical Unit Number, or LUN, is a number used to identify a logical unit, which is a device addressed by the SCSI protocol or Storage Area Network protocols which encapsulate SCSI, such as Fibre Channel or iSCSI. A LUN may be used with any device which supports read/write operations, such as a tape drive, but is most often used to refer to a logical disk as created on a SAN.</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>SRM</td>
<td>SAM</td>
<td>VMAN</td>
<td>WPM</td>
<td>DPA</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>----------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
<td>-----</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NAS Volumes</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>Network-attached storage (NAS) is a type of dedicated file storage device that provides local-area network (LAN) users with centralized, consolidated disk storage through a standard Ethernet connection.</td>
</tr>
<tr>
<td>Pools</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>A storage pool (also called a RAID array) is a collection of disk drives that become a logical entity. When you create a storage pool, you select the desired capacity (number of disk drives) and assign a RAID level to it which provides a redundancy level.</td>
</tr>
<tr>
<td>VServers</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>A virtual storage server (VServer) contains data volumes and one or more LIFs through which it serves data to the clients. A VServer can either contain one or more FlexVol volumes, or a single Infinite Volume. A VServer securely isolates the shared virtualized data storage and network, and appears as a single dedicated server to its clients. Each VServer has a separate administrator authentication domain and can be managed independently by a VServer administrator. In a cluster, a VServer facilitates data access. A cluster must have at least one VServer to serve data. V Servers use the storage and network resources of the cluster. However, the volumes and LIFs are exclusive to the V-Server. Multiple Vservers can coexist in a single cluster without being bound to any node in a cluster. However, they are bound to the physical cluster on which they exist.</td>
</tr>
<tr>
<td>Storage Arrays</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>Storage Arrays consist of two or more disk drives built into a stand-alone unit. Storage arrays provide increased availability, resiliency, and maintainability by using existing components (controllers, power supplies, fans, and so on) often up to the point</td>
</tr>
</tbody>
</table>
where all single points of failure are eliminated from the design.

This AppStack provides a sample of categories and multiple nodes in various health states:

AppStack data overview

The AppStack uses specific colors and icons, hover overs, and navigation options to help identify object status as you monitor:

- Object status and colors
- Using quick links
- Using the overview bar
Object status and colors

Objects in the AppStack display with colors based on their current status, providing a quick summary of your environment. Objects will be in one of the following states according to the icon color and shape:

<table>
<thead>
<tr>
<th>STATUS</th>
<th>COLOR</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Down</td>
<td>Red</td>
<td><img src="image" alt="Red Icon" /></td>
</tr>
<tr>
<td>Critical</td>
<td>Pink</td>
<td><img src="image" alt="Pink Icon" /></td>
</tr>
<tr>
<td>Warning</td>
<td>Yellow</td>
<td><img src="image" alt="Yellow Icon" /></td>
</tr>
<tr>
<td>Unknown</td>
<td>Gray</td>
<td><img src="image" alt="Gray Icon" /></td>
</tr>
<tr>
<td>Unreachable</td>
<td>Black</td>
<td><img src="image" alt="Black Icon" /></td>
</tr>
<tr>
<td>Up</td>
<td>Green</td>
<td><img src="image" alt="Green Icon" /></td>
</tr>
<tr>
<td>Other</td>
<td>Blue</td>
<td><img src="image" alt="Blue Icon" /></td>
</tr>
<tr>
<td>External</td>
<td>Purple</td>
<td><img src="image" alt="Purple Icon" /></td>
</tr>
</tbody>
</table>

You can only filter against statuses actively monitored in the AppStack. For example, if no objects have a status of Down, the Down status is not available for filtering.

Servers can only provide an Up or Down status. To check CPU, memory, or hardware health status, hover over the server icon to view the detailed tooltip. The reported status for applications and LUNs is based on performance thresholds.
The AppStack Environment view offers a parent/child relationship. (Parents can be either servers or hosts.) This relationship is represented as a mixed icon. The parent is the larger of the two icons that is hosting the child. For example, the following illustration graphically shows that an application (child) is Down on a node (parent) that is Up.

![Diagram showing parent node up and child application down]

Using quick links

Use the Quick Links bar to quickly open and close object categories. You can also show or hide the names of objects with a distressed status.

- Expand All
- Collapse All
- Show Names

Expand All

Open all categories to reveal objects in each category. Each category can be individually expanded and collapsed by clicking [+] and [-] next to the category name.

![Expanded categories showing objects]

Collapse All

Close all categories, hiding the objects within each category. Each category can be individually expanded and collapsed by clicking [+] and [-] next to the category name.

![Collapsed categories]

---

page 170
Show/Hide Names

Toggle between showing and hiding the names for each object in a distressed state. If more objects exist than can be displayed, the category name displays the number of displayed objects followed by the total number of objects. For example, (87 of 111), meaning only 87 objects of 111 total objects in this category are being displayed. This provides a numerical summary of your environment.

Click More (located after the last visible object in the category) to display the next 50 objects. Related objects may be found by clicking More. The default number of 50 can be changed in the Settings page.

Using the overview bar

The Overview Bar summarizes your environment in a compact space. If your view is currently filtered, the filtered objects display above the Overview Bar, as shown.

The doughnut chart in the Overview section displays the ratio of objects to one another in all possible states using indicative colored slices. The total number of objects in your environment is also displayed.

Objects under the Issues header are parsed and enumerated according to status. Objects shown here will be in one of the following distressed states: Down, Critical, Warning, Unknown and Unreachable. An icon and count will only appear if at least one object is currently in that state.
Customize the AppStack view

Customize this view by clicking Change Layout Settings in the Layout drop down menu on the AppStack page. These settings affect the look of content and refresh rate of the page. Modifying settings can help with performance, such as limiting the amount of objects displayed, hiding empty categories, and increasing or reducing the update interval.

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

You can modify the following:

- Limit on Up Objects Shown per Category: Objects in the AppStack Environment view are ordered from left to right, with the worst status being shown on the left side of the view. Limiting the number of Up objects can provide more room for objects needing attention.

  Limiting the number of Up objects displayed can improve AppStack performance.

- Object Names: Displays distressed objects.
- Align Objects: By default, all objects are left-aligned.
- Show Category Status Summary: The Category Status Summary are the colored numbers to the right of each category, indicating the number of objects in a particular state. This can visible at all times, or only when categories are collapsed.
• Empty Categories: Select this option to hide categories with no objects, giving the view a cleaner look.
• Update Interval: Change the time between AppStack refreshes.

Use filters for AppStack

You can filter AppStack data by status, display name, and applications to create different layouts for data to speed troubleshooting for servers and virtual servers.

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

Filter options

By default, every object displays in the AppStack Environment view. To display only objects with a certain status, filter the view by selecting one or more statuses and then applying the filter. You can also filter objects based on various properties, as well as keywords.

The filtering sidebar includes the following options:
Statuses only become available for filtering when an object in your environment is in that state. For example, if no objects have a status of Down, the Down status will not be available when filtering.

Creating filters

Creating filters using the AppStack filter properties provides more options to refine the content displayed in the AppStack:

1. Click My Dashboards > Environment, and then click [+ ] Add Filter Properties.
2. In the pop-up menu, select one or more objects from the Orion Object drop down list.

3. Click Add column to display the new filters.

AppStack filter options

By default, every object is displayed when you enter the AppStack Environment view. If you are concerned only about objects with a certain status, you can filter the view by selecting one or more statuses and then applying the filter. Additionally, you can filter objects based on various properties, as well as one or more keywords.
The filtering sidebar includes the following options:

![Filtering Sidebar Diagram]

- **Statuses only become available for filtering when an object in your environment is in that state.** For example, if no objects have a status of *Down*, the *Down* status will not be available when filtering.

Create an AppStack layout

A **Layout** is a user-defined filter with configured settings you can save and use when viewing the AppStack. You can tailor layouts with filters to view specific objects of interest. A default layout is provided that contains all currently monitored objects visible in the AppStack Environment. You cannot modify the default layout. As you create and save layouts, load them via the Layout menu.

To create a layout:

1. Create a filter by [selecting options](#) in the sidebar or selecting [filter properties](#).
2. Apply the filter to update the AppStack.
3. Under the Layout menu, click Save As New Layout. Enter a name and save. The layout adds to the Layout menu.
You can modify the layout by making changes to the filter and clicking Save to update. If you want to save as a new layout, click Save as New Layout. To remove a layout, select the layout as currently used and select Delete this Layout.

For example, to create a Layout where only IIS objects in the AppStack Environment view are shown, add the IIS filter property. Apply the filter and save it as a new layout.

The layout is added to the Layout menu, allowing you to easily navigate to that layout with its defined filter and settings. The dot to the left of the layout in the menu indicates the layout currently used.

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 SolarWinds 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

Several Orion Platform products support the Cloud Infrastructure Monitoring feature, including SolarWinds SAM and VMAN. Click here to see the latest details.

<table>
<thead>
<tr>
<th>FUNCTIONALITY</th>
<th>REQUIREMENTS</th>
</tr>
</thead>
</table>
| Monitor AWS cloud metrics         | An [AWS account configured for cloud monitoring](https://aws.amazon.com) You will need the following credentials to add an account to the Orion Platform or deploy Orion agents to instances:  
  - Access Key ID  
  - Secret Access Key |
| Monitor Azure cloud metrics       | An [Azure account configured for cloud monitoring](https://azure.microsoft.com) You will need the following credentials to add an account to the Orion Platform or deploy Orion agents to VMs:  
  - Subscription ID  
  - Tenant/Directory ID  
  - Client/Application ID  
  - Application Secret Key |

The Orion Platform supports VMs deployed via the [Azure Resource Manager](https://azure.microsoft.com) but not VMs created using a classic deployment model.

The Orion server must be configured to communicate with public services 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 and add an initial cloud account 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](https://aws.amazon.com) and [Azure Rest API](https://azure.microsoft.com), 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.

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.
4. Select a Cloud Service Provider.

<table>
<thead>
<tr>
<th>Cloud Service Provider</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon AWS</td>
<td>Microsoft Azure</td>
<td></td>
</tr>
</tbody>
</table>

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.

9. (Optional) Toggle Auto Monitoring off for instances/VMs added later, either manually or via automated discovery.

10. Click Continue to complete the wizard.

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.
If an instance/VM is a managed node, additional data such as CPU usage and packet loss displays.

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 for details.

Establish AWS IAM permissions

To interact with the Orion Platform, an AWS account must be able to retrieve CloudWatch metrics from various resources. Review Authentication and Access Control for Amazon CloudWatch and use this section as a reference for specific permissions.

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": "2016-10-17",
    "Statement": [{
        "Effect": "Allow",
        "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": "2016-10-17",
     "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 select its check box.
3. Click Policy Actions > Attach.
4. Select the All Types option and Users.
5. Navigate to the account and select 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, 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 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:
  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 and 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 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](https://aws.amazon.com/cloudwatch) 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><strong>Metric</strong></th>
<th><strong>Description</strong></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>
</tbody>
</table>
| Public DNS Name        | 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                        |
| Private DNS Name       | The internal hostname of the instance that resolves to the instance's private IP address.  
<pre><code>                      | Example: fogbugz.dev.local                                                        |
</code></pre>
<p>| Subnet ID              | The range of IP addresses in a virtual private cloud (VPC) that the instance was launched into, if applicable. Click <a href="#">here</a> to learn more about VPCs and subnets. |
| Source/Destination Check | Indicates if source/destination checks are being performed on an instance to determine if it sends/receives traffic. |
| Instance ID            | The ID for the cloud instance.                                                  |
| Instance Type          | The type of instance determines your instance's CPU capacity, memory, and storage (for example, m1.small or c1.xlarge). See the <a href="#">AWS Instance Types page</a> for full details. |
| Instance Creation Date | The time the instance launched.                                                 |</p>
<table>
<thead>
<tr>
<th><strong>Metric</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<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. Example: ari-7d0d2509</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. For example: vpc-c46c9ea1</td>
</tr>
<tr>
<td>KeyPair name</td>
<td>The name of the key pair, if this instance was launched with an associated</td>
</tr>
</tbody>
</table>

For example: vpc-c46c9ea1
<table>
<thead>
<tr>
<th><strong>Metric</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>KeyPair</td>
<td></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>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><strong>METRIC</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume ID</td>
<td>User-friendly name of the cloud volume</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>Sum(VolumeReadBytes) / Period / 1024</td>
</tr>
<tr>
<td><strong>METRIC</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Write Bandwidth (KB/S)</td>
<td>Sum(VolumeWriteBytes) / Period / 1024</td>
</tr>
<tr>
<td>Read Throughput IOPS</td>
<td>Sum(VolumeReadOps) / Period</td>
</tr>
<tr>
<td>Write Throughput IOPS</td>
<td>Sum(VolumeWriteOps) / Period</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](https://portal.azure.com), 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:

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 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, see Azure subscription and service limits, quotas, and constraints. See also Prevent unexpected charges with Azure billing and cost management.

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.

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>Category</td>
<td>Metric</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Category</td>
<td>Metric</td>
</tr>
<tr>
<td>Total I/O Wait</td>
<td></td>
</tr>
<tr>
<td>SQL Disk Read Latency</td>
<td></td>
</tr>
<tr>
<td>SQL Disk Write Latency</td>
<td></td>
</tr>
<tr>
<td>Performance Counters</td>
<td>Transaction Rate</td>
</tr>
<tr>
<td></td>
<td>Buffer Cache Hit Ratio</td>
</tr>
<tr>
<td></td>
<td>Procedure Cache Hit Ratio</td>
</tr>
<tr>
<td></td>
<td>Batch Requests per Second</td>
</tr>
<tr>
<td></td>
<td>SQL Compilations per Second</td>
</tr>
<tr>
<td></td>
<td>SQL Re-compilations per Second</td>
</tr>
<tr>
<td></td>
<td>Log Bytes Flushed per Second</td>
</tr>
<tr>
<td></td>
<td>Log Flashes per Second</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Buffer Cache Size</td>
</tr>
<tr>
<td></td>
<td>Page Life Expectancy</td>
</tr>
<tr>
<td></td>
<td>Page Read per Second</td>
</tr>
<tr>
<td></td>
<td>Page Write per Second</td>
</tr>
<tr>
<td></td>
<td>Plan Cache Size</td>
</tr>
<tr>
<td></td>
<td>CPU Queue Length</td>
</tr>
<tr>
<td></td>
<td>Memory Paging Rate</td>
</tr>
<tr>
<td></td>
<td>Physical I/O Rate</td>
</tr>
<tr>
<td></td>
<td>Physical Read Rate</td>
</tr>
<tr>
<td></td>
<td>Physical Write Rate</td>
</tr>
<tr>
<td></td>
<td>Disk Queue Length</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>CPU Count</td>
</tr>
<tr>
<td></td>
<td>Disk Queue Length</td>
</tr>
<tr>
<td></td>
<td>Instance CPU Utilization</td>
</tr>
<tr>
<td></td>
<td>Signal Waits Percentage</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.

You can request an increase to polling request limits. See AWS API Gateway Limits, Pricing, and Known Issues.

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. For details about AWS throttling, refer to:

- Throttle API requests for better throughput
- Update Stage Settings in AWS
- AWS FAQ

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 adding a cloud account or 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.
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.

- Click Settings > All Settings to navigate to the Main Settings & Administration page. In the Product Specific Settings area of the page, 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. Click Monitor AWS or Monitor Azure.
   - The Continue button changes according to the provider selected.
5. When the Cloud Settings page appears, enter cloud account credentials.
6. Click Test Connection.
   - If an error occurs, verify account credentials and confirm that accounts are configured for the Orion Platform.
7. (Optional) Toggle Auto Monitoring on and off.
8. Click Continue to advance to the API Polling page.

9. (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.

10. (Optional) Change the default polling frequency — 5 minutes.

11. (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.

13. Click Continue.

14. (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.

16. (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 Configure a cloud instance/VM as a managed 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 check box next to 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 **Configure a cloud instance/VM as a managed 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.

If an instance/VM is not available, an icon displays next to it. This may occur if an instance/VM is stopped or a connection issue occurred.

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 Configure a cloud instance/VM as a managed 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 Configure a cloud instance/VM as a managed 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

Cloud Instance: [AWS instance]
Stop | Reboot | Terminate | Unmanage | Poll
```

- 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 or Azure Portal. 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. 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.
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.

**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.

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.
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.
Do not "unmanage" and then delete a cloud instance/VM that is managed as a node — the node will remain in an Unknown state in the Orion Web Console. To fully remove the managed node in the Orion Platform, stop monitoring the cloud instance/VM before deleting it. See Manage monitoring for cloud service accounts.

**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.

This option is an Orion Platform node setting that is useful to pause polling for maintenance, security updates, and more. It does not affect data through the cloud service, nor does it stop cloud service API polling.

1. In the Orion Web Console, select My Dashboards > Home > Cloud.
2. On the Cloud Summary page, locate the instance/VM in the Cloud Instances Status Summary or Cloud Server Infrastructure resource.
3. Click the instance/VM to open its Details page. If an instance/VM is managed as a node, the Node Details page appears.
4. In the Management resource, select Unmanage for an active node (or Manage for a paused node).
5. 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.

1. In the Orion Web Console, select My Dashboards > Cloud.
2. On the Cloud Summary page, locate the cloud instance/VM in the Cloud Instances Status Summary or Cloud Server Infrastructure resource.
3. Click the instance/VM to open its Details page. If an instance/VM is managed as a node, the Node Details page appears.
4. 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.
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.
4. On the Details page, click Manage Instance/VM As Node.

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.
  
  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.

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.
      
   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>5,0000 kB/s</td>
<td>100,000 kB/s</td>
</tr>
<tr>
<td>Network Transmit Rate (kB/second)</td>
<td>50,000 kB/</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 <strong>global cloud thresholds</strong>.</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.

<table>
<thead>
<tr>
<th>Alert</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure throttling is applied for cloud account</td>
<td>This alert notifies you when Azure throttling is applied while calling Azure Monitor API for Cloud Account. See Azure throttling.</td>
</tr>
<tr>
<td>Azure throttling is applied for VM</td>
<td>This alert will notify you when Azure throttling is applied on VM while calling the Azure Monitor API. See Azure throttling.</td>
</tr>
<tr>
<td>Azure throttling is applied for cloud volume</td>
<td>This alert notifies you when Azure throttling is applied on cloud volume while calling Azure Monitor API. See Azure throttling.</td>
</tr>
</tbody>
</table>

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 Orion agents deployed on managed 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; see Amazon API Gateway Limits and Azure Resource Manager. 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 application dependencies

The SolarWinds SAM Application Dependencies feature provides a holistic view of application and server connections, expanding monitoring by detecting how applications and nodes interact with each other. You can use data gathered during Application Dependencies polling to:

- Understand which applications, application processes, and nodes connect with each other.
- Ensure that the most important data for specific applications is monitored.
- Identify unmonitored applications and processes that require attention.
- Leverage latency and packet loss metrics to determine if an issue is caused by an application or the network.

This contextual visibility of relationships between applications and physical/virtual servers also reduces troubleshooting time. For example, instead of searching through many applications, nodes, and component monitors to determine why an application is slow, you can navigate to the Incoming Connections resource and analyze application dependencies to pinpoint the source of the issue.

The Incoming Connections resource on the Application Details and Node Details pages displays data gathered about application dependencies, as shown in this example:
SAM uses two types of polling to discover and monitor connections the following types of connections:

- Application to application, in a typical client/server process monitored by SAM

  ![MySQL on prodmgmt-46](1 ms, 0%) ![Apache (Linux) on prodmgmt-48](>)

- Application to node, with a server process not currently monitored by SAM

  ![prodmgmt-48](1 ms, 0%) ![MySQL on prodmgmt-46](>)

- Node to application, with a client application process not monitored by SAM

  ![MySQL on prodmgmt-46](1 ms, 0%) ![prodmgmt-48](>)

To provide a more granular picture of application dependencies, the Connection Details page shows processes and ports for connections, plus node, application, and process status. You can also enable polling to display latency and packet loss statistics. The Connection Details page shows the entire communication stack from one node to another, which makes it a unique troubleshooting tool.

---

**Application Dependencies polling overview**

SAM uses two types of polling to collect application dependency data:

- Application Dependency polling: Discovers and monitors the following types of connections:
  - Application to application, in a typical client/server process monitored by SAM
  - Application to node, with a server process not currently monitored by SAM
  - Node to application, with a client application process not monitored by SAM
- Connection Quality polling: Tracks TCP communication traveling from client nodes hosting applications to target nodes. This synthetic polling collects latency and packet loss statistics for connections without intercepting network traffic, also known as "packet sniffing."

Application Dependency polling is enabled by default but Connection Quality polling is not. See Enable Connection Quality polling.

How SAM uses Orion agents to find and monitor application dependencies

SAM uses Orion agents to flag nodes for Application Dependency polling. An agent must exist on at least one of the two nodes for which you want to display dependencies. If a node does not host an agent, the Incoming Connections resource displays sample data, as shown here.

Agent plug-in overview

The Orion Platform deploys and removes agent plug-ins as you enable and disable features in the Orion Web Console. A single agent-managed node may include multiple plug-ins to handle different tasks such as polling.

To support the Application Dependencies feature, SAM deploys agent plug-ins to nodes to monitor connections and network communications, then displays data on the Incoming Connections resource and Connection Details page.

To avoid having to update agent-plug-ins manually, make sure the Allow Automatic Agent Updates option is enabled on the Agent Settings page.
For Application Dependency polling:

- SAM deploys plug-ins to nodes if Application Dependency polling detects application-to-application or application-to-node connections.
- Agent plug-ins collect data about dependencies between applications (application-to-application connections) and/or nodes (application-to-node connections). It is available in Linux x64, Linux x86, and Windows versions.

> SAM does not deploy Application Dependencies plug-ins to the Main Polling Engine (that is, the Orion server) to avoid performance issues due to the number of connections that may be involved.

For Connection Quality polling, if enabled:

- SAM deploys additional agent plug-ins to collect TCP latency and packet loss metrics.
- For Windows nodes connected to clients that host applications and application processes, the TCP agent plug-in includes an Npcap driver to support Nping.

> If you enable Connection Quality polling and disable it later, SAM removes the TCP agent plug-in but not the Npcap driver. See Remove an Npcap driver after disabling Connection Quality Polling in the SolarWinds Success Center.

> If polling fails for Windows Server 2012 nodes, see Agent-related issues.

SAM relies on server-initiated communications to detect "from" or to" nodes, also called “passive agents” or "agentless" nodes. Only one node in a pair requires an agent plug-in. However, note that the type of data gathered by polling depends on communication settings for both nodes, as described here:

- If target and client nodes both host agent plug-ins, SAM collects data via Application Dependency and Connection Quality polling for both nodes.
- If only the target node has an agent plug-in, SAM collects IP address and port data for the client node but not application details, process names, or connection statistics.
- If only the client node has an agent plug-in, SAM collects IP address and port data for the server node. If Connection Quality polling is enabled and SAM deployed an TCP agent plug-in to the connection source node, polling can capture latency and packet loss statistics.

> Use the Manage Agents page to check the status of agent plug-ins.

To get started with monitoring connections between applications and nodes, configure the Application Dependencies feature, as described next.
Configure the Application Dependencies feature

To get started detecting and monitoring incoming connections for applications and nodes in SAM, configure the Application Dependencies feature by:

1. Deploying Orion agents to nodes that host applications.
2. Assigning application monitors to nodes.
3. Customizing polling settings.

Before you begin

Before configuring the Application Dependencies feature in the Orion Web Console, review the following details about supported environments, required Orion Platform settings, and recommended limits.

Supported environments

SAM can detect application dependencies for nodes that meet SolarWinds Orion agent requirements with the following OS exceptions:

- IBM AIX Power Systems
- Raspbian 8.0

Note the following details about Connection Quality polling:

- Desktop OSs such as Windows 7 are not supported.
- Windows 2008 R2 and R2 SP1 with driver installation protection enabled are not supported.
- Do not use on IPv6 or link-local addresses to communicate within the network segment (link) or the broadcast domain to which the host is connected.
- The dependency must involve two separate nodes.

Required Orion Platform settings

Users with the Administrator role and the following Node Management rights can configure polling settings for the Application Dependencies feature:

- Execute Application Dependency polling.
- Deploy agents to nodes.

Make sure the Allow Automatic Agent Updates option is enabled on the Agent Settings page. Otherwise, you can update agents for individual nodes on the Manage Agents page.

Recommended monitoring limits

For optimal performance, use the Application Dependencies feature to monitor up to 500 nodes.

Recommended limits per Orion instance for monitoring dependencies include:
- Application to application: 500
- Application to node: 200
- Node to application: 200
- Average number of TCP connections per single dependency: 5

See also Solarwinds Orion agent requirements.

Deploy Orion agents to nodes that host applications you want to monitor

If Orion agents and agent plug-ins do not yet exist on nodes that host applications and application processes you want to monitor, the Incoming Connections resource on the Node and Application Details pages displays sample data, as shown in this example:

![Incoming Connections](image)

Click Deploy Agent to Monitor Connections to add Orion agents and agent plug-ins for the Application Dependencies feature to a node.

💡 You can deploy agents to multiple nodes at the same time on the Manage Agents page.

Note the following details about the Application Dependencies feature:

- Application Dependency polling does not monitor the Main Polling Engine (that is, the Orion server). Otherwise, polling would impact performance due to the multitude of connections involved.
- You do not need to configure nodes for polling in advance. SAM deploys required agent plug-ins during Application Dependency polling and (if enabled) Connection Quality polling.
For Windows Failover Clusters (WFCs), the Application Dependencies feature can create dependencies between connected clients and listening servers on the server side for a cluster Virtual IP (VIP) instead of the active cluster member. See Use the Application Dependencies feature with WFCs.

Assign application monitors to nodes

Assign Application Monitors (either out-of-the-box or custom templates) to nodes with the Add New Application Monitors Wizard. See Application Discovery.

You can also assign application monitors to nodes on the Manage Templates page.

Customize polling settings

The Application Dependencies feature is enabled by default in SAM. To fine-tune related polling and thresholds for your environment, use the Application Dependency Settings page to:

- **Enable Connection Quality polling** to display network communication statistics about application dependencies.
- Indicate when SAM should remove a “down” connection and its dependencies from the Orion database.
- Set critical and warning thresholds for TCP communication alerts.

You can also disable the Application Dependencies feature for specific nodes, if necessary.

To access the Application Dependency Settings page in the Orion Web Console, click Settings > All Settings > Application Connection Settings. For details about each setting, see Manage polling for application dependencies.
Access application dependencies data

As Application Dependency polling and Connection Quality polling (if enabled) occur, the latest data populates these parts of the Orion Web Console:

- The Incoming Connections resource displayed on the Node Details and Application Details pages.
- The Connection Details page that you can access via the Incoming Connections resource.

Incoming Connections resource

Node Details and Application Details pages display the Incoming Connections resource if Application Dependency polling detects these types of dependencies:

- Application-to-application, including application processes
- Application-to-node
- Node-to-application
Sample data appears in the Incoming Connections resource if a node does not yet host an agent with application dependency agent plug-ins, or if polling did not find any dependencies. See Deploy Orion agents to nodes with applications you want to monitor.

If Connection Quality polling is enabled, the Incoming Connections resource displays the following data about TCP connections:

- Latency: Network latency (also called response time) is the time required for a packet to travel across a network path from a sender to a receiver. The higher the latency, the greater the impact on application performance as perceived by users. To troubleshoot latency issues, see Troubleshooting environmental issues with Performance Analysis dashboards.

- Packet Loss: A percentage of packets lost with respect to packets sent, usually caused by network congestion. If this value exceeds the Orion general threshold, navigate to the Nodes with High Packet Loss resource to open the custom chart for the node.
Similar to Spotlight functionality in AppStack, you can click circles at the top of the resource to filter data, as shown here:

Interpret colors and symbols in the Incoming Connections resource

Orion Platform products use icons as a visual language to describe the status of items such as nodes, interfaces, events, or alerts. See Status Indicators for details.

Values that exceed Orion Platform thresholds appear bold on a colored background.
Gray indicates that either an application is unknown or data is not displayed due to database credential account limitations stored in the SolarWinds Information Services (SWIS) business layer:

<table>
<thead>
<tr>
<th>TO DISPLAY...</th>
<th>YOU MUST HAVE PERMISSION TO VIEW...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node-to-node links</td>
<td>Both parent nodes</td>
</tr>
<tr>
<td>TCP connections and statistics about latency and packet loss</td>
<td>Both parent entities — either nodes or applications</td>
</tr>
<tr>
<td>Applications and application processes linked to a node</td>
<td>The parent node</td>
</tr>
<tr>
<td>Network connection thresholds for a node</td>
<td>The parent node</td>
</tr>
</tbody>
</table>

For a more granular picture of application dependencies, view the Connection Details page, as described next.

Connection Details page

The Connection Details page shows the entire communication stack from one node to another, which makes it a unique troubleshooting tool.

Data displayed on the Connection Details page includes:

- The application name and detected process names, such as mysqld.exe.
- Monitored TCP metrics, including:
  - CPU: The percentage of CPU utilization.
  - P-MEM: The amount of physical memory used.
  - V-MEM: The amount of virtual memory used.
  - R-IOPS: Read input/output operations per second.
  - W-IOPS: Write input/output operations per second.
- The port used by the application process.
- Latency and packet loss metrics (if Connection Quality polling is enabled).
- Latest Events details.

The Connection Details page also includes a Commands menu that you can use to configure thresholds, initiate Application Dependency polling, or hide events.

To access the Connection Details page:

1. Access a Node Details page or Application Details page in the Orion Web Console.
2. Click the arrow next to a connection displayed in the Incoming Connections Resource.

The Connection Details page opens, as shown in this example:
3. (Optional) Click an option on the Commands menu to:
   - Configure network connection thresholds.
   - Initiate Application Dependency polling immediately.
   - Show or hide events on the Connection Details page.

![Screen shot of SAM with commands menu and connection details](image)

4. (Optional) Click Thresholds on the Commands menu to adjust settings for the connection.

![Screen shot of SAM thresholds menu](image)

**Manage polling for application dependencies**

SAM uses two types of polling to collect application dependency data:

- **Application Dependency polling:** Discovers and monitors connections between applications and application processes, plus connections between applications, application processes, and nodes.
- **Connection Quality polling:** Collects latency and packet loss for connections between client nodes hosting applications and target.

Options configured on the Application Dependency Settings page impact how polling occurs across agent-monitored nodes with connections to applications. As shown here, Application Dependency polling is enabled by default, but Connection Quality polling is not.
Manage Application Dependency polling

After SAM deploys agent plug-ins to monitored nodes, Application Dependency polling scans nodes twice in the first ten minutes and then every two hours to:

- Detect connections between applications, application processes, and nodes.
  
  SAM also detects "from" or "to" nodes that rely on server-initiated communications, known as “passive agents” or “agentless” nodes. See Agent plug-in overview.

- Identify nodes as either targets or clients.

- Gather IP address and port data.

- Display data in the Incoming Connections resource on the Node and Application Details pages.
Note the following details about Application Dependency polling:

- Application Dependency polling occurs every two hours, so short-term connections are less likely to be detected due to the time between polling.
- For Windows Failover Clusters (WFCs), SAM can create application dependencies between connected clients and listening servers on the server side for a cluster Virtual IP (VIP) instead of an active cluster member. See Monitor application dependencies for WFCs.

In addition to updating global polling settings on the Application Dependency Settings page, you can disable the Application Dependencies feature and re-enable it again later if necessary, as described next.

**Disable the Application Dependencies feature**

The Application Dependencies feature is enabled by default and Application Dependency polling automatically deploys required agent plug-ins to agent-managed nodes when it detects application connections.

To disable the Application Dependencies feature:

1. Navigate to the Application Dependency Settings page.
2. Clear the Application Dependency Mapping option.
3. Click Save changes.

SAM automatically removes related agent plug-ins from nodes and stops Application Dependency polling. Connection Quality polling, if enabled, also stops.

If Connection Quality polling was enabled, SAM removes the agent plug-in that delivered the Npcap driver but does not remove the driver. See Disable Connection Quality polling.

**Enable the Application Dependencies feature after it was disabled**

If the Application Dependencies feature is disabled and you decide to enable it again, SAM redeployes agent plug-ins to nodes connected to clients that host applications and/or application processes.

To enable the Application Dependencies feature again after it was disabled:

1. Navigate to the Application Dependency Settings page.
2. Select the Application Dependency Mapping option.
3. Click Save changes.

Polling may fail immediately after re-enabling the Application Dependencies feature. Navigate to the Manage Agents page to check if an agent or agent plug-in is currently being deployed. Wait ten minutes and try polling again.

**Manage Application Dependency polling for a specific node**

You can manage Application Dependency polling for specific nodes on the Node Details page.
To disable the Application Dependency feature for a specific node:

1. Click Edit Node on the Node Details page.
2. Clear the Application Dependency Mapping Enabled check box.

To start Application Dependency polling for a single node:

1. Navigate to the Node Details page.
2. Click Poll Now.

To execute Application Dependency polling immediately across poll multiple nodes:

1. Navigate to the Manage Nodes page.
2. Select the nodes.
3. Click More Actions > Poll Now.

Manage Connection Quality polling

If Connection Quality Polling is enabled on the Application Dependency Settings page, the Incoming Connections resource includes latency and packet loss for nodes connected to applications. The default interval for Connection Quality polling is five minutes.

To gather TCP data, SAM deploys agent plug-ins to nodes to track communication traveling from clients that host applications and application processes to target nodes detected by Application Dependency polling. SAM analyzes TCP connections and displays packet loss and latency values in the Incoming Connections resource on the Node Details page.

Note the following details about Connection Quality polling:

- Desktop operating systems such as Windows 7 are not supported.
- Windows 2008 R2 and R2 SP1 with driver installation protection enabled are not supported.
- Do not use on IPv6 or link-local addresses to communicate within the network segment (link) or the broadcast domain to which the host is connected.
- SAM uses Nping to generate network packets on Windows-based nodes and collect latency and packet loss data for Connection Quality polling. To support Nping, SAM deploys an Npcap driver. If you disable polling later, SAM removes the plug-in but not the Npcap driver. See Disable Connection Quality polling.

Enable Connection Quality polling

In addition to showing how nodes connect to applications and application processes, the Incoming Connections resource and Connection Details page can display TCP connection metrics. Enable Connection Quality polling to capture packet loss and latency metrics for communication traveling from client nodes hosting applications to target nodes.
To enable Connection Quality polling:

1. Navigate to the Application Dependency Settings page.
2. Under Connection Quality Settings, toggle the Enable Connection Quality Polling option to On.
3. Click Save changes.

Disable Connection Quality polling

If you disable the Connection Quality Settings option on the Application Dependency Settings page, the following processes occur:

- SAM stops gathering latency and packet loss metrics but continues to gather application connection data.
- The status of connection entities appears as Unknown on the Connection Details page.
- SAM removes agent plug-ins deployed to Windows nodes to support polling for connection metrics on Windows nodes with Nping.

**Exception:** SAM removes agent plug-ins that delivered Npcap drivers but does not remove the actual drivers. To remove Npcap drivers, visit the SolarWinds Success Center and see Removing an Npcap driver after disabling Connection Quality Polling.

Monitor Windows Communication Foundation (WCF) communication

The Windows Communication Foundation (WCF) application uses the Net.TCP Port Sharing service to share ports across multiple processes to reduce the number of ports that need to be open on a firewall. That service listens on port 17777, which is the same port several Orion Platform services listen to so they can forward communication to the Orion Platform through an internal, non-TCP communication channel.

**Tip:** Connection Quality polling captures TCP communications only. To track non-TCP communications in the Orion Platform, create a Windows Service monitor for the NetTcpPortSharing service.

Troubleshoot application dependency issues

If the Incoming Connections resource of a Node or Application Details page displays sample data with a "Why don't I see any connections?" message, follow these steps:

1. Review Configure the Application Dependencies feature to ensure that:
   - Nodes use supported environments.
   - Orion Platform settings are configured appropriately.
   - Application Dependency elements do not surpass recommended limits.
2. Make sure Orion agents are deployed to nodes that host applications and application processes that you want to monitor for dependencies.
3. **Assign application monitors to nodes.**

4. Navigate to the [Application Dependency Settings page](#) to customize options for your environment and/or enable Connection Quality polling to monitor TCP metrics.

Application Dependency polling runs twice in the first ten minutes and then polls every two hours. Connection Quality polling, if enabled, occurs every five minutes.

If issues occur, review Events displayed on the Connection Details and [log files](#) to determine if:

- Agent plug-ins were not deployed.
- Communication with agents failed.
- Communication with plug-ins failed.
- Polling timed out, perhaps due to down nodes.
- Agent plug-in exceptions occurred (for example, due to expired licenses).

Review the following topics before contacting SolarWinds Customer Support:

- Agent-related issues.
- Data-related issues.
- Application Dependencies log files.
- Check Application Dependencies services.

**Agent-related issues**

If you suspect agent issues are interfering with Application Dependencies and/or Connection Quality polling, here are some items to check:

- Review [Configure the Application Dependencies feature](#) to make sure that each node being polled:
  - Uses a supported environment.
  - Is monitored by an Orion agent.
  - Has an application monitor assigned to it.
- Navigate to the Manage Agents page to check if an agent is currently being deployed or an agent plug-in is being installed. For Connection Quality polling, wait five minutes for the next poll and check again.
- Check for issues with agents and agent plug-ins deployed by SAM to support application dependencies polling. See [Troubleshooting agents](#).

To learn about feature availability for agent vs. agentless nodes, see these Success Center articles:

- [Comparison of Windows agent versus agentless](#)
- [Comparison of Linux agent versus agentless](#)
Connection Quality polling fails for Windows Server 2012 nodes

If polling fails for Windows Server 2012 nodes, visit the SolarWinds Success Center and see Connection Quality polling fails on Windows Server 2012 nodes.

Polling fails without errors

If application dependency data does not display as expected for a node:

1. Check if SAM deployed agent plug-ins to Orion agents on the node. Click Settings > Manage Agents > Select agent > More Actions > View installed agent plug-ins.

2. Navigate to the Node Details page to ensure that Application Dependency polling was not disabled for the node.

Polling can also fail if:

- A related component was removed or disabled.
- Agent plug-ins are currently being deployed, especially if the Application Dependencies feature or Connection Quality polling was disabled and then enabled again. Wait ten minutes and try again.

“Plug-in update required” notice

By default, the Allow Automatic Agent Updates option is enabled on the Settings > All Settings > Product Specific Settings > Agent Settings page. Application Dependency polling is also enabled by default so that SAM can poll agent-monitored nodes to detect connections between applications, application processes and nodes.

SAM deploys agent plug-ins to agent-monitored nodes when Application Dependency polling detects interaction between an application and/or application process and a node. Although most Orion Platform agents are deployed in advance, application dependency agent plug-ins are deployed immediately if an application-to-node connection is found.

If the Allow Automatic Agent Updates option is disabled on the Agent Settings page in the Orion Web Console, SAM cannot deploy agent plug-ins to server nodes and the status of the agent appears as "Plug-in update required" on the Manage Agents page.

If expected application dependencies do not appear after polling, navigate to the Manage Agents page. If a "Plug-in update required" notice appears for a node, you can either:

- Enable the Allow Automatic Agent Updates option on the Agent Settings page so SAM can deploy plug-ins automatically to all agent-managed nodes.
- Update agents individually on the Manage Agents page.
Agent Issue warning appears in the Incoming Connections resource

A red box in the Incoming Connections resource indicates that a deployed agent is not functioning properly.

Here are some items to check:

- Review [Configure the Application Dependencies feature](#) to check Orion Platform settings, deploy Orion agents, and assign application monitors to nodes, as necessary.
- Navigate to the Manage Agents page to check if the agent is currently being deployed or a plug-in is being installed. For Connection Quality polling, wait five minutes for the next poll and check again.
- Check for issues with agents and/or agent plug-ins. See [Troubleshooting agents](#).

Uninstall Npcap drivers after disabling Connection Quality polling

When Connection Quality polling is enabled on the Application Dependency Settings page, SAM deploys ADMConnectionQuality plug-ins with Npcap drivers to Windows nodes for the collection of latency and packet loss metrics.

If you disable Connection Quality polling, you can use a template to remove Npcap drivers, if necessary. See [Remove Npcap driver after disabling Connection Quality Polling for ADM](#).

Nping returns “Unable to start eithernpcap or npf service” message

This message appears for nodes running Windows 2007 or if driver installation protection is enabled for Windows 2008 R2 or later. It is related to the Npcap driver deployed via an [agent plug-in](#) that supports the Nping tool which SAM uses to gather connection statistics on Windows nodes.

SolarWinds recommends upgrading nodes to Windows 2008 R2 or later. Otherwise, you will be prompted to install Npcap each time polling occurs for Windows nodes.

Data-related issues

Review this section if unexpected data appears in the Incoming Connections resource and/or the Connection Details page.
Stale data

The Application Dependencies feature is designed to group polls into batches for efficiency so different data may be polled at different times and the status of nodes, applications, and connections may not seem synchronized.

If you notice outdated data, check polling intervals on the Application Dependency Settings page, as well as intervals defined for individual nodes on the Node Details page.

Node-specific intervals override global polling intervals defined on the Application Settings page.

Unexpected nodes in Incoming Connections resource

Application Dependency polling and Connection Quality polling check agent-managed nodes to which Application Dependency plug-ins were deployed, but “to” and “from” connections can also be detected with agentless nodes, as described in the following scenarios:

- If only the target node hosts an Application Dependency agent plug-in:
  - Application Dependency polling gathers IP address and port data for the target node.
  - Data related to the client node (application, process name, etc.) and connection statistics is not gathered or displayed.
- If only the client node hosts an Application Dependency agent plug-in:
  - Application Dependency polling gathers IP address and port data for the client node.
  - Only IP address and port data are gathered from the server node.
  - Connection statistics are not gathered.

TCP connection metrics do not update after polling

Application Dependency polling identifies agent-monitored nodes connected to applications and deploys plug-ins to those nodes before Connection Quality polling occurs. There may be a delay in between the two types of polling, plus agents and agent plug-ins need time to deploy. Wait for the next Connection Quality polling cycle to begin.

Date discrepancies on Connection Details page

The Last Polled value on the Connection Details page shows the latest time of Application Dependency polling. If polling intervals were edited for individual nodes, that date may not reflect the date of the last poll across all nodes. For example, if Node1 was polled one hour ago, but the last large-scale Application Dependency poll occurred two hours ago, the Last Poll date reflects the most recent period — one hour.
Applications and application processes lack expected node dependencies

SAM removes application-to-node connections if a parent/child node or parent/child application is removed from the Orion Platform or is no longer monitored by an agent. For dependencies detected by Connection Quality polling, the last TCP connection is removed when the parent dependency is removed.

A TCP connection may also be removed when:

- A related component is removed or disabled.
- The LastSeenTimeStamp for the connection is not updated for over eight hours. Consider changing the Remove down connections options on the Application Dependency Settings page. See Customize polling settings.
- The Application Dependency Mapping Enabled option is disabled for a specific node on the Edit Node page.

If applications and application processes do not have expected dependencies with nodes on the Incoming Connections resource, confirm that SAM detected communication between nodes by checking the inventory log:

C:\Program Files (x86)\SolarWinds\Logs\ADM\{NodeID}_\{NodeIP}.log

Check the data processing logs for monitoring applications on each node:

C:\Program Files (x86)\DataProcessingLogs\Node-{NodeID}*.log

"Unknown" connection status

If you initiate polling from the Connection Details page, Application Dependency polling starts but an "Unknown" connection status may appear until the next Connection Quality poll occurs (every five minutes, by default). Check after the next polling period.

"Loopback" connection status

TCP Loopback connections established internally on a node may appear on the Incoming Connections resource. A Loopback connection status indicates an internal connection on the node (localhost connection). If the destination and source nodes are the same, Connection Quality polling ignores the connection.

Hyperlinks to Orion components (process, port) missing

The application template does not contain any component monitoring that the system can refer to for the given process or port.

Application Dependencies log files

The Application Dependency polling job searches for application and application process connections from nodes monitored by agents to which application monitors were assigned. The job also tracks the creation of application dependencies, as indicated by agent plug-ins that SAM deploys during polling.
SAM stores Application Dependency polling logs on the main Orion server and also on target machines, as described here:

- Default Orion server locations:
  - C:\Program Files (x86)\SolarWinds\Logs\SAM.ADM\n  - C:\Program Files (x86)\SolarWinds\Logs\ADM\ADMPollingJob_{{PID}}.log

- Default target machine locations:
  - C:\Program Files (x86)\SolarWinds\Logs\Agent\SolarWinds.ADM.AgentPlug-in.exe.1360.0001.log.txt

Connection Quality polling logs are stored in the following files on the main Orion server:

- C:\Program Files (x86)\SolarWinds\Logs\ADM\ADMPollingJob_{{PID}}.log
- C:\Program Files (x86)\SolarWinds\Logs\Agent\SolarWinds.ADM.AgentPlug-in.exe.1360.0001.log.txt

To free up disk space, move logs to the C:\Program Files (x86)\SolarWinds\Logs\SAM.ADM\ folder where files are automatically deleted after five days by default.

Check Application Dependencies services

The following table describes where to check to ensure Application Dependencies services are functioning. See Application Dependencies log files for log file locations.

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>GROUP STATUS</th>
<th>EXPECTED RESULTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check nodes that will be polled</td>
<td>Collector Service log</td>
<td>See polling plans for nodes with active applications.</td>
</tr>
<tr>
<td>Check planned jobs</td>
<td>Polling Plan log</td>
<td>See jobs created for node active applications.</td>
</tr>
<tr>
<td>Check that a publish-subscribe pattern (pubsub) succeeded</td>
<td>Business Service log</td>
<td>See the cache that was created, along with inventory messages received for node with active applications.</td>
</tr>
</tbody>
</table>

Handle HTTP listeners port sharing in Windows

A networking Windows OS subsystem is implemented as a kernel-mode device driver called the HTTP protocol stack — also called HTTP.sys. This driver listens for HTTP requests from the network, passes requests to IIS or other applications for processing, and returns processed responses to client applications.
Detecting HTTP connections is not the main goal of the Application Dependencies feature. Typically, communication between clients and HTTP servers is not permanent, and Application Dependency polling occurs relatively infrequently so it will not detect short HTTP connections.

HTTP connections may appear in the Incoming Connections resource in the following circumstances:

- Random capture of common HTTP(s) occurred.
- Orion Server communication was captured during Orion server polling or via user action in the Orion Web Console that initiated a poll.
- HTTP communication persisted for a long time, perhaps due to tunneling of another kind of TCP communication over HTTP(s).

Monitor application dependencies for Windows Failover Clusters (WFCs)

When used with WFCs, the Application Dependencies feature creates dependencies between connected clients and listening servers on the server side for a cluster Virtual IP (VIP) instead of the active cluster member.

Here is the required configuration for this scenario:

- Only one agentless Orion node has an IP address that matches the virtual IP address of the clustered role.

Roles were called "Services and Applications" in SQL Server 2012 and earlier.

- Each VIP node has a unique IP address to support the Application Dependencies feature's cluster-matching algorithm.
- A SAM process monitor such as AppInsight for SQL uses an agentless node.
- Application Dependency polling deploys agent plug-ins to agent-monitored cluster member machines so they can be assigned to non-cluster VIP addresses.
The following diagram illustrates an example of MSSQL running on a WFC:

Note these details about this figure:

- An agentless node has the same IP address, 10.140.126.20, as the SQL Cluster VIP role and AppInsight for SQL is assigned to the node.
- The cluster has two members with unique IP addresses monitored as Orion agent nodes.
- The Orion Server is monitored by an Orion Server template.
- The Orion Server instance uses the cluster VIP address, 10.140.126.20, for the SQL Server data store.

SAM can detect the database connection from the Orion Server to the SQL database as a connection between an application (the Orion SQL Server, as monitored by a template) and AppInsight for SQL (MSSQLSERVER) even though the target of the database connection is SQL running on an active cluster member.

**Monitor hardware health**

Get immediate insight into hardware issues on your network. Monitoring hardware health on Cisco, Dell, F5, 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.

### 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>![Image]</td>
<td>![Image]</td>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>Power Supply status</td>
<td>![Image]</td>
<td>![Image]</td>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>Temperature</td>
<td>![Image]</td>
<td>![Image]</td>
<td>![Image]</td>
<td>![Image]</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

![Manage Hardware Sensors](image-url)
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.

**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.

Configure the SolarWinds Orion server to use the correct syslog port

By default, SolarWinds Syslog Service listens for syslog messages on port 514 (UDP). If your devices use a different port for sending syslog messages, consider reconfiguring the port on devices, or change the port on which the service listens.

1. Log in to the Orion Web Console as an administrator.
2. Go to Advanced Configuration settings. Copy /Admin/AdvancedConfiguration/Global.aspx, and paste it into your browser address bar, after /Orion. The address in the address bar should look as follows: <your product server>/Orion/Admin/AdvancedConfiguration/Global.aspx
3. On the Global tab, scroll down to SyslogService.SyslogSettings, and enter the UDP port number in the UDPListenPort entry.
4. Click Save.
5. Restart the syslog service from the notification bar or the Orion Service Manager.

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>NUMBER</td>
<td>SEVERITY</td>
<td>SUGGESTED ACTIONS</td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
<td>--------------------</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>

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>NUMBER</td>
<td>SOURCE</td>
<td>NUMBER</td>
<td>SOURCE</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------</td>
<td>--------</td>
<td>--------------------</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>
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.
2. 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.
3. 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.
4. 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.

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 and SNMP Traps > 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 Define the number of messages displayed, message retention, and the displayed columns in 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.

Define the number of messages displayed, message retention, and the displayed columns in 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 and SNMP Traps > Syslog Viewer.
2. Click File > Settings.
3. Click the General tab in the Syslog Server Settings window.
4. Adjust the Maximum Number of Messages to Display in Current Messages view slider to set the number of messages you want to display.
5. 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 and SNMP Traps > 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.
      - Syslog alerts use a unique set of variables.
   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.

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.
   a. 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.
   b. 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.
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.

You can monitor SNMP traps with SolarWinds NPM or SolarWinds SAM.

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.

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. The Trap Viewer application allows you to 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 to the Orion Web Console.
2. Click Alerts & Activity > Traps in the menu bar.
3. 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.
4. 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.

5. Confirm the number of traps displayed in the Number of Displayed Traps field.

6. 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 > Syslog and SNMP Traps > Trap Viewer.
2. Click View > Current Traps.
3. Click a column header to order listed traps by the selected trap characteristic.
4. Configure the Trap Viewer by clicking and dragging columns to order the presentation of trap characteristics.

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 > Syslog and SNMP Traps > 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.
Define how many traps to display, if you want to refresh the traps view, trap retention, and the information displayed in the Trap Viewer

1. Click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer.
2. Click File > Settings.
3. On the General tab, configure the 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.

   i 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.

   i With the exception of the asterisk (*) and underscore (_) wildcards, SolarWinds recommends against using non-alphanumeric characters in filter definitions.

   Trap rules are not applied to unmanaged nodes.

1. Click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer.
2. Click File > Settings, and click the Alerts / Filter Rules tab.
3. Click Add Rule or click Edit Rule.
4. Click the General tab, and select Enabled.
5. Select the servers from the Apply This Rule To list.
6. 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 field.
   - Click Community String, and enter the patterns in the Community String Pattern field to apply the rule to specific community strings.

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.

**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;</td>
<td>This line displays how long the device has been up.</td>
</tr>
<tr>
<td>ValueName=&quot;0&quot; DataType=&quot;67&quot; ValueName=&quot;0&quot; HexValue=&quot;&quot;</td>
<td></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;</td>
<td>This line displays the enterprise associated with the trap.</td>
</tr>
<tr>
<td>Value=&quot;1.3.6.1.4.1.11307&quot; DataType=&quot;6&quot; ValueName=&quot;enterprises.11307&quot;</td>
<td></td>
</tr>
<tr>
<td>ValueName=&quot;enterprises.11307&quot; HexValue=&quot;&quot;</td>
<td></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;</td>
<td>When the template is used in an alert, this line displays the alert message associated with the triggered alert.</td>
</tr>
<tr>
<td>Value=&quot;${AlertMessage}&quot; DataType=&quot;4&quot; ValueName=&quot;${AlertMessage}&quot; HexValue=&quot;&quot;</td>
<td></td>
</tr>
</tbody>
</table>

Add more information by adding another OID element and incrementing the OID.
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.

### SENSOR LIMITATIONS

<table>
<thead>
<tr>
<th><strong>VALUE</strong></th>
<th><strong>SENSOR LIMITATIONS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Gbps</td>
<td>Maximum throughput (NPAS and SPAS)</td>
</tr>
<tr>
<td>50 nodes</td>
<td>Maximum number of nodes per sensor (NPAS)</td>
</tr>
<tr>
<td>50,000 pairs</td>
<td>Maximum number of node and application pairs (NPAS and SPAS)</td>
</tr>
<tr>
<td>1,000 sensors</td>
<td>Maximum number of sensors deployed on your network</td>
</tr>
<tr>
<td>1,000 applications per node</td>
<td>Maximum number of applications per node or sensor (NPAS and SPAS)</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><strong>AGGREGATION LEVEL</strong></th>
<th><strong>SENSOR DEPLOYMENT</strong></th>
<th><strong>CONFIGURATION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>I HAVE ACCESS TO MY NETWORK (NPAS)</strong></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>
</tbody>
</table>

<p>| <strong>I HAVE ACCESS TO MY APPLICATION SERVERS (SPAS)</strong> | | |
| Per application       | Deploy the SPAS directly on the application server | Automatic |</p>
<table>
<thead>
<tr>
<th><strong>AGGREGATION LEVEL</strong></th>
<th><strong>SENSOR DEPLOYMENT</strong></th>
<th><strong>CONFIGURATION</strong></th>
</tr>
</thead>
<tbody>
<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.
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)

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.
3. 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.
Identify a sample set of users whose computers are monitored by the 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)

- 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.
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.

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.
3. Select Server, and click Add Nodes.

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.

**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.
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
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.

<table>
<thead>
<tr>
<th>Node</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.110.67.159</td>
<td>4Shared, Amazon Web Services, CIFS, FTP, HTTP, MS SQL</td>
</tr>
</tbody>
</table>
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.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Applications.
3. Toggle Monitoring or Discovery OFF.

Use the following table to determine which combination of settings you want to use.

<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.

   ![](image)

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.
   - 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.

- 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).

**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 Core version 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.

Install and configure the SolarWinds 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.
8. Click Save.
Manage Asset Inventory

The Asset Inventory dashboard lets you maintain a current and detailed inventory of your environment's hardware and software. Automatic inventory data collection benefits those interested in tracking asset depreciation, gathering information for insurance purposes, or managing and maintaining your infrastructure.

For more information, see:

- Enable and disable the Asset Inventory dashboard
- Asset Inventory data collection
- Add server hardware monitoring
Enable and disable the Asset Inventory dashboard

The Asset Inventory sub-view is automatically displayed for each node supported. You can enable Asset Inventory data collection for an individual node via the Add Node Wizard or by navigating through the Management resource.

The Asset Inventory option is available only if the node supports Asset Inventory polling.

Enable Asset Inventory data collection via the Management Resource

1. Navigate to the Node Details view by clicking any node.
2. From the Management resource, click List Resources.
3. Select the Asset Inventory box to enable Asset Inventory data collection.

The option to display Asset Inventory information may not be available if the node does not have a supported operating system.

Disable Asset Inventory data collection by un-checking this box.
Asset Inventory data collection

Asset Inventory data collection is automatically enabled during the Network Sonar Discovery and/or the upgrade process. Data collected for Asset Inventory purposes uses less than 100KB of database space per node. For a larger environment consisting of roughly 1,000 servers, the total Asset Inventory data should total just under 100MB.

Required sub-views are enabled by default for nodes with Asset Inventory enabled.

Inventory data does not need to be collected with the same degree of regularity as status information, therefore, the impact on your polling engine is minimal. Asset Inventory data collection occurs once daily. This data collection interval can be configured to suit your needs.

Change the Default Asset Inventory Collection Period

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

1. On the Web Console, click Settings >All Settings > Orion Polling Settings.
2. Adjust the number of days for the Default Asset Inventory Poll Interval field.
   Note: 1 is the minimum allowable value for this field.

3. Click Submit.

Add server hardware monitoring

There are two ways for administrators to add server hardware monitoring for nodes; through the Add Node wizard, and through the Node Details group of the Node Details page.
Add Node Wizard

From the Add Node wizard, the option to display Hardware Health of Servers is available after a node has been defined. Check this box to enable hardware health monitoring.

![Hardware Health Sensors]

Manually add hardware monitoring

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

2. In the All Nodes resource, click the node you want to monitor.
3. Click List Resources.

4. Select Hardware Health Sensors, and click Submit.

To disable hardware monitoring, navigate back to this screen and uncheck Hardware Health of Servers, then click Submit.

For information on troubleshooting hardware health polling, see Troubleshooting hardware health.
Manage processes, services, tasks, and events in real time

SAM provides a number of options for monitoring real-time events, including options to create component monitors from events and handle Windows tasks for monitored servers.

For details and options, see:

- Real-Time Process Explorer
- Service Control Manager
- Windows Scheduled Task Monitor
- Real-Time Event Log Viewer
Real-Time Process Explorer

The Real-Time Process Explorer (RTPE) is available for WMI and SNMP monitored nodes and displays monitored and unmonitored processes directly in SAM. The advantage of the RTPE is that you no longer need to physically or remotely log in to a computer and run the Task Manager to retrieve that machine's vital statistics.

You can view the Real-Time Process Explorer displays on the details page for an application through the Component Details pages and Node Details page.

- Only SAM administrators can end processes as well as enable and disable the RTPE.
- The User Name and Command Line columns are hidden by default.
- Using the RTPE on a node monitored via ICMP, which has no working component, requires you to select Windows credentials manually. Consider promoting the selected node to SNMP or WMI to avoid this prompt.

$i$ Pop-ups must be enabled for the Real-Time Process Explorer to be viewed.

To access the Real-Time Process Explorer:

1. On the Web Console, click My Dashboards > SAM Summary page.
2. In the All Applications group, click an Application.

A new window opens, accessing the server and application data with administrative credentials. To use different credentials, select the Use Different Credentials option. All processes list by name with checkboxes to select and end processes.
Monitor unmonitored processes

Processes currently monitored by SAM are indicated by the application icon and name of the assigned application. Processes that are not currently monitored by SAM are indicated by the [+] symbol, followed by the words, Start monitoring.

1. From the RTPE, click Start monitoring.
2. From the Edit Properties section of the Component Monitor Wizard you can begin setting up the selected component monitor.
Use the Real-Time Process Explorer

Different information is displayed in the RTPE depending on which protocol you use to monitor a node. The table below shows the differences in the information gathered based on the protocol used.

<table>
<thead>
<tr>
<th>Monitor Process</th>
<th>WMI</th>
<th>SNMP</th>
<th>Orion Agent for Linux/Unix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Process ID</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Assigned Application</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CPU usage</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Physical Memory</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual Memory</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Disk I/O</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>User Name</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Command Line</td>
<td>Yes*</td>
<td>Yes*</td>
<td>Yes*</td>
</tr>
<tr>
<td>Polling interval</td>
<td>Five seconds</td>
<td>Up to two minutes</td>
<td></td>
</tr>
</tbody>
</table>

Windows servers update their SNMP statistics every two minutes. It takes two updates to these statistics to provide an accurate calculation. Data displayed in the RTPE via SNMP can take up to four minutes to display.

* Information on certain processes may not be exposed which can result in certain rows being blank.

By default, all available columns, with the exception of the User Name and Command Line, are shown for the top ten running processes. Each column can be sorted, added, or removed by clicking the column head and then clicking the drop down arrow.

Show all running processes

Click Show All in the bottom-left of the window.

Show a set number of running processes

Change the number in the text box next to the Show All button

Pause polling

If available, click Pause Polling in the top-left of the window.
End processes

Check the boxes next to the processes you want to end and then click End Process. This option is only available when the RTPE is using a WMI connection.

Start polling

Click Start Polling in the top-left of the window.

For Windows-based nodes, change the credentials by clicking the Use Different Credentials button to bring up the credential library dialog box.

- Clicking Refresh will re-poll the running processes.
Real-Time Process Explorer alerts

Three alerts are included with the Real-Time Process Explorer:

- High CPU Percent Utilization with Top 10 Processes
  This alert sends an email when the CPU utilization is greater than 80%.
- High Physical Memory Utilization with Top 10 Processes
  An alert is sent when physical memory usage is at or above 90%.
- High Virtual Memory Utilization with Top 10 Processes
  An alert is sent when virtual memory usage is at or above 90%.

These alerts can be found in the Alert wizard. For more information, see Use alerts to monitor your environment.

Alerts may lag if you are monitoring hardware via SNMP. It takes two updates to these statistics to provide an accurate calculation, meaning an alert can take up to four minutes to reach its recipient. To expedite this process, change the protocol to WMI, which updates every five seconds. Also, consider adjusting the trigger time to a value greater than two minutes.
Real-Time Process information in top 10 alerts

SAM provides additional troubleshooting information for high CPU, memory, and virtual memory by sending email alerts. This is done by utilizing the Top Offending Processes metric running on the server at the time of the alert.

Find the executable path `SolarWinds.APM.RealTimeProcessPoller.exe` and its command line arguments below.

Command line argument syntax:

```
```

Command line argument variables

<table>
<thead>
<tr>
<th>VARIABLE</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>-n</td>
<td>ID of a Node (NodeID), which is polled.</td>
</tr>
<tr>
<td>-count</td>
<td>The number of processes to show.</td>
</tr>
<tr>
<td>-sort</td>
<td>The criteria used for the selection of top processes. Process:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CPU - Processor time. This is the default value if the</td>
</tr>
<tr>
<td></td>
<td>command line argument is not specified.</td>
</tr>
<tr>
<td></td>
<td>• PhysicalMemory - Process physical memory.</td>
</tr>
<tr>
<td></td>
<td>• VirtualMemory - Process virtual memory.</td>
</tr>
<tr>
<td></td>
<td>• DiskIO - Process disk I/O per second.</td>
</tr>
<tr>
<td>-timeout</td>
<td>Timeout for polling in seconds.</td>
</tr>
<tr>
<td>-alert</td>
<td>The AlertDefID of associated triggered alert. If this argument</td>
</tr>
<tr>
<td></td>
<td>is provided, then alert notes are updated with the results</td>
</tr>
<tr>
<td></td>
<td>from polling.</td>
</tr>
<tr>
<td>-activeObject</td>
<td>The ActiveObject property of the associated triggered alert. If</td>
</tr>
<tr>
<td></td>
<td>this argument is not provided, NodeID is used.</td>
</tr>
</tbody>
</table>

Example 1

This example returns the top 20 processes with the highest virtual memory consumption running on the host with node ID 123.
SolarWinds.APM.RealTimeProcessPoller.exe -n=123 -count=20 -sort=VirtualMemory -timeout=300

**Example 2**

This example uses the Execute an External Program alert action:

SolarWinds.APM.RealTimeProcessPoller.exe -n=${NodeID} -alert=${AlertDefID}

**Example 3**

This example uses the Execute an External Program alert action for an alert defined for the Volume object type:

SolarWinds.APM.RealTimeProcessPoller.exe -n=${NodeID} -alert=${AlertDefID} -activeObject=${NetObjectID} -sort=VirtualMemory
Real-Time Event Log Viewer

View Windows event logs in real-time using the WMI protocol with the Real-Time Event Log Viewer (RTEV). Event logs can be filtered by log type, event source, and the level of severity.

The viewer allows you to:

- Start monitoring selected real-time Windows event log entries
- Pause and restart polling
- Log into the selected server with different credentials

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

Access the Real-Time Event Log Viewer

2. Select an application from the All Applications resource.

The Real-Time Event Log Viewer opens with a filterable list of all events and logs.

⚠️ Pop-ups must be enabled for the RTEV to be viewed.
Filter Real-Time Events

After the events of the selected Log Type are collected and displayed in the window on the right, you can filter the results with various criteria.

1. Select an option from the log type drop-down menu:

2. Select Custom Sources from the Event Sources drop-down menu. Select only the sources you want to keep when the filter is applied, as highlighted:
3. Select the type of messages you want the filter to keep by selecting the Event Level.

![Event Levels]

4. Click Apply Filter to have the events filtered and displayed.

After filtering is complete, hide and unhide the filtering pane on the left by clicking either of the two arrows, highlighted in red:

![Filter Pane]

The display window shows a list of the most recent events. Should any new events occur while this window is open, a green bar at the top of the window indicates that new events have arrived. Click the green bar to add these new events to the display window.

- The Level column icons correspond to the Event Level icons in the legend of the events pane.

Clicking any message in the display window brings up a message box providing the entire message along with additional details.

**Monitor events**

You can monitor selected events from the Real-Time Event Log Viewer by selecting an event and creating a component monitor:

1. Select an event and click Start Monitoring in the Message Details view. The Add Component Monitor wizard opens with the selection.
2. Modify the Component Monitor based on the application you selected, following the wizard steps.
3. After you begin the Component Monitor Wizard, use the option to Disable Keyword Matching. The Include Events drop-down menu provides options to help you filter results.
4. Save and assign the component monitor.
Service Control Manager

The Service Control Manager (SCM) is similar to the Real Time Process Explorer, except with the SCM you manage the services of monitored Windows nodes instead of processes. The advantage of the SCM is that you no longer need to physically, or remotely, log in to a Windows computer to view and control its services. Information for running and stopped services is displayed directly through SAM using the Service Control Manager.

Services viewed in the Service Control Manager are polled every 25 seconds using WMI.

If the tool is located in the Management resource of the Node details page, you may need to add access to the user account.

The Service Control Manager (SCM) shows all the services that are on the monitored computer. Hovering the mouse over the row of any service will give you detailed information about that service.
Enable the Service Control Manager

To enable the tool:

1. In the Orion Web Console, click Settings > All Settings > Manage Accounts.
2. Locate the account and click Edit.
3. Expand the Server & Application Monitor Settings section.
4. For the Service Control Manager option, select Yes.
5. Save changes to the account.

Access the Service Control Monitor

You can access the Service Control Manager (SCM) through node details pages. Click the option to open and manage the SCM. If the option does not display, check your Orion Web Console account permissions.

- You may need to log in with an administrator account to perform this action.
- Pop-ups must be enabled in your browser to view the Service Control Manager.

The Service Control Manager button is not available on the Node Details page if the Top 10 resources are hidden.

2. In the All Nodes group, click a node.
3. On the Node Details page, locate the Management resource. This resource includes a number of tools and options.
4. Click Service Control Manager.

5. The SCM opens in a new window with services sorted alphabetically.

**Start and stop a service**

Services monitored by SAM are indicated by the application icon and name of the assigned application. Services that are not monitored by SAM are indicated by the [+] symbol, followed by the words, Start monitoring this service.

1. Click the row of a service to select it.
2. At the top of the window, select Stop Service, Start Service, or Restart service.

**Monitor a service with SAM**

1. Click Start monitoring this service in the row of the service to monitor.
2. The Edit Properties section of the Component Monitor wizard opens. Begin customizing the selected component monitor.

The table below shows the default settings for the Service Control Manager:

By default, all available columns are shown.

<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
<th>DEFAULT SETTING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Job Life Time</td>
<td>This is used to specify how long the information for a service exists.</td>
<td>3 min</td>
</tr>
<tr>
<td>Service Poll Interval</td>
<td>This is used to specify the refresh frequency of the information reported by the service.</td>
<td>25 sec</td>
</tr>
<tr>
<td>Service Action Job Time</td>
<td>This reports the timeout for a service.</td>
<td>3 min</td>
</tr>
</tbody>
</table>
Windows Scheduled Task Monitor

The Windows Scheduled Task Monitor (WSTM) is a resource designed to provide you with quick visual access to the status of scheduled tasks configured on your Windows nodes.

**Only tasks from root directory can be monitored. The WSTM will not work for tasks from every level of the Task Scheduler Library.**

Only tasks from root directory can be monitored. The WSTM will not work for tasks from every level of the Task Scheduler Library.

- Hovering over any item in the Task Name column will provide detailed information about the listed task.
- Sort the display by clicking the head of each column.

The Edit option allows you to:

- Change the polling frequency
- Change the polling timeout period
- Change credentials
- Add custom notes

You can also use the Windows Task Monitor in alerting: Alert me when task last run result is non successful

**Requirements**

The WSTM comes with an alert that will notify you of any task execution failures, as well as web-based reports that show all scheduled tasks configured across all servers in your environment. Additionally, there is a dedicated Task Failure Report you can view on-screen or have emailed to you.

**This resource is hidden when the WSTM is not being monitored on a node.**

The WSTM supports monitoring tasks on the following operating systems:
When SAM is installed on Windows 2003 R2 SP2, scheduled tasks on Windows 2008 or later cannot be polled by the Windows Scheduled Task Monitor (WSTM).

The WSTM consumes five SAM license units per node.

Only tasks from root directory can be monitored. The WSTM will not work for tasks from every level of the Task Scheduler Library.

**Enable the Windows Scheduled Task Monitor**

To enable the Windows Scheduled Task Monitor:

1. On the Web Console, click Settings > Manage Nodes.
2. Click [+] Add Node and then select the Windows Servers: WMI and ICMP option and enter the credentials.
3. Click Next and then select Windows Scheduled Tasks.
4. Complete the wizard as instructed.

The Windows Schedule Tasks option is:

- Checked when tasks are already being monitored
- Unchecked by default when at least one task is found on the target machine
- Hidden when a task is not found on the target machine

**Access the Windows Scheduled Task Monitor**

You can access the Windows Scheduled Task Monitor through the All Nodes resource in the Orion Web Console.
1. On the Web Console, click My Dashboards > Home > All Nodes resource.
2. Expand the Windows tree by clicking Windows, and then click a Windows node to be taken to the Node Details page for that node.
3. On the Node Details page, find the Windows Scheduled Task resource, as shown:

![Windows Scheduled Tasks](image)

- When monitored, the Windows Schedule Task Monitor resource is only on the Node Details view of the monitored server.

For details on status and triggers, see:

- [Windows Scheduled Task Monitor returned status codes](#)
- [WTSM status](#)
Windows Scheduled Task Monitor returned status codes

This table provides a list of status codes and their meanings that may appear in the WSTM resource.

<table>
<thead>
<tr>
<th>HEX CODE STATUS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0x0)</td>
<td>The operation completed successfully.</td>
</tr>
<tr>
<td>(0x1)</td>
<td>Incorrect or unknown function called.</td>
</tr>
<tr>
<td>(0x2)</td>
<td>File not found.</td>
</tr>
<tr>
<td>(0xA)</td>
<td>The environment is incorrect.</td>
</tr>
<tr>
<td>(0x41300)</td>
<td>The task is ready to run at its next scheduled time.</td>
</tr>
<tr>
<td>(0x41301)</td>
<td>The task is currently running.</td>
</tr>
<tr>
<td>(0x41302)</td>
<td>The task will not run at the scheduled times because it has been disabled.</td>
</tr>
<tr>
<td>(0x41303)</td>
<td>The task has not yet run.</td>
</tr>
<tr>
<td>(0x41304)</td>
<td>There are no more runs scheduled for this task.</td>
</tr>
<tr>
<td>(0x41305)</td>
<td>One or more of the properties that are needed to run this task on a schedule have not been set.</td>
</tr>
<tr>
<td>(0x41306)</td>
<td>The last run of the task was terminated by the user.</td>
</tr>
<tr>
<td>(0x41307)</td>
<td>Either the task has no triggers or the existing triggers are disabled or not set.</td>
</tr>
<tr>
<td>(0x41308)</td>
<td>Event triggers do not have set run times.</td>
</tr>
<tr>
<td>(0x4131B)</td>
<td>The task is registered, but not all specified triggers will start the task.</td>
</tr>
<tr>
<td>(0x4131C)</td>
<td>The task is registered, but may fail to start. Batch log in privilege needs to be enabled for the task principal.</td>
</tr>
<tr>
<td>(0x41325)</td>
<td>The Task Scheduler service has asked the task to run.</td>
</tr>
<tr>
<td>(0x8004020D)</td>
<td>Cannot modify or delete an object that was not added using the COM+ Admin SDK.</td>
</tr>
<tr>
<td>(0x80041309)</td>
<td>A task's trigger is not found.</td>
</tr>
<tr>
<td>(0x8004130A)</td>
<td>One or more of the properties required to run this task have not been set.</td>
</tr>
<tr>
<td>(0x8004130B)</td>
<td>There is no running instance of the task.</td>
</tr>
<tr>
<td>(0x8004130C)</td>
<td>The Task Scheduler service is not installed on this computer.</td>
</tr>
<tr>
<td>Hex Code Status</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>(0x8004130D)</td>
<td>The task object could not be opened.</td>
</tr>
<tr>
<td>(0x8004130E)</td>
<td>The object is either an invalid task object or is not a task object.</td>
</tr>
<tr>
<td>(0x8004130F)</td>
<td>No account information could be found in the Task Scheduler security database for the task indicated.</td>
</tr>
<tr>
<td>(0x80041310)</td>
<td>Unable to establish existence of the account specified.</td>
</tr>
<tr>
<td>(0x80041311)</td>
<td>Corruption was detected in the Task Scheduler security database. The database has been reset.</td>
</tr>
<tr>
<td>(0x80041312)</td>
<td>Task Scheduler security services are available only on Windows NT.</td>
</tr>
<tr>
<td>(0x80041313)</td>
<td>The task object version is either unsupported or invalid.</td>
</tr>
<tr>
<td>(0x80041314)</td>
<td>The task has been configured with an unsupported combination of account settings and run time options.</td>
</tr>
<tr>
<td>(0x80041315)</td>
<td>The Task Scheduler Service is not running.</td>
</tr>
<tr>
<td>(0x80041316)</td>
<td>The task XML contains an unexpected node.</td>
</tr>
<tr>
<td>(0x80041317)</td>
<td>The task XML contains an element or attribute from an unexpected namespace.</td>
</tr>
<tr>
<td>(0x80041318)</td>
<td>The task XML contains a value which is incorrectly formatted or out of range.</td>
</tr>
<tr>
<td>(0x80041319)</td>
<td>The task XML is missing a required element or attribute.</td>
</tr>
<tr>
<td>(0x8004131A)</td>
<td>The task XML is malformed.</td>
</tr>
<tr>
<td>(0x8004131D)</td>
<td>The task XML contains too many nodes of the same type.</td>
</tr>
<tr>
<td>(0x8004131E)</td>
<td>The task cannot be started after the trigger end boundary.</td>
</tr>
<tr>
<td>(0x8004131F)</td>
<td>An instance of this task is already running.</td>
</tr>
<tr>
<td>(0x80041320)</td>
<td>The task will not run because the user is not logged in.</td>
</tr>
<tr>
<td>(0x80041321)</td>
<td>The task image is corrupt or has been tampered with.</td>
</tr>
<tr>
<td>(0x80041322)</td>
<td>The Task Scheduler service is not available.</td>
</tr>
<tr>
<td>(0x80041323)</td>
<td>The Task Scheduler service is too busy to handle your request. Please try again later.</td>
</tr>
<tr>
<td>(0x80041324)</td>
<td>The Task Scheduler service attempted to run the task, but the task did not run due to one of the constraints in the task definition.</td>
</tr>
<tr>
<td>HEX CODE STATUS</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>(0x80041327)</td>
<td>The task has properties that are not compatible with earlier versions of Windows.</td>
</tr>
<tr>
<td>(0x80041328)</td>
<td>The task settings do not allow the task to start on demand.</td>
</tr>
<tr>
<td>(0x80070002)</td>
<td>The system cannot find the file specified.</td>
</tr>
<tr>
<td>(0x800700C1)</td>
<td>Not valid Win32 application.</td>
</tr>
<tr>
<td>(0x800704C7)</td>
<td>The operation was canceled by the user.</td>
</tr>
<tr>
<td>(0x800704DD)</td>
<td>The operation being requested was not performed because the user has not logged on to the network. The specified service does not exist.</td>
</tr>
<tr>
<td>(0xC000013A)</td>
<td>The application terminated.</td>
</tr>
<tr>
<td>(0xC06D007E)</td>
<td>Unknown software exception.</td>
</tr>
</tbody>
</table>

For a complete list of error codes, see [Task Scheduler Error and Success Constants](#).
WTSM status

The following table lists the conditions that must be met in order for a status of Available and Not Available.

The **Undefined** status is the default status.

**Available** status triggers for:

- Task Success
- Task Ready
- Task Running
- Task Disabled
- Task Has Not Run
- Task No More Runs
- Task Not Scheduled
- Task Terminated
- Task No Valid Triggers
- Event Trigger
- Some Triggers Failed
- Batch Log on Problem
- Task Queued

**Not Available** status triggers for:

- Trigger Not Found
- Task Not Ready
- Task Not Running
- Service Not Installed
- Cannot Open Task
- Invalid Task
- Account Information Not Set
- Account Name Not Found
- Account Database Corrupt
- No Security Services
- Unknown Object Version
- Unsupported Account Option
- Service Not Running
- Unexpected Node
- Name space
- Invalid Value
- Missing Node
- Malformed XML
- Too Many Nodes
- Past End Boundary
- Already Running
- User Not Logged On
- Invalid Task Hash
- Service Not Available
- Service Too Busy
- Task Attempted
- Task Not V1 Compatible
- Start On Demand
- Service Does not Exist
- No File Specified
- Cannot Delete Object
- Not Valid Application
- Incorrect Function
- File Not Found
- Environment Is Incorrect
- Application Terminated
- Unknown Software Exception
- Operation Canceled
**AppInsight Applications**

AppInsight applications provide a level of detail and expert knowledge far beyond what a simple template can provide, allowing you to monitor virtually every aspect of the assigned application.

Like any unassigned application in SAM, AppInsight applications are considered templates until applied. Until applied, you can review the AppInsight templates in the Application Monitor Templates collection.

Once applied to a node, AppInsight templates become monitored as applications. AppInsight monitoring includes multiple component monitors and performance counters.

Currently, SAM offers three different AppInsight applications:

- [AppInsight for SQL](#)
- [AppInsight for IIS](#)
- [AppInsight for Exchange](#)
AppInsight for Exchange

AppInsight for Exchange monitors virtually every aspect of your Exchange environment. It was designed exclusively for the Exchange Mailbox role that offers a detailed view of your Exchange environment. It provides detailed metrics on mailboxes, databases, and a host of performance counters without the use of agents or templates. After it is applied to a node, AppInsight for Exchange is considered an application and reports data to SAM through a set of component monitors.

You can add AppInsight for Exchange automatically for your environment through Discovery or adding it to a node manually. AppInsight uses the Exchange credentials you enter to directly access the servers, complete configuration, and collect data at polling intervals. Before adding AppInsight, verify you have the correct requirements and account permissions.


To further refine AppInsight for Exchange monitoring:

- Customize the view of resources
- Add and remove component monitors in the AppInsight for Exchange template
- Enable, modify, and use alerts for receiving notifications of Exchange server usage, issues, and thresholds

💡 To optimize your Exchange server performance, see 5 Tips to Optimize Exchange Server for Improved Performance.

Navigating AppInsight for Exchange

AppInsight for Exchange can be found in the All Applications resource on the Application Summary view.

View the AppInsight for Exchange Details page:

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

1. On the Orion Web Console, locate the All Applications resource by clicking My Dashboards > Applications > SAM Summary.
2. Expand the AppInsight for Exchange tree and click [+].
3. Expand the node tree, click [+], and then click the application.

The AppInsight for Exchange Details view provides a customizable view of resources for monitoring your Exchange servers and services. Through the resources, you can access additional Exchange details pages including performance counter, database, and mailbox details.
- Click any performance counter within a resource to view the Exchange Performance Counter Details page.

![Critical Processes and Services](image)

- Click any database within a Database resource to view the AppInsight for Exchange Database Details page.

![Mailbox Database Status](image)
Click any user name within a Mailbox resource to view the AppInsight for Exchange Mailbox Details page.

![Users By Mailbox Size](image)

**Recommendations for AppInsight for Exchange**

When using and configuring AppInsight for Exchange, SolarWinds recommend the following tips, tricks, and best practices:

- After first configuring AppInsight for Exchange, you may not receive active data for all of your resources and alerting for the first 24 hours. Resources and polling have varied polling intervals at the minutes to hours to an amount per day. After the first 24 hours, your resources should all start reporting data.
- When first testing alerts, only assign the alerts to your own or other tester email addresses.
- Watch and monitor the alerts for two weeks, to allow for generating stable baselines. You can configure to use the new baselines for refining monitoring and alert actions for the usage and performance in your specific environment. Your environment may have a unique baseline and performance expectation compared to the default thresholds.
- You can create customized NOC and resource views including AppInsight for Exchange resources for different user groups in your company and organization.
Configure AppInsight for Exchange on nodes

To configure and monitor Exchange servers in SAM, add AppInsight for Exchange to an existing node manually or to a new node through the Discovery Wizard.

Before configuring, check the Exchange requirements and permissions:

- Local administrator permissions are required for automatic configuration. You do not need these credentials for monitoring Exchange.
- To provide organization-wide capability, the service account (Domain User) needs to be a member of the View-Only Organization Management group. Membership to this group gives the user object read-only access to the entire Exchange environment, without providing any domain or local access on the Exchange server. It also prevents abuse by an unauthorized user, for example modifying Exchange environment configuration, creating or deleting users, and so on.
- In order to gather information, the user object must be assigned the Mailbox Search management role within Exchange. To configure the account, it must be a member of the Local Administrators group.

SolarWinds recommends adding this application on WMI managed nodes. If you convert an SNMP managed node to WMI, interface statistics become lost. To convert SNMP managed nodes to WMI, see Promote a Node to WMI Monitoring.

AppInsight and SAM do not support the following:

- Multiple instances of Exchange on the same server
- Nodes that are not added via WMI do not display in the List Resources dialog
- Monitoring an Exchange Database Access Group (DAG) by way of a Virtual IP address (VIP) is not supported. AppInsight for Exchange should only be applied to the physical IP address of each mailbox server in the DAG individually.

Add through the Discovery Wizard

Use the Discovery Wizard to add a new node and select AppInsight for Exchange for monitoring.

1. On the Web Console, click Settings > All Settings > Add a Node.
2. Complete the information on the Define Node step, and then click Next.
4. Click Next and complete the wizard as instructed.

   When you complete the wizard, you need to enter credentials for Exchange through another page.

5. Click My Dashboards > Applications > SAM Summary.
6. Locate the All Applications resource, expand the listed servers to locate the new node, and click the added Microsoft Exchange application and node. The node requires Exchange credentials to begin polling and monitoring. When selected, a page displays requesting credentials.

7. Enter your Exchange credentials when prompted, and click Configure Server.

![Configure Exchange Server For Monitoring](image)

Additional configuration is needed for this Exchange server. SAM will configure this Exchange server automatically (recommended). >>What changes will be made?

Enter Exchange Server Credentials

Credentials with administrative rights to Microsoft Exchange are required to configure and monitor this Exchange Server. >>Help me find these credentials.

Choose Credentials: <Inherit Windows credential from node>

Credential Name: 

User Name: 

Password: 

Confirm Password: 

TEST CREDENTIALS

Advanced Configuration (Not Recommended)

Microsoft Exchange on LAB-EXCH-HUB

CONFIGURE SERVER CLOSE

Add to an existing node

You can add AppInsight for Exchange monitoring to an Exchange server already monitored as a node in SAM.

2. Expand and select the monitored Exchanger server node in the All Nodes - Tree View resource. The details page for the node displays.
3. From the Management resource, click List Resources. The list may take a few minutes to generate.

4. Select Microsoft Exchange to enable AppInsight for Exchange data collection. When done, click Submit.

5. Click My Dashboards > Applications > SAM Summary.

6. Locate the All Applications resource, and click the Microsoft Exchange application on the specific node you modified.
   The node requires Exchange credentials to begin polling and monitoring. When selected, a page displays requesting credentials.
7. Enter your Exchange credentials when prompted, and click Configure Server.

**AppInsight for Exchange requirements and permissions**

AppInsight for Exchange works only with the MailboxRole, which is used for data storage. All other Exchange servers running different roles should use the Exchange application templates included with SAM if you intend to monitor them. Data is collected at the same default five minute polling interval as traditional application templates.

**Microsoft Exchange Versions Supported:**

- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
AppInsight for Exchange Requirements and Permissions

- Local administrator permissions are needed for automatic configuration, but they are not needed for monitoring once configuration is complete.
- To provide organization-wide capability, the service account (Domain User) needs to be a member of the View-Only Organization Management group. Membership to this group gives the user object read-only access to the entire Exchange environment, without providing any domain or local access on the Exchange server. It also prevents possible abuse by an unauthorized user accessing the account (e.g. modifying Exchange environment configuration, creating/deleting users, and so on.)
- In order to gather information, the user object must be assigned the Mailbox Search management role within Exchange. In order for the account to be configured correctly, the account must be a member of the Local Administrators group.

For Exchange access this is not required, but in order to modify Exchange and WinRM settings on the server, as well as to poll performance counters, this additional level of permission is required.

PowerShell Requirements

- Exchange 2010 must have PowerShell 2.0 installed
- Exchange 2013 must have PowerShell 3.0 installed
- Exchange 2016 must have PowerShell 3.0 installed
- Permissions must be granted for PowerShell to be accessed
- PowerShell 2.0 is required for Windows 2012 (regardless of Exchange version)
Edit the AppInsight for Exchange template

The AppInsight for Exchange application monitors metrics and status for Exchange servers through the AppInsight for Exchange template.

The template includes component monitors with default settings, some of which cannot be modified due to dependencies. For a majority of component monitors, you can modify only the notes and threshold settings for warning and critical levels.

- The primary needs for editing the template is to set general configurations such as polling frequency, polling method, and thresholds for warning and critical states for monitored metrics.
- You cannot add additional component monitors to the out-of-the-box template.
- Some component monitors can be enabled and disabled, a few others include additional configuration options.

See the out-of-the-box template description for detailed information on each component monitor and the settings you can change.

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

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Check the AppInsight for Exchange template in the list and click Edit.
3. From here, you can edit component monitor settings within the template. See the out-of-the-box template description for detailed information on each component monitor and the settings you can change.
4. When done editing, click Submit at the bottom of the page.

To begin gathering metrics, assign to Exchange servers.
Advanced Manual Configuration of AppInsight for Exchange

Manual configuration is only recommended for experienced Exchange administrators. For quick credential configuration, see Configure AppInsight for Exchange on nodes.

- Configuration changes to enable AppInsight for Exchange
- Verify Microsoft Exchange credentials
- Manually configure the Microsoft Exchange server
- Set PowerShell permissions for Exchange
- Find Exchange URL settings
- Edit the AppInsight for Exchange template

Configuration changes to enable AppInsight for Exchange

The configuration tool first transfers to the Exchange Server by using the Windows administrative share. Once on the Exchange Server, the tool uses a custom PowerShell script to make configuration changes. SAM will add the Mailbox Search Role to the Exchange server with the credentials provided. The tool then reports back to SAM with the results. If errors are reported, you will be asked to configure Exchange.

The target machine must have the following:

- WinRM 2.0
- PowerShell v2.0
- IIS

SAM will make the following configuration changes:

- Enable WinRM
- Enable Windows Authentication for PowerShell's web site
- WinRM and Windows Authentication configurations are performed remotely from SAM

⚠️ SAM uses a specially designed configuration tool to make the necessary changes for enabling AppInsight for Exchange. Once this tool completes remote configuration, it will automatically remove and unregister itself.
Verify Microsoft Exchange credentials

Here are requirements for accounts used to access Exchange:

- The account must be a domain account.
- To modify IIS and PowerShell settings on the Exchange server, the account must be a Local Administrator.
- SolarWinds recommends using accounts that are not part of the Domain Administrators group. You can add a custom domain security group to define a specific type of administrator with specific permissions to the Local Administrators group. In large environments, use Group Policy Objects (GPOs). For smaller environments, you can perform create security groups manually.

To verify Exchange credentials, run this PowerShell cmdlet in the Exchange Management Shell (EMS): `Get-ManagementRoleAssignment -RoleAssignee “USER_IDENTITY”`
Manually configure the Microsoft Exchange server

Before manually configuring an Exchange server for AppInsight for Exchange:

- Make sure to have credentials and a proper Exchange account
- Review the configuration changes to enable AppInsight for Exchange

Use the following instructions to configure an Exchange server:

- Define Exchange credentials
- Grant Exchange access
- Set mailbox search access
- Install PowerShell 2.0
- Set PSLanguageMode to FullLanguage for the PowerShell website
- Create a self-signed certificate
- Configure WinRM 2.0 on an Exchange server
- Create a firewall rule
- Configure IIS
- Test the application

Define Exchange credentials

Use domain accounts to access Exchange Management interfaces; AppInsight for Exchange does not support local accounts. Select an existing Active Directory account or create one to use with AppInsight for Exchange. See Verify Microsoft Exchange credentials.

1. On the server where you are granting local administrative privileges, open the Computer Management console.
   - On Windows Server 2012, use the Active Directory console to manage administrative privileges.
2. Navigate to the Administrators group.
3. Add the type in the Active Directory user name of the account. (Ensure the location is set to either the domain where the account is located or Entire Directory.)
4. Save your changes.

   Alternatively, add an Active Directory group to the local administrators group and add Active Directory user accounts to that group.

To verify the account and local group membership was configured properly, run the following in a PowerShell session:

```
$Recurse = $true
```
$GroupName = 'Administrators'

Add-Type -AssemblyName System.DirectoryServices.AccountManagement


$group = [System.DirectoryServices.AccountManagement.GroupPrincipal]:FindByIdentity($ct,$GroupName)

$LocalAdmin = $group.GetMembers($Recurse) | select @{N='Domain'; E={$_.Context.Name}}, samaccountName, @{N='ObjectType'; E={$_.StructuralObjectClass}} -Unique

$LocalAdmin = $LocalAdmin | Where-Object {$_.ObjectType -eq "user"}

Grant Exchange Access

To grant Least Privilege access to the Exchange Organization:

1. Open Active Directory Users and Computers (ADUC) and find the Microsoft Exchange Security Groups OU.
2. From the View-Only Organization Management group, add the user name of the account you want to grant access to the Exchange organization.

See Microsoft.com for detailed instructions.
### Set Mailbox Search Access

Mailbox Search access is required to determine attachment counts and sizes.

1. From the Start menu, open the Exchange Management Shell (EMS).
2. Type: `New-ManagementRoleAssignment -Role "Mailbox Search" -User <Username of account being granted access>` and then press Enter.
3. To verify the management role has been properly assigned, enter the following command:
   ```powershell
   Get-ManagementRoleAssignment -RoleAssignee <Username of account>
   ```

### Install PowerShell 2.0

PowerShell 2.0 is usually installed in Microsoft Server 2012; use Server Manager to confirm that PowerShell 2.0 is fully installed. Install it, if necessary.

If you have Microsoft Server 2008 R2, PowerShell 2.0 comes fully installed.

You may also need to set the PowerShell permissions. See [Set PowerShell permissions for Exchange](#).

If you need to download and install PowerShell:

1. Navigate to Windows Management Framework ([http://go.microsoft.com/fwlink/?LinkId=177670](http://go.microsoft.com/fwlink/?LinkId=177670)).
2. Review the information on the web page, and then click the link for the download of the Windows Management Framework Core for your platform in the Download Information section.
3. On the Update page, click Download.
4. When the download is complete, click Finish.

See Microsoft.com for detailed installation instructions.

### Set PSLanguageMode to FullLanguage for the PowerShell website

Use IIS Manager on the Exchange server to configure application settings for the default website and PowerShell virtual directory, and then recycle the MSExchangePowerShellAppPool application pool.

See Microsoft.com for detailed instructions.

### Create a self-signed certificate

SolarWinds provides a [Self-signed Certificate PowerShell script for AppInsight for Exchange](#). Alternatively, follow these steps to create your own certificate:

1. Using PowerShell and CertEnroll, open PowerShell in the Run as Administrator context.
2. Enter the following code:

   ```powershell
   Use the following format in the CN (Subject): "<IP Address of Server>_Solarwinds_Exchange_Zero_Configuration." For Example: "10.199.15.106_Solarwinds_Exchange_Zero_Configuration"
   ```
$name = new-object -com "X509Enrollment.CX500DistinguishedName.1"
$name.Encode("CN=TestServer", 0)

$key = new-object -com "X509Enrollment.CX509PrivateKey.1"
$key.ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
$key.KeySpec = 1
$key.Length = 1024
$key.SecurityDescriptor = "D:PAI(A;;0xd01f01ff;;;SY)(A;;0xd01f01ff;;;BA)
(A;;0x80120089;;;NS)"
$key.MachineContext = 1
$key.Create()

$serverauthoid = new-object -com "X509Enrollment.CObjectId.1"
$serverauthoid.InitializeFromValue("1.3.6.1.5.5.7.3.1")
$ekuoids = new-object -com "X509Enrollment.CObjectIds.1"
$ekuoids.add($serverauthoid)
$ekuext = new-object -com "X509Enrollment.CX509ExtensionEnhancedKeyUsage.1"
$ekuext.InitializeEncode($ekuoids)

$cert = new-object -com "X509Enrollment.CX509CertificateRequestCertificate.1"
$cert.InitializeFromPrivateKey(2, $key, "")
$cert.Subject = $name
$cert.Issuer = $cert.Subject
$cert.NotBefore = get-date
$cert.NotAfter = $cert.NotBefore.AddDays(3650)
$cert.X509Extensions.Add($ekuext)
$cert.Encode()

$enrollment = new-object -com "X509Enrollment.CX509Enrollment.1"
$enrollment.InitializeFromRequest($cert)
$certdata = $enrollment.CreateRequest(0)
$enrollment.InstallResponse(2, $certdata, 0, "")

For details, see [Generating a Certificate](#).

**Configure WinRM 2.0 on an Exchange server**

1. Open a command prompt in the Run as Administrator context.
2. Type: `winrm create winrm/config/listener?Address=*+Transport=HTTPS @
{Port="5986";CertificateThumbprint="<Thumbprint value of certificate";Hostname="<IP Address of Server>_Solarwinds_Exchange_Zero_Configuration"}` and press Enter.
3. Verify the configuration by typing: `winrm get winrm/config/listener?Address=*+Transport=HTTPS`.

Create a firewall rule

1. Open PowerShell using Run as Administrator.
2. Create a function for adding firewall rules using the following code:

   ```powershell
   function Add-FirewallRule {
   param(
     $name,
     $tcpPorts,
     $appName = $null,
     $serviceName = $null
   )
   $fw = New-Object -ComObject hnetcfg.fwpolicy2
   $rule = New-Object -ComObject HNetCfg.FWRule
   $rule.Name = $name
   if ($appName -ne $null) { $rule.ApplicationName = $appName }
   if ($serviceName -ne $null) { $rule.serviceName = $serviceName }
   $rule.Protocol = 6 #NET_FW_IP_PROTOCOL_TCP
   $rule.LocalPorts = $tcpPorts
   $rule.Enabled = $true
   $rule.Grouping = "@firewallapi.dll,-23255"
   $rule.Profiles = 7 # all
   $rule.Action = 1 # NET_FW_ACTION_ALLOW
   $rule.EdgeTraversal = $false
   $fw.Rules.Add($rule)
   }
   ```
3. Run the function to create the firewall exception for WSMAN with this command:
   ```powershell
   function Add-FirewallRule {
     param(
       $name,
       $TcpPorts,
       $AppName = $null,
       $serviceName = $null
     )
     $fw = New-Object -ComObject hnetcfg.fwpolicy2
     $rule = New-Object -ComObject HNetCfg.FWRule
     $rule.Name = $name
     if ($AppName -ne $null) { $rule.ApplicationName = $AppName }
     if ($serviceName -ne $null) { $rule.serviceName = $serviceName }
     $rule.Protocol = 5 #NET_FW_IP_PROTOCOL_TCP
     $rule.LocalPorts = $TcpPorts
     $rule.Enabled = $true
     $rule.Grouping = "@Firewallapi.dll,-23255"
     $rule.Profiles = 7 # all
     $rule.Action = 1 # NET_FW_ACTION_ALLOW
     $rule.EdgeTraversal = $false
     $fw.Rules.Add($rule)
   }
   Add-FirewallRule "Windows Remote Management" "5986" $null $null
   ```

4. Verify the rule was created.

Configure IIS

1. Open a command prompt in the Run as Administrator context.
2. Change to the C:\Windows\System32\Inetsrv directory.
4. Open PowerShell in the Run As Administrator context.
5. Type: `Import-Module WebAdministration` and press Enter.
6. Type: `(Get-WebConfiguration system.webServer/security/authentication/windowsAuthentication 'IIS:\sites\Default Web Site\PowerShell').enabled` and press Enter.
7. If the return value is True, Windows Authentication is configured. If the value returned is False, follow these steps:

   i. **Type:**
      
      ```
      Set-WebConfiguration
      system.webServer/security/authentication/windowsAuthentication
      'IIS:\sites\Default Web Site\PowerShell' -value True and then press Enter.
      ```

   ii. **Type:**
      
      ```
      (Get-WebConfiguration system.webServer/security/authentication/windowsAuthentication
      'IIS:\sites\Default Web Site\PowerShell').enabled
      ```
      to verify the setting changed.

   iii. Close PowerShell.

   iv. In the open command prompt, **type:**
      
      ```
      appcmd.exe lock config -section:system.webServer/security/authentication/windowsAuthentication
      ```
      and then press Enter.

   v. Close the command prompt.

Test the application

Navigate to the Application Edit page and click Test. Your screen should look like the following illustration.
Set PowerShell permissions for Exchange

After verifying an install, or installing PowerShell 2.0 or higher, you need to set the permissions. These permissions are required for AppInsight for Exchange and the Exchange server.

1. On the remote computer, open the PowerShell console.
3. Enable Full Control under the Permissions for Everyone group, and select Allow.
4. Ensure that the group containing the polling user has access to Microsoft PowerShell, and click OK.
5. Verify all permissions are set and saved.

Resolving errors after a reinstall

If PowerShell 2.0 was installed on Windows Server 2012 with Exchange 2013 and subsequently uninstalled, a Microsoft error removes the required registry key for remote PowerShell to work properly. Security patches or updates may also cause this issue. You can create the required registry key by following these instructions:

1. **Open Notepad and copy and paste the following text**.

   Windows Registry Editor Version 5.00

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\PowerShellEngine]
   
   "ApplicationBase"="C:\Windows\System32\WindowsPowerShell\v1.0"
   "PSCompatibleVersion"="1.0, 2.0"
   "RuntimeVersion"="v2.0.50727"
   "ConsoleHostAssemblyName"="Microsoft.PowerShell.ConsoleHost,
    Version=1.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35,
    ProcessorArchitecture=msil"
   "ConsoleHostModuleName"="C:\Windows\System32\WindowsPowerShell\v1.0\Microsoft.PowerShell.ConsoleHost.dll"
   "PowerShellVersion"="2.0"
   ```

2. **Save the file as PowerShellv1.reg and then double-click it to add it to the registry.** (A reboot may be required.)
Find Exchange URL settings

As part of the AppInsight for Exchange configurations, you should verify the PowerShell Exchange and WinRM URLs are correct. By default, AppInsight for Exchange uses the following URLs for the Exchange and WinRM sessions, where ${IP} is the IP address of the server node being added.

- **Exchange**: https://${IP}/powershell/
- **WinRM**: https://${IP}:5986/wsman/

Verify the PowerShell instance used by Exchange on a server:

1. Open the IIS Manager and navigate to the default website then to the PowerShell virtual directory.
2. Verify the Virtual Path value (typically in the Advance Settings).

Verify a server's WinRM PowerShell instance:

1. Open a command prompt using Run as Administrator.
2. Enter the command `winrm get winrm/config/listener?Address=*+Transport=HTTPS` to get the current configuration for the HTTPS protocol.

The two items of interest for the URL are Port and URLPrefix. If either of these have been modified, and do not match the default values, edit the AppInsight for Exchange application with the correct values:

- **PowerShell Exchange URL**: https://${IP}/powershell/
- **PowerShell Windows URL**: https://${IP}:9886/Custom_wsman/
Additionally, the value of Hostname must match the CN of the certificate listed in the Certificate Thumbprint property:

![Certificate](image)

CN = 10.199.3.122_Solarwinds_Exchange_Zero_Configuration
For more information, see:

- [Manually configure the Microsoft Exchange server](#)
- [Set PowerShell permissions for Exchange](#)
Attachment extensions acknowledged by AppInsight for Exchange

The following table lists the default attachment extensions that are acknowledged by AppInsight for Exchange:

<table>
<thead>
<tr>
<th>.accdb</th>
<th>.doc</th>
<th>.inf</th>
<th>.mpp</th>
<th>.ppt</th>
<th>.swf</th>
<th>.xml</th>
</tr>
</thead>
<tbody>
<tr>
<td>.arj</td>
<td>.dot</td>
<td>.ini</td>
<td>.mobi</td>
<td>.psl</td>
<td>.tar</td>
<td>.xps</td>
</tr>
<tr>
<td>.avi</td>
<td>.eml</td>
<td>.iso</td>
<td>.mov</td>
<td>.pst</td>
<td>.tmp</td>
<td>.zip</td>
</tr>
<tr>
<td>.bak</td>
<td>.epub</td>
<td>.jar</td>
<td>.mp3</td>
<td>.pub</td>
<td>.txt</td>
<td></td>
</tr>
<tr>
<td>.bat</td>
<td>.flv</td>
<td>.jpg</td>
<td>.mpeg</td>
<td>.psd</td>
<td>.vbs</td>
<td></td>
</tr>
<tr>
<td>.bin</td>
<td>.gif</td>
<td>.jpeg</td>
<td>.msg</td>
<td>.rar</td>
<td>.wav</td>
<td></td>
</tr>
<tr>
<td>.bmp</td>
<td>.gzip</td>
<td>.lnk</td>
<td>.pdf</td>
<td>.reg</td>
<td>.wks</td>
<td></td>
</tr>
<tr>
<td>.cab</td>
<td>.hta</td>
<td>.log</td>
<td>.png</td>
<td>.rtf</td>
<td>.wma</td>
<td></td>
</tr>
<tr>
<td>.cmd</td>
<td>.htm</td>
<td>.mdb</td>
<td>.pot</td>
<td>.sql</td>
<td>.wmv</td>
<td></td>
</tr>
<tr>
<td>.csv</td>
<td>.img</td>
<td>.mid</td>
<td>.pps</td>
<td>.svg</td>
<td>.xls</td>
<td></td>
</tr>
</tbody>
</table>
AppInsight for IIS

AppInsight for IIS automatically monitors your IIS environment to automate identification of IIS Server, Website and Application Pool performance issues. The dashboard provides ease of monitoring with at-a-glance performance metrics for sites and applications pools, updated through access to the IIS. As sites and application pools change through the IIS Manager, the information and connections update in SAM.

As you determine issues, easily stop or restart servers and pools as required.

AppInsight for IIS leverages PowerShell to collect data about your IIS servers. You need PowerShell 2.0 or later installed on the Orion server. You also need WinRM installed and configured on the Orion server and monitored IIS servers. For full details on requirements, see AppInsight for IIS requirements and permissions.

To start using AppInsight for IIS, apply it to a monitored node through Discovery or manually by node. Enter access credentials to add and monitor the IIS servers.

To quickly set up and use AppInsight for IIS, see:

- AppInsight for IIS requirements and permissions
- Configure AppInsight for IIS on nodes
- Manually configure AppInsight for IIS

For advanced managing of IIS sites, disable sites when unused instead of deleting them. To reduce alert noise, disable any alerts associated with those disabled sites. Enable sites anytime you need them through the Site Details pages in AppInsight for IIS. This option and others are available in the Management resource per ISS server, site, and application pool.

The following reports are installed for use with AppInsight for IIS:

- IIS SSL Certificate Expiration Report
- Site Connections Report
- Site Log Size by File
- Site Size by File

Navigate the AppInsight for IIS details view

Access AppInsight for IIS through the All Applications resource in the SAM Summary page.

ℹ️ The default IIS Application name is Microsoft IIS. You may need to log in with an administrator account to perform these actions.
To view the AppInsight for IIS details view:

1. On the Web Console, click My Dashboards > SAM Summary.
2. Locate the All Applications resource and expand the AppInsight for IIS tree by clicking [+].
3. Click an IIS application to view it.

The Sites resource lists the sites (front and backend) for the IIS server. Click a site to view additional site details including response time, connections, and requests.

The Application Pools resource lists up to 5 instances of IIS application pools. You use application pools to separate out applications from one another. If an issue occurs with an application, it may only affect other applications in the pool, not all applications in your environment.

Click a pool to view additional worker process details.

To view the Performance Counter details view, click a performance monitor in any resource.
Configure AppInsight for IIS on nodes

For existing nodes currently managed in the Orion Web Console, you can add AppInsight to the node through the Node Details page. Or you can automatically add AppInsight during Discovery.

Before adding, review the AppInsight for IIS requirements and permissions.

Add through the Discovery Wizard

You can also quickly and easily configure AppInsight for IIS during Discovery.

1. On the Web Console, click Settings > All Settings > Add a Node.
2. Complete the information on the Define Node step, and then click Next.
3. On the Choose Resources step in the Add Node Wizard, select AppInsight for IIS.
4. Click Next and complete the wizard as instructed.
5. Navigate to the All Applications resource and click your AppInsight for Exchange application.
6. Enter your Exchange credentials when prompted, and click Configure Server.
Add via manual configuration

Locate your IIS node and add AppInsight for IIS:

1. Navigate to the Node Details view by clicking any node.
2. From the Management resource, click List Resources.

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

4. Navigate to the All Applications resource to verify the addition by clicking the Applications tab in the web console.

5. Click on the newly added AppInsight for IIS application in this view and then enter your IIS credentials when prompted.
6. Once your credentials are entered, click Configure Server.

7. Click Configure Server to complete.

For more information, see:

- [AppInsight for IIS requirements and permissions](#)
- [Edit the AppInsight for IIS template](#)

**AppInsight for IIS requirements and permissions**

Review the requirements and permissions for configuring AppInsight for IIS nodes in your environment. AppInsight for IIS data is collected at the same default 5 minute polling interval as other application templates.

**AppInsight for IIS requirements and permissions**

- PowerShell 2.0 or higher must be installed on the IIS server.
- Administrator rights or equivalent credentials to the IIS server bring monitored is needed for configuration. Non-administrative permissions for polling and monitoring is only achievable using the optional Orion Agent.
- IIS 7.0 or higher must be installed.
- AppInsight for IIS supports the following versions of Microsoft operating systems and their respective IIS versions:

<table>
<thead>
<tr>
<th>MICROSOFT OS VERSION</th>
<th>&gt;IIS VERSION SUPPORTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 2008</td>
<td>IIS 7.0</td>
</tr>
<tr>
<td>Microsoft Windows 2008 R2</td>
<td>IIS 7.5</td>
</tr>
<tr>
<td>Microsoft Windows 2012</td>
<td>IIS 8.0</td>
</tr>
<tr>
<td>Microsoft Windows 2012 R2</td>
<td>IIS 8.5</td>
</tr>
</tbody>
</table>

If any prerequisite is missing, the application goes into an Unknown state.

Some resources may not function properly in Internet Explorer 8 or earlier. Consider upgrading Internet Explorer or using an alternate web browser such as Firefox or Chrome.

AppInsight for IIS technologies and ports

The following table outlines the technologies and ports used by AppInsight for IIS:

<table>
<thead>
<tr>
<th>TECHNOLOGY</th>
<th>PORT</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPC Endpoint Mapper</td>
<td>TCP port 135</td>
<td>SAM uses this port to establish WMI/RPC connections to the remote computer. RPC is required for getting performance counters information via the ASP.NET resource.</td>
</tr>
<tr>
<td>WMI</td>
<td>TCP ports 1025 - 5000 or TCP ports 49152 - 65535</td>
<td>By default, Microsoft Windows uses a random port from this range for WMI communications. The default port range differs based on the operating system. You must create a firewall exception on the remote computer.</td>
</tr>
<tr>
<td>PowerShell</td>
<td>TCP port 5986</td>
<td>This is a secure listener hosted in the WinRM service.</td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP, At least one port mentioned in the bindings of a site.</td>
<td>If the connection is not allowed, the HTTP Monitor is hidden.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP. At least one port mentioned in the secure</td>
<td>If the connection is not allowed, the HTTPS Monitor will be hidden.</td>
</tr>
</tbody>
</table>

The IIS server must have the ports open on the managed nodes.
<table>
<thead>
<tr>
<th>Technology</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>bindings of a site.</td>
<td></td>
</tr>
<tr>
<td>SSL</td>
<td>TCP. At least one port mentioned in the secure bindings of a site.</td>
<td>If the connection is not allowed, the SSL Certificate Expiration Date Monitor will be hidden.</td>
</tr>
<tr>
<td>SMB (Windows Shares)</td>
<td>TCP port 445</td>
<td>Used for Site Directory Information and Log Directory Information.</td>
</tr>
</tbody>
</table>
Edit the AppInsight for IIS template

The AppInsight for IIS application monitors metrics and status for IIS through the AppInsight for IIS template.

The template includes component monitors with default settings, some of which cannot be modified due to dependencies. For a majority of component monitors, you can modify only the notes and threshold settings for warning and critical levels.

- The primary needs for editing the template is to set general configurations such as polling frequency, polling method, and thresholds for warning and critical states for monitored metrics.
- You cannot add additional component monitors to the out-of-the-box template.
- Some component monitors can be enabled and disabled, a few others include additional configuration options.

See the out-of-the-box template description for detailed information on each component monitor and the settings you can change.

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

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Search or browse for the AppInsight for IIS template.
3. Click the checkbox and click Edit.

4. Modify the polling settings for the template as needed.
5. You can edit specific values for component monitor such as threshold values, number of records to retrieve, notes, and so on. See the out-of-the-box template description for detailed information on each component monitor and the settings you can change.
6. When done editing, click Submit at the bottom of the screen.

To begin gathering metrics, assign to IIS servers.
Manually configure AppInsight for IIS

In the event automatic configuration of AppInsight for IIS failed, visit the sections below in order and take the steps outlined to manually configure the remote computer.

For automatic AppInsight for IIS configuration see, [Configure AppInsight for IIS on nodes](#).

⚠️ **Important:** Ensure that Windows Remote Management (WS-Management) is running and that this service's Startup Type property is set to Automatic. Once this is verified, continue manual configuration in the order listed below:

1. Install PowerShell 2.0 and the WebAdministration snapin
2. Set execution policy on the target computer
3. Create a self-signed certificate
4. Create a firewall rule
5. Update WsMan limits
6. Create a WinRM listener

You can also edit the [Edit the AppInsight for IIS template](#).
Install PowerShell 2.0 and the WebAdministration snapin

The following procedures outline the installation of PowerShell and the required snapins.

Download and Install PowerShell 2.0 on Windows Server 2008

The following steps are not necessary for Windows Server 2008 R2 and Windows Server 2012.

Download PowerShell 2.0

2. Review the information on the web page, and then click the link for the download of the Windows Management Framework Core for your platform in the Download Information section.
3. On the Update page, click Download.
4. When the download is complete, click Finish.

Install PowerShell 2.0 on Windows Server 2008 and 2008 R2

Installation of PowerShell 2.0 can typically be done from the Server Manager as shown below. For installation instructions, visit www.microsoft.com

Select one or more features to install on this server.

Features:

- Remote Assistance
- Remote Differential Compression
- Remote Server Administration Tools (Installed)
- Remote PowerShell
- Simple TCP/IP Services
- SNMP Server
- SNMP Services
- Storage Manager for SMB
- Subsystem for UN*X-based Applications
- Telnet Client
- Telnet Server
- Telnet Client
- Telnet Server
- Windows Dynamic Framework
- Windows Internal Database
- Windows PowerShell Integrated Scripting Environment
- Windows Process Activation Service
- Windows Server Backup Features
- Windows Server Migration Tools
- Windows System Resource Manager
- Windows TFTP Server

Description:

Windows PowerShell Integrated Scripting Environment (ISE) enables you to run interactive commands, and edit and debug scripts in a graphical environment. The main features include color-coded syntax, selective execution, graphical debugging, Unicode support, and context-sensitive Help. Windows PowerShell ISE also includes the Out-Window command, which sends the output of a command to an interactive table in a separate window.

Install the WebAdministration Snapins.

For Managed Nodes with IIS 7.0, download and install the PowerShell WebAdministration snapins found at the following link: http://www.iis.net/learn/manage/powershell/installing-the-iis-powershell-snap-in.
The IIS PowerShell Snap-in requires the following prerequisites

- Windows Server 2008 or higher
- Microsoft PowerShell 2.0
- IIS 7.0

Install the IIS PowerShell snap-in

1. The IIS PowerShell Snap-in is available as x86 and x64 version. Download the 32-Bit version or 64-Bit version.
2. Run the MSI file to install the IIS PowerShell Snap-in.

Use the PowerShell snap-in

PowerShell snap-ins like the IIS PowerShell Snap-in have to be registered with PowerShell. There are two ways to do this:

1. **Automatic Registration by using the IIS PowerShell Management Console**

   The IIS PowerShell snap-in setup creates a new program menu shortcut. By starting this shortcut, the IIS PowerShell snap-in is registered automatically. Navigate to Start > All Programs > IIS 7.0 Extensions > IIS PowerShell Management Console. The prompt of the new PowerShell command window is set to "IIS:\" - the root of the IIS snap-in namespace.

2. **Manual Registration**

   If you want to use the IIS PowerShell snap-in from an existing PowerShell command window, you have to register the IIS snap-in manually. You can do this by simply executing the `IISConsole.psc1` file located in the $env:programfiles\IIS\PowerShellProvider directory:

   ```
   PS C:\> & "$env:programfiles\IIS\PowerShellSnapin\iisConsole.psc1"
   ```
Set execution policy on the target computer

For AppInsight, the Execution Policy needs to be set to RemoteSigned.

1. Open a PowerShell session in the Administrator context (Right-click and select Run as Administrator).
2. Enter the following command: `Set-ExecutionPolicy RemoteSigned`
Create a self-signed certificate

SolarWinds has created a PowerShell script to create a self-signed certificate suitable for AppInsight for IIS. This can be found at:

https://support.solarwinds.com/Success_Center/Server_%26_Application_Monitor_(SAM)/AppInsight_for_IIS:_Create_certificates

Once downloaded, execute the script by right-clicking it and selecting, Run with PowerShell. The following parameters apply:

- **IP address**: Mandatory
- **Certificate lifetime in days**: Optional

You can run this script with the default arguments from the PowerShell console or specify each one.

**For example:**

& '.\Create self-signed certificate script.ps1' 192.168.2.69 3650

where 192.168.2.69 is the IP address of the node to be monitored by AppInsight for IIS and 3650 is 3,650 days (10 years).
Create a firewall rule

SolarWinds has created a PowerShell script to create a firewall rule. This can be found at:

https://support.solarwinds.com/?title=Success_Center/Server_%26_Application_Monitor_(SAM)/AppInsight_for_IIS:_Create_a_firewall_rule

Once downloaded, execute the script by right-clicking it and selecting, Run with PowerShell. The following parameters apply:

- **Without parameters**: The rule is created with the default name, "Windows Remote Management HTTP/SSL" for port 5986.
- **With one parameter**: Non-default custom port.
- **With two parameters**: Non-default custom port and rule name

You can run this script with the default arguments from the PowerShell console or specify each one.

**For example:**

```
& '.\Add firewall rule.ps1' 5988 "My custom firewall rule name"
```

⚠️ The default port for this rule is 5986 and does not need to be specified. Custom ports, as in the example above that uses port 5988, must be specified.
Update WsMan limits

WsMan provides methods and properties used to create a session. SolarWinds has created a PowerShell script to update the WsMan limits suitable for AppInsight for IIS. This can be found at:

https://support.solarwinds.com/?title=Success_Center/Server_%26_Application_Monitor_(SAM)/AppInsight_for_IIS:_Update_WsMan_limits

Once downloaded, execute the script by right-clicking it and selecting, Run with PowerShell. The following parameters apply:

- maxConcurrentUsersDefaultValue - Default value is 5
- maxShellsPerUserDefaultValue - Default value is 5
- maxMemoryPerShellMBDefaultValue - Default value is 150
- serviceRestartRequired - Default value is $false

You can run this script with the default arguments from the PowerShell console or specify each one.

For example:

& '.\Update WsMan Limits.ps1'
Create a WinRM listener

**Important**: If you received the following error: *An HTTPS listener currently exists on port 5986*, use the following steps to configure the listener on an available port by changing "5986" to an available port number throughout these steps.

1. To configure WinRM on an IIS server, open a command prompt in the Run as Administrator context.
2. Type: `winrm create winrm/config/listener?Address=*+Transport=HTTPS @ {Port="5986";CertificateThumbprint="<Thumbprint value of certificate>";Hostname="<IP Address of Server>_Solarwinds_Zero_Configuration"}` and then press Enter.

   ```
   C:\Windows\system32>winrm create winrm/config/listener?Address=*+Transport=HTTPS @ {Port="5986";CertificateThumbprint="784b5ff3a3450bba920210f9564015cf1d2ec628";Hostname="10.199.3.122_Solarwinds_Exchange_Zero_Configuration"}
   ResourceCreated
   Address = http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
   ReferenceURI = http://schemas.microsoft.com/wbem/wsman/1/config/listener
   Select-Set
   Select-Set: Address = *, Transport = HTTPS
   ```

3. Verify the configuration by typing the following: `winrm get winrm/config/listener?Address=*+Transport=HTTPS`.

   ```
   C:\Windows\system32>winrm get winrm/config/listener?Address=*+Transport=HTTPS
   Listener
   Address = *
   Transport = HTTPS
   Port = 5986
   Hostname = 10.199.3.122_Solarwinds_Exchange_Zero_Configuration
   Enabled = true
   URLPrefix = wsman
   CertificateThumbprint = 78a4b5ff3a3450bba920210f9564015cf1d2ec628
   ListeningOn = 10.199.3.122, 127.0.0.1, 169.254.96.84, ::1
   ```
Find IIS URL settings

By default, AppInsight for IIS uses the following URL for the IIS and WinRM sessions, where \( \${IP} \) is the IP address of the server node being added.

**WinRM:** https://\( \${IP} \):5986/wsman/

**Verify a server’s WinRM PowerShell instance**

1. Open a command prompt in the Run as Administrator context.
2. Type: `winrm get winrm/config/listener?Address=*+Transport=HTTPS` to get the current configuration for the HTTPS protocol.
Additionally, the value of Hostname must match the CN of the certificate listed in the Certificate Thumbprint property.
AppInsight for SQL

Identify performance and troubleshoot issues for SQL databases and queries with AppInsight for SQL. This feature provides consolidated resource views into over 100 performance metrics across all SQL servers monitored by SAM. These metrics include read and write latency, index fragmentation, expensive queries (based on CPU time), SQL agent job status with logs, capacity, and resource consumption for CPU, memory, and drive space. Through one page, monitor resource consumption, respond to alerts, and monitor expensive queries without digging through multiple pages and views.

Investigate issues and performance trends without hunting through numerous views into the SQL servers in your environment. AppInsight for SQL provides a level of detail and expert knowledge far beyond what a SQL template can provide, allowing you to monitor virtually every aspect of your SQL instances and databases. The feature polls and reports metrics without use of agents, directly accessing the SQL server using configured access permissions and credentials using SNMP and WMI.

You may need to log in with an administrator account to perform these actions.

To add a node and configure AppInsight for SQL, see the following:

- **Add AppInsight for SQL to a node**: to monitor SQL servers through the Discovery wizard or manually.
- **Monitor an SQL named instance with AppInsight for SQL**: to monitor a named SQL server using the server's Virtual IP (VIP).
- **Monitor clusters with AppInsight for SQL**: to monitor an SQL cluster (used for high availability).

When applied to a Microsoft SQL instance, the AppInsight for SQL page replaces the default node details page. It monitors as an application using multiple component monitors the AppInsight for SQL template.

To modify the template or use other templates, see *Edit the AppInsight for SQL template*.

The views are accessible through one of the following:

- **SQL Server**: provides all monitored SQL applications. Select My Dashboards > Applications > SQL Server, locate and access a node.
- **AppInsight for SQL**: in the All Applications resource provides all monitored SQL server nodes. Select My Dashboards > Applications > SAM Summary, locate the All Applications resource. Expand AppInsight for SQL and select a node to view.

The SQL Server Application Summary provides resources to monitor overall data for all SQL servers including alerts, events, consumed resources:

- All Applications view of all currently managed SQL servers as nodes, expandable to locate specific nodes
- Active Application Alerts for specific alerts affecting SQL servers
- Top Processes by CPU Load, Physical Memory, Virtual Memory and more to gauge applications consuming resources
- Top Monitored Processes by I/O Total Operations, Reads, and Writers for highest bandwidth consumption, reads, and write latency
Further expanding the All Applications on the SQL Server Application Summary displays a quick view into performance counters and status. Each counter and metric can be expanded to review data.
To view all information for an application node, select the application from the view to open the details page for the AppInsight for SQL node. For example, MSSQLSERVER on lab-dem-sql-02.demo.lab in the Orion demo encountered a critical alert. To troubleshoot, access the SQL server through the All Applications resource.

This view consolidates all specific data for the selected SQL server:

- Summary of data including an AppStack view for troubleshooting, alerts, events, expensive queries, capacity usage, and other metrics
- Queries to filter expensive queries
- Transactions of WPM transaction monitors for that installed module
- DB performance for DPA IM data for that installed module
To review database data, in the AppInsight for SQL Details view, locate and select a database in the All Databases resource. The database details view includes details, a list of all databases on the node, alerts, AppStack, and more.

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATUS</th>
<th>DATABASE SIZE</th>
<th>TRANSACTION LOG SIZE</th>
</tr>
</thead>
<tbody>
<tr>
<td>master</td>
<td>Online</td>
<td>4.00 MB</td>
<td>768.00 KB</td>
</tr>
<tr>
<td>model</td>
<td>Online</td>
<td>3.06 MB</td>
<td>768.00 KB</td>
</tr>
<tr>
<td>msdb</td>
<td>Online</td>
<td>18.38 MB</td>
<td>19.63 MB</td>
</tr>
<tr>
<td>SolarWindsOnion</td>
<td>Online</td>
<td>52.06 MB</td>
<td>18.13 MB</td>
</tr>
<tr>
<td>tempdb</td>
<td>Online</td>
<td>8.00 MB</td>
<td>768.00 KB</td>
</tr>
</tbody>
</table>

To see performance counter details, in the AppInsight for SQL Details view, locate and select a performance counter in any resource.
Add AppInsight for SQL to a node

With the credentials and permissions configured on the target SQL server, quickly and easily add AppInsight for SQL to SQL servers through the Discover Wizard or manually. When added, you create a monitored node in SAM for the Microsoft SQL Server application. SAM polls the node for metrics including read and write latency, index fragmentation, expensive queries (based on CPU time), SQL agent job status with logs, capacity, and resource consumption for CPU, memory, and drive space.

To view monitored nodes, access the SQL Server page and specific SQL server details pages. See AppInsight for SQL for details.

This instance is grayed until the poller has polled this node. Once polled, the status color updates.

Add through the Discovery Wizard

Use the Discovery Wizard to add a new node and select AppInsight for SQL for monitoring.

1. Click Settings > Discovery Wizard.
2. In the Network panel, enter the IP addresses to scan through. Run through the screens as instructed.
3. On the Applications panel, all detected and supported Microsoft SQL Servers display. Select the servers to add for monitoring as nodes. Only supported versions of Microsoft SQL are located and displayed for monitoring. To see all supported versions, see AppInsight for SQL requirements and permissions.
4. Click Next and complete the wizard as instructed.
5. Navigate to the All Applications resource and click your AppInsight for SQL application. The Enter Credentials screen displays.

![Enter Credentials]

Microsoft SQL Server credentials are required to monitor SOLARWINDS_ORION on lab fsm tex

Choose Credential: New Credential

Credential Name:

User Name:

Password:

Confirm Password:

SQL Server Port Type: Use default port

SOLARWINDS_ORION on lab fsm tex

> Remove this application monitor

[ASSIGN CREDENTIAL] [CANCEL]
6. Enter your SQL credentials and select a port (or use default port).
7. Click Test to verify the credentials and configured permissions.
8. Click Assign Credential to save and complete configuration.

**Add an SQL server as a node manually**

When added, you need to select the appropriate Microsoft SQL server version from the AppInsight Applications list.

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

1. On the Web Console, click Settings > All Settings > Add Node.
2. Enter the IP address or hostname for the SQL server. Select the polling method and continue.
3. On the Choose Resources panel, check the appropriate AppInsight Application for the SQL server you will monitor.
4. Complete the steps making selections as desired such as specific metrics or custom pollers.
5. Review and adjust any settings and click Add Node.
6. Navigate to the All Applications resource and click your AppInsight for SQL application. The Enter Credentials screen displays.

7. Enter your SQL credentials and select a port (or use the default port).
8. Click Test to verify the credentials and configured permissions.
9. Click Assign Credential to save and complete configuration.

**AppInsight for SQL requirements and permissions**

AppInsight for SQL supports the following versions of Microsoft SQL Server.

<table>
<thead>
<tr>
<th>Microsoft SQL Server Version</th>
<th>Versions Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server 2008</td>
<td>Without SP, SP1, SP2, SP3</td>
</tr>
<tr>
<td>Microsoft SQL Server 2008 R2</td>
<td>Without SP, SP1, SP2 SP3</td>
</tr>
<tr>
<td>Microsoft SQL Server 2012</td>
<td>Without SP, SP1</td>
</tr>
<tr>
<td>Microsoft SQL Server 2014</td>
<td></td>
</tr>
<tr>
<td>Microsoft SQL Server 2016</td>
<td></td>
</tr>
</tbody>
</table>

AppInsight for SQL data is collected at the same default five minute polling interval as traditional application templates. Following are the requirements and permissions needed for AppInsight for SQL.

See also [SAM port requirements](#).

AppInsight for SQL does not require named-pipes. However, it does require TCP. For example, SAM uses TCP detection during discovery. You may receive an error message pertaining to "named-pipes." This is the result of the last client protocol that is tried during connection to the SQL server.
AppInsight for SQL permissions

The minimum SQL permissions required to use AppInsight for SQL are as follows:

- Must have administrator permission at the host level.
- Must be a member of the db_datareader role on the msdb system database
- Must have VIEW SERVER STATE permissions
- View any definition
- Connect permission to Master database
- Execute permission on the Xp_readerrorlog stored procedure
- Connect permission to the Msdb database
- Must be member of db_datareader role in the MSDB database
- Connect permission to all databases

Review the following information regarding monitoring SQL servers with AppInsight for SQL:

- AppInsight for SQL supports both the SNMP and WMI protocols and uses SQL to gather information about the application. Additional information is available for nodes managed via WMI.
- Agents do not work with AppInsight for SQL when the SQL server being monitored is in a cluster.
- SQL clusters cannot be polled with domain credentials via the Orion agent because agents do not work with AppInsight for SQL when the SQL server being monitored is in a cluster.

SQL account permissions

The following script configures permissions for a SQL account:

```sql
USE master
GRANT VIEW SERVER STATE TO AppInsightUser
GRANT VIEW ANY DEFINITION TO AppInsightUser
GRANT VIEW ANY DATABASE TO AppInsightUser
EXEC sp_adduser @loginame = 'AppInsightUser', @name_in_db = 'AppInsightUser'
GRANT EXECUTE ON xp_readerrorlog TO AppInsightUser
USE msdb
EXEC sp_adduser @loginame = 'AppInsightUser', @name_in_db = 'AppInsightUser'
EXEC sp_addrolemember N'db_datareader', N'AppInsightUser'
```

Windows Authentication

The following script configures permissions for a SQL account with Windows Authentication:

```sql
USE master
GRANT VIEW SERVER STATE TO AppInsightUser
GRANT VIEW ANY DEFINITION TO AppInsightUser
GRANT VIEW ANY DATABASE TO AppInsightUser
EXEC sp_adduser @loginame = 'AppInsightUser', @name_in_db = 'AppInsightUser'
GRANT EXECUTE ON xp_readerrorlog TO AppInsightUser
USE msdb
EXEC sp_adduser @loginame = 'AppInsightUser', @name_in_db = 'AppInsightUser'
EXEC sp_addrolemember N'db_datareader', N'AppInsightUser'
```
USE master
GRANT VIEW SERVER STATE TO "Domain\AppInsightUser"
GRANT VIEW ANY DEFINITION TO "Domain\AppInsightUser"
EXEC sp_adduser @loginame = 'Domain\AppInsightUser',@name_in_db = 'Domain\AppInsightUser'
GRANT EXECUTE ON xp_readerrorlog TO "Domain\AppInsightUser"
USE msdb
EXEC sp_adduser @loginame = 'Domain\AppInsightUser',@name_in_db = 'Domain\AppInsightUser'
EXEC sp_addrolemember N'db_datareader', N'Domain\AppInsightUser'
EXECUTE sp_MSforeachdb 'USE [?]; EXEC sp_adduser @loginame = ''Domain\AppInsightUser'', @name_in_db = ''Domain\AppInsightUser'''

Domain account with Orion agent

To use a domain account with an Orion agent, the domain account needs to have "Log on as a batch job" policy enabled for the default batch execution mode. Set this permission either locally on the monitored SQL server or as a domain policy (which enforces the policy to all machines within the domain). For details on this batch mode, see this Microsoft Technet article: https://technet.microsoft.com/en-us/library/cc957131.aspx

ℹ️ This policy is only enabled for a LocalSystem account by default and explicitly needs to be added for the domain account.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

The location for the policy is Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment.

If you have issues, see Use a domain user to monitor AppInsight for SQL through an agent.
Monitor an SQL named instance with AppInsight for SQL

A named SQL instance is an SQL server given a name consisting of the network name of the server plus the instance name specified during installation. To monitor SQL named instances in SAM with AppInsight for SQL, you need the Virtual IP (VIP) of the SQL server and the full name.

Before adding the server as a node, verify the credentials and permissions are configured on the target SQL server.

To view monitored nodes, access the SQL Server page and specific SQL server details pages. See AppInsight for SQL for details.

Locate the VIP for the server

If you do not know the VIP, ping the server through the following instructions.

1. Open a command prompt.
2. Ping the server name: ping NAME.
3. Make note of the returned IP. You will use this IP when adding the server as a monitored node.
4. Close the command prompt.

Add the node manually with AppInsight for SQL

With the VIP, add the named SQL instance as a node for monitoring. These instructions manually add the node. You can also use the Discovery Wizard. For details, see Add AppInsight for SQL to a node.

1. On the Web Console, click Settings > All Settings > Add Node.
2. Enter the VIP address for the SQL named instance for the Polling Hostname or IP Address.
3. Select a polling method, then select the polling engine for that node.
4. On the Choose Resources panel, check the appropriate AppInsight Application for the SQL server you will monitor.

5. Complete the steps making selections as desired such as specific metrics or custom pollers.

6. Review and adjust any settings and click Add Node.

7. Navigate to the All Applications resource and click your AppInsight for SQL application. The Enter Credentials screen displays.

8. Enter your SQL credentials and select a port (or use the default port).

9. Click Test to verify the credentials and configured permissions.

10. Click Assign Credential to save and complete configuration.
Monitor clusters with AppInsight for SQL

Your environment may include clustered SQL servers in your environment, such as for high availability. These clustered SQL servers can be added and monitored with AppInsight for SQL through SAM.

Agents do not work to poll AppInsight for SQL when the SQL server being monitored is in a cluster.

Before adding the server as a node, verify the credentials and permissions are configured on the target SQL server.

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

To view monitored nodes, access the SQL Server page and specific SQL server details pages. See AppInsight for SQL for details.

This instance is grayed until the poller has polled this node. Once polled, the status color updates.

First, you need the IP address of the cluster.

1. Connect to the instance that you want to monitor using SQL Management Studio.
2. Execute the following query to make sure you have the proper target node and instance name:
   ```sql
   SELECT SERVERPROPERTY('ServerName')
   ```
3. Determine the IP address of the target node.
   Open a command prompt and ping the server: `ping NAME`. For example, `ping P111SQLV23` in the following example. The IP address is determined to be 10.1.70.123.
Next, add the node and assign AppInsight for SQL.

1. On the Web Console, click Settings > All Settings > Add Node.
2. Enter the IP address for the SQL cluster for the Polling Hostname or IP Address. If the IP address represents a cluster, the node name of the active cluster member populates. SolarWinds recommends changing the node name to something more easily understood during the final step of the Add Node Wizard. For example, for this cluster you could enter the name and (cluster): P11SQLV23 (cluster).
3. Select a polling method, then select the polling engine for that node.
4. On the Choose Resources step, check the appropriate AppInsight Application for the SQL server to monitor.

5. Complete the wizard as instructed to add the node for monitoring.
6. Navigate to the All Applications resource and click your AppInsight for SQL application. The Enter Credentials screen displays.
7. Enter your SQL credentials and select a port (or use default port).
8. Click Test to verify the credentials and configured permissions.
9. Click Assign Credential to save and complete configuration.
Edit the AppInsight for SQL template

The AppInsight for SQL template includes numerous component monitors for providing data on all AppInsight monitored SQL instances. If you modify these settings and configurations, the details in AppInsight update to match. For full information on the template and component monitors, see the AppInsight for SQL template.

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

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Check the AppInsight for SQL template in the list and then click Edit.
3. From here, you can edit specific component monitors within the template.
   Each component monitor has different settings and options including threshold values, number of records to retrieve, and component monitor description.
4. When done editing, click Submit.

On the AppInsight details page, you can modify the listed resources. Each resource provides data configuration and display options, consuming data provided by the template application and component monitors.

1. From the resource, click Edit in the upper right-hand corner of the resource.
2. Select resources as needed, then click Submit.

Pertinent data for each resource is grouped together by default.

Monitor with other SQL application templates

If you want to monitor without using AppInsight for SQL for specific nodes, SolarWinds recommends using SQL templates.

For example, you may have a large amount of SQL database instances to monitor such as a service provider with SQL instances per customer. For performance, you may not want an AppInsight for SQL running for each of these instances.

To monitor these SQL named instances, add the SQL instance as a node. For details, see the following options. Do not select the option for AppInsight for SQL during node creation.

After added, assign and modify specific templates or application monitors to those nodes. For a list of available templates, see SAM Component Monitor Types and SAM Template Reference.

1. Click Settings > All Settings > SAM Settings > Manage Templates.
2. Search or browse for SQL Server templates.
3. Select the SQL Server template you want to assign to SQL named instances to monitor. You may want to assign multiple templates to the node. Assign these one at a time.
4. Once assigned, you can edit one or more templates by checking the boxes and selecting MultiEdit.
5. Enter the SQL named instance for the SQL Server Instance.
6. You can further modify the templates and application monitors as needed. Data captured through the templates should display on the Node Details for those monitored nodes.

All component or application monitors in a template relate to the SQL named instance, not the server. In Microsoft, the SQL server is a series of instances. These instances are default, unnamed instances or specifically named SQL instances. An instance is an installed Microsoft SQL in a specific directory path.
Manage application monitor templates and component monitors

SAM includes a number of out-of-the-box templates to assign to nodes as needed. Templates include component monitors for specific applications or for scripts, grouped by application categories. SolarWinds recommends creating a copy of these templates to customize, remove, or add component monitors.

You can also create, modify, and configure Application Monitor templates for customized monitoring. To create templates:

- Create new templates using copies of OOTB templates
- Create a template from scratch
- Import and customize templates from THWACK

To work with templates and monitors, see the following:

- Manage templates
- Modify and customize monitors
- Monitors and templates using WMI
- Assign and edit application monitors to nodes
- Create component monitors from the Component Monitor Wizard
- Scan for applications to monitor
- Manage templates and groups
- Unmanage and manage assigned application monitors
- Script custom component monitors
- Application Monitor Thresholds
- Example tasks for application monitors
For details on application templates and monitors, see [SAM Component Monitor Types](#) and [SAM Template Reference](#).

**Component Monitors**

Component monitors are the building blocks of SolarWinds SAM. Each monitors the status and performance of a different aspect of an application. There are several different types of component monitors, each containing settings that define what is monitored and how to monitor it.

Some types of component monitors allow you to set threshold conditions on the monitored parameters. You can set separate thresholds to indicate warning and critical conditions. For example, if you are monitoring the percentage of free space remaining on a volume, you can set a warning threshold at 15%, and a critical condition at 5%.

As an analogy, pretend SolarWinds SAM is monitoring a car. You would have component monitors to check tire pressure, engine RPM, water temperature, battery voltage, and other important subsystems of that vehicle. You can set alerts to give notification if the water gets too hot, or if the battery voltage drops too low.

**Application Monitor Templates**
A template is a group of component monitors modeling the total availability and performance level of an application. A complicated application such as Windows Server may require dozens of component monitors to accurately assess its current status and performance.

Instead of creating component monitors one-by-one for every application server, you can assign a pre-made template. The template can either be one included with SolarWinds SAM, or a custom template you make yourself. For example, you can assign the included Microsoft Windows Server 2003-2008 template to your Windows 2003 and Windows 2008 computers and obtain vital statistics on all of them.

A template is only a blueprint and does not perform any monitoring on its own. Only after assigning the template to a server node are active assigned component monitors created.

To continue the car analogy, pretend you want to monitor a fleet of 50, 2010, blue Dodge Charger automobiles. Instead of defining the component monitors for 50 cars, you can define all the component monitors in a Dodge Charger template.

**Assigned Component Monitors**

Assigned component monitors are created by assigning Application Monitor templates to server nodes. Each actively monitors its assigned node according to its settings. Component monitors inherit these initial settings from the template. If you make a change to a template, that same change is rolled out to all assigned Application Monitors based on the template.

You can override the template settings at any time, breaking the inheritance relationship between the component monitor and its template. For example, the user name and password usually differ for each node, and you would select a different credential for each assigned Application Monitor, thus overriding the template setting for the Credentials field.

To restore the inheritance relationship between a component monitor and its template, click Inherit From Template next to the setting.

Continuing the car analogy, when you assign the Dodge Charger template to a Dodge Charger vehicle, you now have a set of assigned component monitors for monitoring the vehicle’s tire pressures, engine RPM, and so forth.

**Assigned Application Monitors**

An assigned Application Monitor runs its assigned component monitors at regular intervals, and then uses the status results from the component monitors to determine an overall status for the application.

If some of the component monitors are up and others are down, the Application Monitor follows the Status Rollup Mode setting in the SolarWinds Web Console Settings to show either the worst status of the group or a warning status.

The difference between an assigned Application Monitor and a template is that the template is only a blueprint and does not perform any monitoring on its own. Only after assigning the template to a server node does SolarWinds SAM conduct any actual monitoring on the node.
To complete the car example, you assign the Dodge Charger template to all the Dodge Charger vehicles to create the assigned Application Monitor for determining the overall status for your Dodge Charger fleet. For example, the fleet may be 95% available at a given time due to warnings for some of the cars.

The following diagram illustrates the work flow involved in creating an application to be monitored by SAM.
Manage templates

You can create a new template, copy a current template, or manage existing templates. You can access existing templates, assigned monitors, and THWACK via the All Settings > SAM Settings > Manage Templates page.

ℹ️ You may need to log in with an administrator account to perform these actions.

To manage templates, you can:

- Create a template, including a SolarWinds Windows Services template
- Assign a template to a node
- Edit a template
- Copy a template
- Export and import templates
- Delete templates
- Tag a template
- Change between 32-bit and 64-bit polling

Create a template

You can create a template through the SAM Settings page or when managing templates. Creating a new template does not include any configured settings beyond the defaults for polling frequency and timeout (300).

To quickly create a template with multiple instance of a component monitor, use the Component Monitor Wizard.

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates > Create New Template.
2. Add general information and settings for the template including the name, description, tags, and polling frequency.
3. You have two options for adding component monitors. You can select Manually Add Component Monitors (select and add, editing in the template view) or Browse for Component Monitors (opens the Component Monitor Wizard). When added, you can modify the configurations and custom settings per monitor. For details on each monitor, you can access the help link. See Component Monitor Types.
4. When done, click Submit to save the changes.

Make sure the name of the template does not begin or end with a space. If so, application resources may not list all applications. Edit the template name to remove any extra spaces in the name.

Create a custom template (Example)

The following procedure creates a SolarWinds SAM Application Monitor template that monitors a locally installed SQL Server instance. The template is simplified by using the Windows Service component monitors, a TCP port monitor for your SQL Server, and an HTTP monitor for the local Web Console.

Create an application template with the following component monitors:

- TCP port component monitor to monitor port 1433, the port through which SolarWinds communicates with the SQL Server.
- Service component monitors for the following windows services:
  - SolarWinds Alerting Engine
  - SolarWinds Network Performance Monitor
  - SolarWinds Job Engine
  - SolarWinds Job Scheduler
  - SolarWinds Module Engine
  - SolarWinds Syslog Service
  - SolarWinds Trap Service
- HTTP component monitor to monitor port 80, the port through which you access the SolarWinds Web Console.

Create a SolarWinds Windows service application template

You can create templates specifically for the following SolarWinds Windows services:

- SolarWinds Network Performance Monitor
- SolarWinds Job Engine v2
- SolarWinds Job Scheduler
- SolarWinds Module Engine
- SolarWinds Syslog Service
- SolarWinds Trap Service

When creating the templates, use these instructions with variations based on the services you are monitoring:

1. On the Web Console, click Settings > All Settings > SAM Settings > Create New Template.
2. Add general information to the template including a name, description, and tags. Tags are used for searching or opening lists of templates per tag.
3. Click Add Component Monitor, expand the Network Protocol Component Monitors list, and select TCP Port Monitor. Click Submit to add.

4. Click Rename and name the TCP port monitor, and click OK.

5. Ensure the Port Number field corresponds to the port used to communicate with the SolarWinds SQL Server instance. By default, this is port 1433.

6. Click Add Component Monitor, expand the Process and Service Component Monitors, and check Windows Service Monitor and click Submit.

7. Click Rename, name the SolarWinds Alerting Engine monitor, and click OK.

8. Enter or select the credential set to use when accessing the Windows service information.

9. Enter the name of the SolarWinds Alerting Engine service in the Net Service Name field.

10. Click Add Component Monitor then expand the User Experience Component Monitors list, and then check HTTP Monitor.

11. Click Rename, name the HTTP port monitor, then click OK.

12. Ensure the Port Number field corresponds to the port you use for the SolarWinds Web Console port, then click Submit.

Assign a template to a node

To begin monitoring with templates, you need to assign the application templates and monitors to a node. When assigned and enabled, the template collects and reports on polling data to the node according to the application monitors and configuration settings. To add nodes, see [Discover and add network devices](#).

To assign templates to nodes:

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Check the template(s) to assign, and click Assign to Node.
3. Specify the node(s) to monitor and click Next.
4. Enter or select the appropriate credentials.
5. Click Assign Application Monitors.

Edit a template

Every template, including default SAM templates, can be modified. You can change the name, description, general settings, and application monitors. You can also create a copy of a template and modify the copy.

1. On the Web Console, click Settings > All Settings > Settings > Manage Templates.
2. Check an application template and click Edit.
3. Specify the values for the Polling Frequency and Polling Timeout fields.

   Setting a polling frequency below 30 seconds can result in erratic monitor behavior.

4. To add a monitor, click Add Component Monitor. Expand and filter through the options to add one or more monitors to the template.
5. You can edit one or more monitors, update settings per monitor, and more. See Modify and customize monitors for details. To review help information per monitor, use the help option in the web console.

6. When done, click Submit to save the changes.

**Copy a template**

You can modify current templates, or create a copy. With copies, you can use a base template from the default templates, imported templates, or templates you created. Using a copy for a new template can make the process much faster than starting a new template without pre-filled monitors and configurations.

The copied templates use the same name of the original name with "- Copy" appended.

> If you want to completely modify a current template, use a copy to keep the original.

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Select the application template you want to copy, and click Copy. A new template is added copying all of the application and component monitors, including any configured settings.

**Export and import templates**

Templates can be exported and imported to share and use between all Orion users. Exporting templates creates a file you can share on thwack with other users.

> Ensure the imported file format is XML with .apm-template extension. Unzip templates before importing.

**To export to THWACK:**

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

1. On the Web Console, click Settings > All Settings > SAM Settings, and click Manage Templates.
2. Browse or select for a template in the list.
3. Click Import Export > Export to THWACK.
4. Enter your THWACK account credentials when prompted. If you need an account, click Create Account and follow the steps.

To export to a file:

1. On the Web Console, click Settings > All Settings > SAM Settings, and click Manage Templates.
2. Browse or select for a template in the list.
3. Click Import Export > Export as File, and click Save. The template packages into a file with an extension .apm-template. You can also post a zip file of templates if needed.
4. To share the template, visit the Application Monitor Templates folder on THWACK.
5. Click Write a document, add a title and description for the template, and attach the .apm-template file.
6. Add apm_monitoring_template in the Tags field.
7. Select Application Monitor Templates in Categories.
8. Click Publish to post the information and template.

To import templates from THWACK:

1. On the Web Console, click Settings > All Settings > SAM Settings, and click Manage Templates.
2. Click the Shared Templates on THWACK tab. A page opens and populates with available templates from THWACK.
3. Search or browse the templates. Select a template file and click Import. To view information per template from the authors, click the link for content exchange area on THWACK.
4. Enter your THWACK account credentials when prompted.

![THWACK LOG IN DIALOG](image)

5. The template imports into the Orion Web Console. Search or browse to locate and edit the template as needed.

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

If you receive an invalid file error, check the file format. The template should be XML code with `.apm-template` extension. If you are importing a ZIP, unzip the contents then import the template file.

**To import templates from file:**

You can download templates and import templates from your local computer using the Import option. You can locate these templates on THWACK. If the template is in a .zip file, extract the zip and verify it is XML and has an extension of `.apm-template`. If not, you will receive an invalid file error.

1. On the Web Console, click Settings > All Settings > SAM Settings, and click Manage Templates.
2. Click Import/Export, and click Import.
   A page opens to browse and select the file.
3. Browse and select the template file from your local drive.
4. Click Submit.
   SAM checks the file type and format.
5. The template imports into the Orion Web Console. Search or browse to locate and edit the template as needed.

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

Deleting a template also deletes all of its assigned applications, both modified and unmodified. To speed up user interface interaction, data is not immediately removed from the database, but systematically updated every few minutes in the background.

If you may want to use the template at a later time, export to the template to file to save a backup. You can later import the template from file to add it back into SAM.

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Check the template(s) to delete and then click Delete.
3. Confirm deletion by clicking Yes.

Tag a template

Tags are descriptive labels that help you classify and sort your application templates on the Manage Application Monitor Templates page. The application templates included in SolarWinds SAM have already been tagged with several descriptive labels you can modify as you see fit.

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Select the templates you want to tag, then click Tags.
3. Click Add existing tag(s) or select the tags from the list.
4. Type the tags, separating multiple tag entries with commas, then click Submit.

To remove tags:

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Select the templates you want to tag, then click Tags > Remove Tags.
3. Select the tags from the list, then click Submit.

Change between 32-bit and 64-bit polling

You should use 64-bit polling on 64-bit OS systems. Using AppInsight applications with 32-bit polling on 64-bit computers via an agent prevents certain performance counters from collecting information.

You may need to log in with an administrator account to perform these changes.

Change to 64-bit polling at the application resource level:

1. On the Web Console, click My Dashboards > Applications > SAM Summary.
2. Select an AppInsight Application (Exchange, SQL, IIS) and then click Edit Application Monitor.
3. Expand Advanced, and then click Override Template.
4. In the Platform to run polling job field, change the value to x64.
5. Click Submit.
Change to 64-bit polling at the template level:

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Select an AppInsight application and click Edit.
3. Expand Advanced, and in the Platform to run polling job on field, change the value to x64.
Modify and customize monitors

Through the Manage Application Templates page, you can modify default and new templates. Every template consists of one or more application or component monitors. You can modify each of these monitors one at a time or in multi-edit.

You can access the help information per monitor through the Orion Web Console for more information.

For details on supported templates, see:
- Monitors and templates using WMI
- SAM Template Reference

You can edit each monitor or select more for multi-editing, add new monitors, and disable or delete templates. To begin collecting data, these monitors and templates need to be assigned to a node.

To modify the specific configurations per monitor, you should edit each monitor individually. The multi-edit function only updates shared settings between the selected monitors. See Component Monitor Types.

Multi-edit components

You can simultaneously edit multiple component monitors within a template. You can select multiple monitors using the checkboxes to modify, without needing to be of the same type. To reorder the monitors, drag and drop them in the table view. You can perform the following types of multi-edit options:

- Multi-Edit: A prompt displays with editing options specific to the type of monitors selected. For example, the Fetching Method for the three Services selected can be changed from RPC to WMI.

- Assign Credentials: Modify the credentials as needed for the selected monitors.
- Test: Run a communication test on the monitors using agent or agentless communication as configured.
- Set Test Node: Modify the test node for communication tests.
- Disable/Enable: Start and stop polling for the monitor.
- Delete: Permanently removes the monitor.
When editing a template, the green arrows to the right of each component monitor, highlighted below, lets you to change the order of each monitor. This new order is respected only on the All Applications resource and the Application Details resource.

You may need to log in with an administrator account to perform these actions.

Delete or Disable a monitor

You can disable or delete application monitors as needed. When you disable, the monitor remains in the Orion Web Console without communicating and collecting data. You can disable one or monitors.

- If you want to stop all monitoring using the monitor, click Disable.
- If you want to monitor using the monitor again, select and click Enable.

If you no longer want the monitor in the template, you can delete to permanently remove it from the Orion Web Console.

1. When editing a template, select the monitor you want to remove.
2. Confirm by clicking Yes. The monitor is permanently removed from the template.

Linux/Unix system configurations for component monitors

To effectively monitor Linux/Unix systems with the Orion agent for Linux/Unix, consider and complete the following configurations for component monitor and templates. You may need to reference vendor documentation, as well as work with your NOC and server management groups to complete modifications.

This information is also included with the [SAM Component Monitor Types](https://www.solarwinds.com) and [SAM Template Reference](https://www.solarwinds.com).

- Apache configurations
- Tomcat configurations
- JMX
- Squid
- Nagios
- ODBC configurations
- PostgreSQL
- MySQL
- IBM DB2 with ODBC

Apache configurations

You should have the following packages installed:

- Apache `httpd`
- `LWP::UserAgent` (Perl)

To install and configure:
1. Login to your Apache server using SSH or telnet client. Grant yourself root permissions (so root).
2. Use the command: `yum install perl-libwww-perl`
3. Locate `httpd.conf`: `find /etc -iname httpd.conf`. The file is typically located in `/etc/httpd/conf/httpd.conf`.
4. Locate the following section:

```bash
#<Location /server-status>
#   SetHandler server-status
#   Order deny,allow
#   Deny from all
#   Allow from .example.com
</Location>
```

5. Uncomment the code. Edit the `Allow from` rule, substituting the IP address or hostname of your Apache server for localhost. Use localhost only if the Apache server services the loopback interface. Also make sure the `ExtendedStatus` is On.

```bash
<Location /server-status>
SetHandler server-status
Order deny,allow
Deny from all
Allow from localhost
</Location>
ExtendedStatus On
```

6. Restart the Apache: `service httpd restart`
   or
   Reload the configuration: `service httpd reload`

**Tomcat configurations**

Apache Tomcat is an open-source web server, implementing several Java EE specifications.

The following information walks through installing and configuring Tomcat servers to work with SAM component monitors. If you have Tomcat installed, you can skip to step 4 to create an account used for polling.

1. Determine the version of Tomcat you want to install. You may have multiple versions available to install. To locate all versions, use this command:

   ```bash
   yum search tomcat
   ```
2. After determining the version, you can install the tomcat package and the admin webapps package. Locate the versions to install from the search results. For example:

```
tomcat5.i386 : Apache Servlet/JSP Engine, RI for Servlet 2.4/JSP 2.0 API
tomcat5-admin-webapps.i386 : The administrative web applications for Jakarta Tomcat
```

3. Install the versions using the located versions. To install the example above:

```
yum install tomcat5 tomcat5-admin-webapps
```

4. Next, you need to modify the tomcat-users.xml file to create and provide a user account to access the web manager ('manager','manager-gui'). To locate, use this command:

```
find /etc -iname tomcat-users.xml
```

5. Edit the file and locate the `<tomcat-users>` section. If commented out, uncomment the configuration. Edit to add a user of tomcat with the password of tomcat. The template uses this account to access data.

```
<tomcat-users>
  <user name="tomcat" password="tomcat" roles="tomcat,manager,manager-gui" />
  <user name="role1" password="tomcat" roles="role1" />
  <user name="both" password="tomcat" roles="tomcat,role1" />
</tomcat-users>
```

6. Restart the service. The command depends on the version you installed. For example, this command restarts the installed service above:

```
service tomcat5 restart
```

### JMX

For JMX configurations, you need to install and configure WebSphere per your Linux/Unix distribution. For details, see the [IBM WebSphere documentation site](http://www-01.ibm.com/support/docview.wss?rs=895&context=SSGT7452&cc=us&lang=en&vid=0000000000514961).

The overall steps include:
1. Get and install WebSphere. You may require credentials for the installation.
2. During installation, you can turn off the secure storage option as this is not needed. You may need to create a new package group. Make sure to select the Application Server during installation. You may also need to create an administrator account.
3. Start and stop the WebSphere AppServer.
4. Access the WebSphere AppServer console to continue configurations. You can access by pointing a browser to http://<websphere-host>:9060/ibm/console. You may need to open a port to 9060 on the websphere host. Use the credentials for the account created during installation.
5. You need to expose the JMX platform mbeans in the WebSphere AppServer using the console. Click Servers > Server Types > WebSphere application servers and select the listed application server.
6. Locate the Java and Process Management > Process definition. In the dialog box titled "Generic JVM arguments" enter the following:

   ```
   Djavax.management.builder.initial=  
   i There is nothing after the = sign.
   Dcom.sun.management.jmxremote=true
   Dcom.sun.management.jmxremote.port=8686
   Dcom.sun.management.jmxremote.ssl=false
   Dcom.sun.management.jmxremote.authenticate=false
   Djava.rmi.server.hostname=localhost
   ```

7. Restart the AppServer.

**Squid**

Squid is a caching and forwarding web proxy. It has a wide variety of uses, from speeding up a web server by caching repeated requests; to caching web, DNS and other computer network lookups for a group of people sharing network resources, to aiding security by filtering traffic.

To configure Squid for agent polling:

- **SNMP is required** - Enable the SNMP feature for Squid. If using Squid-3, this feature is available to enable by adding a configuration option to squid.conf. If using Squid-2, you will need to enable the feature using a series of scripts then configure.
- **perl-switch is required** - Add per your Linux distribution vendor's documentation.

Review your vendor documentation for details at http://www.squid-cache.org/.

**Nagios**

Nagios monitors systems, networks, and infrastructure. It offers monitoring and alerting servers, switches, applications, and services. Refer to your vendor’s documentation to properly install and configure Nagios according to your Linux distribution.

You can use the Nagios Script monitor and Linux/Unix Script monitor for monitoring Nagios.
If you are using this component monitor with Nagios and polled by Orion agent for Linux, you need to enter a script as follows. The argument would be python $(SCRIPT) with a body of:

```python
def random_statistic(stat_id):
    print('Statistic.random%d: %d Message.random%d: %s' % (stat_id, randint(1,100), stat_id, 'random number: ' + str(randint(1,100))))
```

**ODBC configurations**

To monitor a database with an ODBC connector, you need to install an ODBC driver for your installed database type, create a user, and test access. Use the new account credentials in your SAM template and component monitors. For a full list of available templates, see [SAM Template Reference](https://www.solarwinds.com/support/article/SMP11014).

For the following instructions, you should have a database installed such as MySQL or PostgreSQL.

1. (Required) To begin, you should have unixODBC installed to support Microsoft Windows ODBC. If not, download and install the unixODBC driver to the Linux/Unix-based computer.
2. Install the DBMS driver.
3. Download and install an ODBC driver for your installed database type.
4. Create a user account for the database.
5. Configure the user access privileges with administrative privileges.
6. Test access to the database using the newly created account credentials.

Configure and assign a SAM template with the credentials.

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Search for a template based on the database type such as ODBC or Oracle. SolarWinds recommends creating a copy of the template. Select a template and click Copy.
3. Modify the settings of the template and component monitors based on the metrics you want to monitor.
4. To enter credentials, select the component monitor checkboxes and click Assign Credentials.
5. Enter the credentials you created for the database and click OK.
6. Test the access for the template by assigning it to a node. Click Test Node to assign and test the access. If you encounter issues, verify the credentials and privileges for the account.

**PostgreSQL configurations**

To monitor a PostgreSQL database server with component monitors, you need to install an ODBC driver, create a user, and test access. Use the new account credentials in your SAM template and component monitors.

SAM provides a [PostgreSQL template](https://www.solarwinds.com/support/article/SMP11014) and component monitors for PostgreSQL 9.
For the following instructions, you should have PostgreSQL installed on a Linux-based computer.

1. Login to the Linux-based computer with administrator privileges. You will need to create a user account on the server and in the PostgreSQL database.

2. (Required) To begin, you should have unixODBC installed to support Microsoft Windows ODBC. If not, download and install the unixODBC driver to the Linux-based computer.

   Command: `yum install unixODBC`

3. Download and install the PostgreSQL ODBC driver on the target Linux-based computer.

   Command: `yum install postgresql-odbc`

4. Create a user account for the database.
The example of commands adds a user account dbuser with the password Password1 to the Linux-based computer. The next commands login as the database superuser to the PostgreSQL server and modify the created user.

   ```
   # adduser dbuser
   # passwd Password1
   # su - postgres
   $ psql -d template1 -U postgres
   ```

   At the prompt, create the dbuser account with the Password1 password:

   ```
   template1=# CREATE USER dbuser WITH PASSWORD 'Password1';
   ```

   Next, grant privileges for your PostgreSQL database (TestDatabase) to the user account:

   ```
   template1=# GRANT ALL PRIVILEGES ON DATABASE TestDatabase to dbuser;
   ```

   Close the template:

   ```
   template1=# \q
   ```

5. Test access to the database using the newly created account credentials.

   ```
   $ su - dbuser
   $ psql -d TestDatabase -U dbuser
   ```

Configure and assign a SAM template with the credentials.

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Search for the PostgreSQL template. SolarWinds recommends creating a copy of the template. Select the template and click Copy.
3. Modify the settings of the template and component monitors based on the metrics you want to monitor.
4. To enter credentials, select the component monitor checkboxes and click Assign Credentials.
5. Enter the credentials you created for the database and click OK.
6. Test the access for the template by assigning it to a node. Click Test Node to assign and test the access. If you encounter issues, verify the credentials and privileges for the account.

**Troubleshooting**

If you receive the error "FATAL: Peer authentication method failed for user 'postgresuser'", change the authentication method to md5.

**MySQL configurations**

To configure MySQL, you need to install and configure the appropriate MySQL repository, create a user account, and test access. Use the new account credentials in your SAM template and component monitors.

SAM templates include two options for MySQL 5.7.9 and earlier and 5.7.9 and later.

For the following instructions, you should have MySQL installed on a Linux-based computer.

1. Login to the Linux-based computer with administrator privileges. You will need to create a user account on the server and in the MySQL database.
2. (Required) To begin, you should have unixODBC installed to support Microsoft Windows ODBC. If not, download and install the unixODBC driver to the Linux-based computer.
3. Install the MySQL ODBC driver.
   Command: yum install mysql-connector-odbc
4. Create a user account for the database.
   The following commands create a MySQL account of dbuser with the password Password1 for the database dbtest. The commands also grant all access to the user account.

```sql
create database testdb;
create user 'dbuser'@'localhost' identified by 'Password1';
grant all on dbtest.* to 'dbuser' identified by 'Password1';
```
5. (Required) Grant the following access for local access to monitor through SAM and the Orion Platform.
Enter the IP address of this MySQL Linux-based computer, replacing the example value of 10.100.100.100.

```
mysql -uroot -p
CREATE USER 'dbuser'@'%' IDENTIFIED BY 'Password1';
GRANT ALL ON testdb.* TO dbuser@'%' IDENTIFIED BY 'Password1';
GRANT SELECT ON performance_schema.* TO dbuser@'10.100.100.100' IDENTIFIED BY 'Password1';
```

6. Test access to the database using the newly created account credentials. 
   
   **Command:** `mysql -u testuser -p`

Configure and assign a SAM template with the credentials.

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Search for the MySQL templates. SolarWinds recommends creating a copy of the template. Select a template based on version and click Copy.
3. Modify the settings of the template and component monitors based on the metrics you want to monitor.
4. To enter credentials, select the component monitor checkboxes and click Assign Credentials.
5. Enter the credentials you created for the database and click OK.
6. Test the access for the template by assigning it to a node. Click Test Node to assign and test the access. If you encounter issues, verify the credentials and privileges for the account.

**Troubleshooting**

**Error:** Data source name not found and no default driver specified. This error occurs on a CentOS system.

**Solution:** Verify the CentOS system has the mysql-connector-odbc installed. Use the following command to receive a package and version name on the target Linux-based computer: `rpm -q mysql-connector-odbc`

Verify you have the appropriate credentials assigned for each component monitor.

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Search for the SAM template. Select and click Edit.
3. Select the component monitor to check assigned credentials.
4. To modify, click Assign Credentials, enter credentials, and click OK.
5. Test the template.
If you continue to encounter issues, verify the appropriate driver is defined on the CentOS system to match the connection string.

For example:

```bash
cat /etc/odbcinst.ini
[MySQL]
Description=ODBC for MySQL
Driver=/usr/lib/x86_64-linux-gnu/odbc/libmyodbc.so
Setup=/usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
UsageCount=1
[MySQL ODBC 5.3 Unicode Driver]
Driver=/usr/lib/x86_64-linux-gnu/odbc/libmyodbc.so
Setup=/usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
UsageCount=1
```

IBM DB2 with ODBC configurations

For IBM DB2, you need to download, install, and configure DB2. For details, see the IBM DB2 documentation site.

SAM provides two IBM DB2 templates: **IBM DB2** and **IBM DB2 HADR Health**.

Linux-based computers

For the following instructions, you should have IBM DB2 installed on a Linux-based computer. To run commands, you will need the instance users for the database. The instance user connects to the DB and should have the sqllib directory set up.

1. Login to the Linux-based computer with administrator privileges.
   You will need to create a user account on the server and in the IBM2 database.

2. Install the unixODBC package.
   Command: `yum -y install unixODBC`

3. Update the ODBC config files. Add the following settings to `/etc/odbcinst.ini`:
   ```ini
   [DB2]
   Description = DB2 Driver
   Driver = /opt/ibm/db2/V10.5/lib64/libdb2.so
   FileUsage = 1
   DontDLClose = 1
   
   i Verify libdb2.so has the correct file path.
   ```

4. Add the following settings to `/etc/odbc.ini`:
   ```ini
   [dbname]
   Driver = DB2
   
   i The drivers should match in both files.
   ```
5. Connect locally to the database with the instance user credentials. For example:
   isql -v dbname db2inst1 Password1

6. Log into the DB2 database with the instance user credentials and open the DB2 command line tool.

7. Enable the required following setting used by the SAM IBM DB2 template:
   - UPDATE DBM CFG USING DFT_MON_BUFPOOL ON
   - UPDATE DBM CFG USING DFT_MON_LOCK ON
   - UPDATE DBM CFG USING DFT_MON_STMT ON
   - UPDATE DBM CFG USING DFT_MON_UOW on

8. Grant execute on function SYSPROC.MON_GET_TABLE to the instance user account.
Configure DB2 on AIX devices

Prerequisites

- DB2 ODBC CLI driver from IBM
  The commands use the following driver bundle name: v11.1.1fp1_aix64_odbc_cli_32.tar.gz.
  - info-6.4-1.aix5.1.ppc.rpm
  - libiconv-1.15-1.aix5.1.ppc.rpm
  - libtool-ltdl-1.5.26-2.aix5.1.ppc.rpm
  - readline-7.0-3.aix5.1.ppc.rpm
  - libffi-3.1.1.aix5.1.ppc.rpm (not a direct dependency, but needed by the SAM monitor plugin)
- gunzip utility
- IBM rpm.rte package: verify that /usr/bin/rpm utility exists

Configure ODBC for AIX

1. Log in to the AIX-based computer with administrator privileges.
2. Install the RPM packages.
   Run the following command as root: rpm -ivh unixODBC-2.3.4-1.aix5.1.ppc.rpm
   To install all dependencies, run the following command. The command expects that the dependencies are in the same directory.
   ```sh
   rpm -ivh *.rpm
   ```
3. Install the DB2 ODBC driver. The example code creates a directory odbc_cli_32 in the /opt directory.
   ```sh
   gunzip v11.1.1fp1_aix64_odbc_cli_32.tar.gz
tax -x -f v11.1.1fp1_aix64_odbc_cli_32.tar -C /opt
   ```
4. Add the following settings to /etc/odbcinst.ini:
   ```ini
   [DB2]
   Description = DB2 Driver
   Driver = /opt/odbc_cli_32/clidriver/lib/libdb2.so
   FileUsage = 1
   DontDLClose = 1
   ```
   Verify libdb2.so has the correct file path.
5. Add the following settings to /etc/odbc.ini:

```ini
[dbname]
Description = IBM DB2 ODBC data source
Driver = DB2
DMEnvAttr = SQL_ATTR_UNIXODBC_ENVATTR=/opt/odbc_cli_32/clidriver
```

- In [dbname], enter the name of the database to be monitored.
- DMEnvAttr value depends on the installation directory for the DB2 ODBC CLI driver.

6. Run the following command as root. It allows the unixODBC manager driver to find the DB2 ODBC file.

```bash
ar -X32 x libdb2.a shr.o
mv shr.o libdb2.so
```

7. Verify that SAM python plugin can connect to the DB2 database to monitor. Save the following script as verifyodbc.py.

The script is written for Agents in the default location /opt/SolarWinds/Agent.

```python
import sys
sys.path.insert(0, "/opt/SolarWinds/Agent/bin/Plugins/SharedPythonLibs")
import pypyodbc

# Set Database, Uid, and Pwd to the database name, username, and user's password to access said database respectively.
# In this example, database name, username, and the user's password are TEST, db2inst1, and Password1 respectively.

conn_str = 'Driver={DB2};Database=TEST;Uid=db2inst1;Pwd=Password1;'

try:
    conn = pypyodbc.connect(conn_str, ansi=True)
    conn.close()
except Exception, ex:
    print ex
    print "Failure"
```

8. Run the script using the following command:

```bash
/opt/SolarWinds/Agent/bin/python2 verifyodbc.py
```
9. SolarWinds recommends that you configure the utilities bundled in the DB2 ODBC CLI bundle. Create the `db2cli.ini` configuration file in `/opt/odbc_cli_32/clidriver/cfg/db2cli.ini`:

```
[db2]
Database=TEST
dbaalias=TEST
Protocol=TCPIP
Hostname=127.0.0.1
ServiceName=50000
```

Replace TEST with your database name.

Configure and assign the SAM IBM DB2 template to your Linux/Unix-based computer with the instance user credentials.

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Search for a IBM DB2 template. SolarWinds recommends creating a copy of the template. Select a template based on version and click Copy.
3. Modify the settings of the template and component monitors based on the metrics you want to monitor.
4. To enter credentials, select the component monitor checkboxes and click Assign Credentials.
5. Enter the credentials for the instance user account and click OK.
6. Modify the connection strings for monitors to match your DB. Use one of the following methods:
   - **Specify the actual DB and driver:**
     ```
     Driver={DB2};Database=TESTDB;Hostname=${IP};Port=50000;Protocol=TCPIP;Uid=${USER};Pwd=${PASSWORD};
     ```
   - **Specify the existing data source in odbc.ini:**
     ```
     DSN=testdb;Uid=${USER};Pwd=${PASSWORD};
     ```
Monitors and templates using WMI

These lists provide the component monitors and templates that use and support WMI.

Microsoft Windows by default uses a random port between 1024 and 65535 for WMI communications. You must create firewall exceptions to allow TCP/UDP traffic on ports 1024 - 65535 or the component monitors and templates that use WMI will not work.

Component monitors using WMI

- Performance Counter Monitor
- Process Monitor – Windows (if script uses WMI access)
- Windows Event Log Monitor
- Windows PowerShell Monitor (if script uses WMI access)
- Windows Script Monitor
- Windows Service Monitor (if script uses WMI access)

Templates using WMI

For information on these templates, see the template reference.

- Active Directory 2003-2008 Services and Counters
- Active Directory 2008 R2 - 2012 Services and Counters
- Apache (Windows)
- APC PowerChute Agent (Windows)
- AppInsight for Exchange
- AppInsight for IIS
- AppInsight for SQL
- BizTalk Server 2010-2013 Adapters Performance Counters
- BizTalk Server 2010-2013 Host Throttling Performance Counters
- BizTalk Server 2010-2013 Message Box and Orchestrations Performance Counters
- BlackBerry Delivery Confirmation
- BlackBerry Enterprise Server
- BlackBerry Enterprise Server 10 Services (Windows)
- CiscoWorks LAN Management Solution
- Citrix XenApp 5.0 Core WMI counters
- Citrix XenApp 5.0 ICA Session WMI counters
- Citrix XenApp 5.0 Presentation Server WMI counters
- Citrix XenApp 5.0 Services
- Citrix XenApp 6.0 Core counters
- Citrix XenApp 6.0 ICA Session
- Citrix XenApp 6.0 Presentation Server
- Citrix XenApp 6.0 Services
- Distributed File System (DFS)
- Errors in Application Event Log
- Exchange 2007 Client Access Role Counters (Advanced)
- Exchange 2007 Edge Transport Role Counters (Advanced)
- Exchange 2007 Hub Transport Role Counters (Advanced)
- Exchange 2007 Mailbox Role Counters (Advanced)
- Exchange 2007 Unified Messaging Role Counters (Advanced)
- Exchange 2016 Client Access Role Services and Counters (Basic)
- Exchange 2016 Common Performance Counters
- Exchange 2016 Edge Transport Role Service and Counters (Basic)
- Exchange 2016 Hub Transport Role Service and Counters (Basic)
- Exchange 2016 Unified Messaging Role Service and Counters (Basic)
- Exchange 2016 Client Access Role Counters (Advanced)
- Exchange 2016 Edge Transport Role Counters (Advanced)
- Exchange 2016 Hub Transport Role Counters (Advanced)
- Exchange 2016 OWA Form Login (PowerShell)
- Exchange 2016 Unified Messaging Role Counters (Advanced)
- Exchange 2013 Client Access Role Counters (Advanced)
- Exchange 2013 Client Access Role Services and Counters (Basic)
- Exchange Active Sync Connectivity
- Exchange Server 2000 and 2003
- File Count Script
- GoodLink Server for Microsoft Exchange
- Group Policy Object (System and Application Logs)
- Helix Universal Media Server (Windows)
- Internet Information Service (IIS) 6
- JD Edwards EnterpriseOne Server Manager (Windows)
- Kaspersky Security Center Antivirus
- Kiwi Syslog Server
- Log Parser (PowerShell)
- Microsoft DirectAccess 2008 R2
- Microsoft DirectAccess 2012
- Microsoft DirectAccess 2012 R2
- Microsoft DirectAccess 2012-2012 R2 (Health with PowerShell)
- Microsoft Dynamics CRM 4.0 Events
- Microsoft Dynamics CRM 4.0 Statistics
- Microsoft Dynamics CRM 2011 Events
- Microsoft Dynamics CRM 2011 Statistics
- Microsoft Forefront Endpoint Protection 2010 Client
- Microsoft Forefront Endpoint Protection 2010 Server
- Microsoft Forefront Threat Management Gateway 2010
- Microsoft IIS SMTP Server
- Microsoft Lync Server 2013 (Edge Role)
- Microsoft Lync Server 2013 (Front-End Role)
- Microsoft Lync Server 2013 (Mediation Role)
- Microsoft Lync Server (Edge Role)
- Microsoft Lync Server (Front-End Role)
- Microsoft Lync Server (Mediation Role)
- Microsoft Message Queuing Events
- Microsoft Message Queuing Performance
- Microsoft Network Policy Server Events
- Microsoft Network Policy Server RADIUS Proxy
- Microsoft Network Policy Server RADIUS Server
- Microsoft Routing and Remote Access 2008-2012 R2
- Microsoft Routing and Remote Access 2008-2012 R2 (Events)
- Microsoft System Center Configuration Manager 2012
- Microsoft System Center Operations Manager 2012 (Agent)
- Microsoft System Center Operations Manager 2012 (Management Server)
- Microsoft Windows Internet Name Service (WINS) Events
- Microsoft Windows Internet Name Service (WINS) Statistic
- Microsoft Windows Server 2003 Failover Cluster
- Microsoft Windows Server 2008 Failover Cluster
- Microsoft Windows Server 2008 R2-2012 R2 Failover Cluster (Advanced)
- Microsoft Windows Server 2012 Failover Cluster
- Microsoft Windows Server 2012-2012 R2 Failover Cluster
- MongoDB (Windows)
- Novell GroupWise Message Transfer Agent (Windows)
- Novell GroupWise Post Office Agent (Windows)
- Office 365 User Statistics with PowerShell
- Orion Server
- Remote Desktop Services Licensing
- Server Clock Drift (PowerShell)
- SharePoint Server 2010
- SharePoint Server 2013
- SharePoint Server (MOSS) 2007
- SharePoint Services (WSS) 3.0
- SolarWinds Failover Engine
- SolarWinds NetFlow Traffic Analyzer
- SolarWinds Web Performance Monitor (WPM) Player
- SQL Server 2005 Analysis Services
- SQL Server 2008 Analysis Services
- SQL Server 2008 R2 Reporting Services
- SQL Server 2008 Reporting Services
- SQL Server 2008-2012 Reporting Services (Events)
- SQL Server 2012 Analysis Services
- SQL Server 2012 Reporting Services
- Squid (Windows)
- Streaming Media Services 2008
- Symantec Backup Exec Remote Agent
- Symantec Backup Exec Server
- Symantec Endpoint Protection Client
- Symantec Endpoint Protection Server
- Symantec NetBackup Client
- Symantec NetBackup Server
- Terminal Licensing Server
- Trend Micro OfficeScan Client
- Trend Micro OfficeScan Server
- Trend Micro Server Protect (Windows)
- UniData Database (Windows)
- Veeam Backup and Replication Server
- VMware vCenter Server 5.5
- Websense Web Security
- Windows 2003-2008 FTP Service
- Windows 2008 R2 - 2012 FTP Service
- Windows DHCP Server
- Windows DNS Server
- Windows Network Load Balancing
- Windows Print Services
- Windows Remote Desktop Services (Session Host Role)
- Windows Server 2003 Domain Controller Security
- Windows Server 2003-2012 Services and Counters
- Windows Server 2008-2012 Domain Controller Security
- Windows Update Monitoring
Assign and edit application monitors to nodes

To begin collecting data in SAM, you need to assign the application monitors or templates to nodes managed by the Orion Web Console. The quickest way to assign Application Monitors to nodes is through the Add New Application Monitors Wizard. You can also assign them through the Manage Templates page.

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

To assign a template using the Add New Application Monitors Wizard:

1. On the Web Console, click Settings > All Settings > SAM Settings > Manually Assign Application Monitors.
2. Select the Application Monitor template to apply, and then click Next.
3. Select the server nodes to which you want to apply the Application Monitor template, and then click Next.
4. Select existing credentials or create new credentials, then click Assign Application Monitors.

To assign a template through the Manage Application Monitor Templates page:

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Browse and select the template you want to assign.
3. Click Assign to Node, then select the server nodes to which you want to apply the Application Monitor template, and then click Next.
4. Select existing credentials or create new credentials, then click Assign Application Monitors.
5. Review the information for the assigned Application Monitor and then click Done.

To remove application monitors:

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Select a template and click Edit. The template opens displaying all currently assigned monitors.
3. Select the monitors you want to remove and click Delete.

Create component monitors from the Component Monitor Wizard

The Component Monitor Wizard provides a starting point where you can select component monitors based on a specific process, performance counter, or service. You can add these monitors with modifications to application monitors and templates for assigned node monitoring. You can then discover and monitor nodes that match the selected process.
Component monitors are a part of the larger whole of application monitors and templates used to monitor applications. Templates include multiple application monitors, which include multiple component monitors, for tracking and providing data on nodes and applications. The application template can then be applied to nodes running the application the template was designed for. To learn how to create an application template, see Assign and edit application monitors to nodes.

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

1. On the web console, click > Settings > All Settings > SAM Settings > Component Monitor Wizard.
2. Select a component monitor type to add to your application or template. These include monitors based on operating system: Windows Systems, Linux - Unix Systems, VMWare Systems, and Applications.

   When using the Component Monitor Wizard, the only component monitor supported for Orion Agent for Linux is the Linux - Unix System: Process Monitor. To create and assign component monitors and templates for Orion Agent for Linux, see the available list here: Monitor with Orion agents in SAM

3. Depending on the component monitor you select, a new set of steps display. For example, if you create a Process Monitor, you should select a Target system by browsing to supported systems in your environment. You may also need to select a platform bitness and enter credentials for the target system. Select and enter all required information.
4. When you click next, if you entered credentials, a connection test runs. If it passes, continue adding component monitors and properties. Depending on the components, you may need to enter additional server and credentials data.
5. With your component monitors set, you can add the component monitor to other application monitors and templates.
6. Finally, assign the application monitor or template to nodes in your environment. When confirmed, the node details page will include these new monitors and resulting data.
Scan nodes for applications

SolarWinds SAM can scan nodes for you and automatically assign the Application Monitors it deems suitable for each scanned node. You select the nodes to be scanned, the application templates to use in the scan, and the scanning parameters to determine a match. When run, SAM compares applications located on nodes with the parameters to automatically assign monitors.

You may need to log in with an administrator account to perform these actions.

You cannot scan for user experience (UX) monitors, but you can assign them to nodes manually. Adding monitors from this page does not affect your scan.

Use the Scan Nodes for Applications to configure, scan, and assign monitors:

1. On the Web Console, click Settings > All Settings > SAM Settings > Click Scan Nodes for Applications.
2. Browse or filter to select nodes for scanning. You can select all or pick and choose from lists. The number of nodes selected lists on the page. Click Next.
3. Browse, filter, and select the applications you want to scan for. These applications have associated monitors. Expand the Advanced Scan Settings to set the exactness for matches. Click Next.

- Exact Match: All the components must match to assign the template.
- Strong Match: Most of the components must match to assign the template.
- Partial Match: Some of the components must match to assign the template.
- Minimal Match: At least one component must match to assign the template.

To keep the time it takes to scan to a minimum, we recommend you initially scan for only a limited number of application templates. To see more application templates, select a different template group from the Show Only list.

4. Some application templates require credentials either to access restricted resources, or to run within the context of a specific user. To scan for these templates, add the necessary credentials to the list, moving them into an order for using. If a template you are scanning for requires credentials, the credentials in this list are tried in the order in which they appear. You can add credentials or allow credentials to inherit from the node's local credentials. Click Next.

If you have domains sharing user names with different passwords, we recommend you run separate application discoveries for each domain.

Credentials are tried several times over the course of a scan, so an incorrect password is likely to lock out an account. To avoid potential account lockouts that affect actual users, we recommend you create and use service accounts. A service account is an account that is created specifically for the purpose of providing credentials to use for SolarWinds monitoring. With service accounts, no actual user is affected by an account lockout if a password should be entered incorrectly.
5. Review the selected options before scanning. If the automatic discovery matches templates that are already assigned to the node, by default the template is not assigned a second time. If you want to assign duplicate templates, select Yes, Assign Anyway from the Do you want to assign duplicates list.

6. Click Start Scan to start the discovery and assignments.

7. The scan runs in the background. You are notified by a message near the top of the window when scanning is completed. Click View results to see the results of the scan.

You can modify the assigned applications monitors through the Manage Application Monitors page at Settings > All Settings > SAM Settings.
Unmanage and manage assigned application monitors

You may need to unmanage or manage assigned application monitors. When a template of application monitors is unmanaged, you no longer receive data in SAM. To resume viewing status and polled data, you need to manage the application monitors template.

You cannot unmanage specific application monitors within a template. Monitors have an enable/disable option.

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

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Application Monitors.
2. Locate the application monitor template you want to manage or unmanage.
3. Select the option as needed: Manage or Unmanage.
4. When unmanaging, a scheduler opens to set the date and time to begin and end the unmanaged state. Click OK to save.
5. When managing, the application monitor template immediately begins polling per the configured intervals.
Manage templates and groups

You can assign templates and application monitors to groups, applied to all nodes within the group. Any node added to the group automatically has the templates and application monitors assigned as configured. Likewise, if you add a new template or application monitor to the group, all node members receive the new additions.

- Assign an application template to a group
- Unassign application monitors from a group

The group assignments have the following logic:

- Added nodes receive the assigned templates and application monitors, regardless of template type. For example, if a template assigned to a group monitors a specific OS version such as Windows 2003, all group members regardless of the template receive it such as an OS node of Windows 2012.
- If an OS specific template such as Windows is assigned to a group with Linux nodes, the template is assigned and reports a status of Unknown due to OS mismatch.
- If a node added to the group already has the template assigned to it, no changes occur.
- If a node is part of two groups with shared templates, the node only receives one copy of each assigned template and application monitors.
- If you delete a group, the assigned templates may remain assigned depending on the Advanced section configuration. In the Auto Delete Application Monitor option, select Yes to remove the templates if the group is deleted or nodes are removed from the group.

![Advanced Settings](image)

- You cannot assign credentials to a node and have all templates assigned to the group use those credentials. Credentials are not associated by group. You can select Inherit Credentials from Node when using WMI or an agent. The new application created from the template will use credentials from the node that is assigned to.

Assign an application template to a group

Assigning an application template to a group is more efficient than applying the template to individual nodes one at a time. Before you begin, a group must be created. To create a group, see Create groups.
The process may take about 10 minutes for templates to be assigned to the group. If the templates do not assign, you may need to restart services to verify.

- Nested groups are not supported. AppInsight applications cannot be assigned to groups. Application assignment to a group happens in the background and can take some time to be created depending on the size of the application.

1. On the web console, click Settings > All Settings > SAM Settings > Manage Templates > Application Monitor Templates.
2. Select an application template and then click, Assign to Group.

![Manage Application Monitor Templates](image)
3. Select a group from the Available Groups column, click the green arrow, and then click Next.

   By default, the template is assigned to those nodes in the group that are running a server operating system. This can be changed in the Advanced section at the bottom of the page. When a node is removed from a group, the application is deleted from the node by default. You can override this by selecting No under the Advanced section.

4. Select your credentials and then click, Assign Groups.

5. Click Done.

Your application templates are now assigned to a group.

To view the applications within a group, in the web console, click My Dashboards > SAM Summary and then click a group in the Application Templates Assigned to Group resource.
You can create dynamic groups and assign templates to these groups. For example, a dynamic group can be created for all Windows computers and the Windows Update template can be applied to the nodes of the group dynamically.

Unassign application monitors from a group

1. On the web console, click Settings > All Settings > SAM Settings > Manage Templates > Application Monitor Templates.

2. Select the application monitor you want to unassign from the group, and then click the link in the Assigned To column.

3. On the Template Assignments page, click the Group tab and then click Unassign > Yes, Unassign.

4. Click Close.
Assign an application template to a group

Assigning an application template to a group is more efficient than applying the template to individual nodes one at a time. Before you begin, a group must be created. To create a group, see Create groups.

The process may take about 10 minutes for templates to be assigned to the group. If the templates do not assign, you may need to restart services to verify.

Nested groups are not supported. AppInsight applications cannot be assigned to groups. Application assignment to a group happens in the background and can take some time to be created depending on the size of the application.

1. On the web console, click Settings > All Settings > SAM Settings > Manage Templates > Application Monitor Templates.
2. Select an application template and then click, Assign to Group.
3. Select a group from the Available Groups column, click the green arrow, and then click Next.

   By default, the template is assigned to those nodes in the group that are running a server operating system. This can be changed in the Advanced section at the bottom of the page. When a node is removed from a group, the application is deleted from the node by default. You can override this by selecting No under the Advanced section.

4. Select your credentials and then click, Assign Groups.
5. Click Done.

Your application templates are now assigned to a group.

To view the applications within a group, in the web console, click My Dashboards > SAM Summary and then click a group in the Application Templates Assigned to Group resource.
You can create dynamic groups and assign templates to these groups. For example, a dynamic group can be created for all Windows computers and the Windows Update template can be applied to the nodes of the group dynamically.
Unassign application monitors from a group

1. On the web console, click Settings > All Settings > SAM Settings > Manage Templates > Application Monitor Templates.

2. Select the application monitor you want to unassign from the group, and then click the link in the Assigned To column.

3. On the Template Assignments page, click the Group tab and then click Unassign > Yes, Unassign.

4. Click Close.
Script custom component monitors

Ten output pairs can be returned when using script monitors. A usage example using the PowerShell script monitor might go like this:

Imagine you have an Exchange PowerShell script. With multiple values returned, you can get a mail traffic report broken down by day, hour, message size, and number of recipients.

If you exceed the maximum number of allowed output pairs of ten, the remainder above the tenth output pair is ignored.

The following sections provide information and guidance to help you create some of the more complicated types of component monitors.

- Linux/Unix Script monitor
- Windows Script monitor
- Nagios Script monitor
- Windows PowerShell monitor

For general information about the settings for each component monitor, click the More Information help link in the SolarWinds SAM component monitor description.

SolarWinds fully supports scripts written and provided by the company; however, we do not provide customer support for custom scripts written by outside sources. SolarWinds does provide sample scripts that we do support located at C:\Program Files\SolarWinds\Orion\APM\Sample-Script Monitors.
Linux/Unix Script monitor

This component monitor uses SSH to upload a script to a Linux/Unix server, runs the script on the server, and then processes the return value and text output. To create this monitor, see Create a Linux or Unix script monitor.

To use scripts with Nagios formats, we recommend using the Nagios Script monitor.

Statistic

The statistic for this component monitor is the Statistic value returned by the script.

A maximum of 10 output pairs can be returned. If you exceed the maximum allowed, remove the excess output pairs or they will simply be ignored.

Prerequisites for Orion agent for Linux

You need to include credentials that can run scripts on the monitored Linux-based computer. Agentless monitoring does not require these credentials.

You need to verify your installation of python and python-xml. Depending on your Linux distribution, you may have need to install these libraries. You can verify your Python installed libraries with the following command:

```
python -c "import sys; from xml.dom.minidom import parseString; print sys.version"
```

See the Python site for documentation and install commands. The following command typically updates and installs the required Python libraries: `apt-get install python`

Depending on your Linux distribution, you may need to verify install and configure specific applications and services to use the Linux/Unix Script monitor. For example, to use the Linux/Unix Script monitor with Apache services (as with the Apache template), you need to configure Apache access. For full configuration details for all services, see Linux/Unix system configurations for component monitors.

Troubleshooting high CPU usage

This component monitor uses SSH for connecting to target machines. Due to supported key exchange algorithms, the JobWorker process used by SAM may encounter high CPU usage. If the issue is due to the algorithm, you can modify the order of supported algorithms. If you have concerns making these changes, contact Support.

1. Locate the file `c:\Program Files (x86) \SolarWinds\Orion\APM\SolarWinds.APM.Probes.dll.config`
2. Edit the text file and locate `<LinuxScriptSettings PromptWait="2" ColumnCount="200" TemporaryScriptFileNamePrefix="APM_" />`. 
3. Modify the order of algorithms, such as: `<LinuxScriptSettings PromptWait="2" ColumnCount="200" TemporaryScriptFileNamePrefix="APM_" KeyExchangeList="diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1,diffie-hellman-group14-shal" />

4. Save changes.

Field Descriptions

Description

This field provides a default description of the monitor. You have the ability to override the default description by adding to or replacing the text, which is automatically saved. The variable to access this field is `${UserDescription}`.

Enable Component

Determines whether the component is enabled. Disabling the component leaves it in the application in a deactivated state not influencing either SolarWinds SAM application availability or status.

Authentication Type

Choose either User name and Password or User name and Private Key. The second option allows you to use certificates for authentication.

Credential for Monitoring

Select a credential that can access the Linux or Unix server over SSH, and that has sufficient rights to run scripts. If the credentials you need are not already present in the credentials list, use the Quick Credentials section to add a new credential.

When providing credentials, make sure:

- The account exists on the system receiving the executed script
- The account has elevated permissions

For details on credentials used by Orion agents, see [Credentials and privileges used on Linux-based computers](#).

<i>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.</i>

Port Number

This field allows you to specify the port number used for the SSH connection. The default value for this field is 22.

Script Working Directory

This field allows you to specify the working directory of the script process.
Count Statistic as Difference

Changes the statistic to be the difference in query values between polling cycles.

Command Line

This field allows you to specify the shell command run after the SSH connection is established. The default command line value `perl ${SCRIPT} arg1 arg2` attempts to run in a Perl interpreter the script defined in the Script Body field using the parameters `arg1 arg2`.

- The length of the Command Line field is limited to 266 characters for Solaris systems, minus the length of the `${SCRIPT}` variable after being resolved to a file name such as the following: APM_937467589.pl. Since the length of the file name will typically be around 16 characters, this means that the actual user Command Line input cannot be longer than 266 – 16, or about 250 characters (not including the length of the 9 characters for the “${SCRIPT}” variable itself).

- If you need to pass a longer command line to the target node, you can create a shell script on the target node (for example `myscript.sh`) that contains the long command line, and place the call to this script in the Command Line field, for example: `/opt/sw/myscript.sh`

Script Body

This field allows you to specify the script you want to run on the Linux or Unix server.

Status Roll-Up

This option allows you to choose how you would like the monitor to report based on the output provided by the script. The default selection is “Show worst status.”

User Notes

This field allows you to add notes for easy reference. You can access this field by using the variable, `${UserNotes}`.

Create a Linux or Unix script monitor

Linux and Unix Script component monitors allow you to execute a command line script that can return statistical data. When collecting information for this monitor, SAM runs the script with the credentials defined with the Credential Library.

- A maximum of 10 output pairs can be monitored per script monitor. More than 10 defined pairs results in a failure of the monitor.
Adapt an existing Perl script to a Linux/Unix Script component monitor in a new template

1. On the Web Console, click Settings > All Settings > SAM Settings > Create a new template, and then name the template.
2. Click Add Component Monitor, expand the Custom Component Monitors group, and then select Linux/Unix Script Monitor.
3. Click Submit then select credentials with SSH permissions in the Credential for Monitoring field.
4. Type a valid working directory in the Script Working Directory field.
5. Click Edit to open the script dialog and enter your script into the Script Body field.
6. Type the Linux command that runs the script in the Command Line field. It should be similar to the following: perl ${SCRIPT} arg1 arg2. 
   {SCRIPT} is replaced by the actual file name of the script after it's deployed to the target node. A temporary file is created in temp directory for the script.
7. Click Get Script Output. SAM then tests the script by executing it and parse its output, then return the values.
8. Click Save, then specify the critical and warning thresholds and click Submit.

Here is a sample Perl script using the Linux/Unix component monitor returning multiple output pairs, in this case, two:

The code in red shows where the output pairs are defined.

```perl
#!/usr/bin/perl
if (@ARGV[0] =~ /hlp\b/) {

    print "MemoryUsage.pl SNMPver community hostname\n";
    print "SNMPver - version of SNMP protocol\n";
    print "community - community name of SNMP protocol\n";
    print "hostname - Target host\n";
    exit 1;
}
# Get hostname and trim newline
$localhost = `hostname`;
$localhost =~ s/\s*$//g;
$hostname = shift || $localhost;
$community = shift || "public";
$version = shift || "v1";
$results = "";
$MIB_TotalMemory = "UCD-SNMP-MIB::memTotalReal.0";
#$MIB_TotalMemory = "UCD-SNMP-MIB::memTotalReal.0";
$outres = "snmpget -$version -c $community $hostname $MIB_TotalMemory |";
open(OUTMEM,$outres) || die "Unable read pipe\n";
while ($line = &lt;OUTMEM&gt;) {
```
if ($line =~ /\bINTEGER\b/) {
    $indval = index($line,"=");
    $indval+=index($line,";",$indval);
    $val = substr($line,$indval+1,length($line) - $indval);
    $val =~ s/[a-zA-Z]/\n
    print "Message.1: Available memory at host "$hostname": $val in kB\n"
    print "Statistic.1: $val\n"
    print "Message.2: Again, the available memory at host "$hostname": $val in kB\n"
    print "Statistic.2: $val\n"
    exit 0;
}
print "Statistic: 0\n";
exit 1;

Below is the output from this script:

![Script Output: Message.1: Available memory at host "lab-fedora32": 1027012 in kB
   Statistic: 1027012
   Message.2: Again, the available memory at host "lab-fedora32": 1027012 in kB
   Statistic: 1027012](image)

Linux/Unix scripts

Linux/Unix scripts are uploaded by SSH and then run on the target node using the string from the Command Line field.

You can use the following variable in the command line field:

- `{$SCRIPT}` - Replaced with the script body.

You can use the following variables in the script body field:

- `{$IP}` - Replaced with the target node's IP address.
- `{$USER}` - Replaced with the user name from the credential.
- `{$PASSWORD}` - Replaced with the password from the credential.

Example Scripts

There are several sample scripts installed with SolarWinds SAM you can use to create Linux/Unix script component monitors. These sample scripts are installed on your SolarWinds SAM server, in the folder: `C:\Program Files\SolarWinds\Orion\APM\SampleScriptMonitors\LinuxScripts`

Scripts Must Report Status Through Exit Codes

Scripts must report their status by exiting with the appropriate exit code.
To correctly create this component monitor, you must first return an exit code which results in an Up (0), Warning (2), or Critical (3) status. When one of these exit codes is received the appropriate dynamic evidence table structure is created and all further exit codes are handled correctly. If the component only returns Down (1) or Unknown (4) on first use, the appropriate dynamic evidence table structure is not created appropriately.

<table>
<thead>
<tr>
<th><strong>EXIT CODE</strong></th>
<th><strong>MEANING</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>1</td>
<td>Down</td>
</tr>
<tr>
<td>2</td>
<td>Warning</td>
</tr>
<tr>
<td>3</td>
<td>Critical</td>
</tr>
<tr>
<td>Any other value</td>
<td>Unknown, for example 4</td>
</tr>
</tbody>
</table>

For example, if you want to inform SolarWinds SAM that a Script reports Up status, you would exit the script using code similar to the following, where 0 reports Up: `Wscript.quit(0)`

**Scripts with Text Output**

Scripts report additional details by sending text to the script's standard output.

SAM supports multiple values returned by a script using the following format.

```
Statistic.Name1: x
Message.Name1: abc

Statistic.Name2: y
Message.Name2: abc
```

<table>
<thead>
<tr>
<th><strong>DETAIL TYPE</strong></th>
<th><strong>REQUIRED</strong></th>
<th><strong>MEANING</strong></th>
</tr>
</thead>
</table>
| Statistic       | Yes          | A numeric value used to determine how the monitor compares to its set thresholds. This must be an integer value, (negative numbers are supported).
|                 |              | `Statistic.Name1: 123` |
|                 |              | `Statistic.Name2: 456` |
| Message         | No           | An error or information message to be displayed in the monitor status details. Note: Multi-line messages are supported. To use this functionality print each line using a separate command. For example:
|                 |              | `Message.Name1: abc` |
|                 |              | `Message.Name2: def` |

---

**ADMINISTRATOR GUIDE: SERVER & APPLICATION MONITOR**

---

*page 431*
There is a limit of ten Statistic and Message pairs for the script. These can be placed anywhere in the script output. The Statistic and Message names you give must contain valid letters and/or numbers.

Sample output:

```
# Script comment: This shows two pairs. Ten pairs are possible.
Statistic.CPU: 31.08
Message.CPU: svchost.exe cpu usage

Statistic.RAM: 1234.56
Message.RAM: svchost.exe ram usage
```

Nagios scripting

If you are using this component monitor with Nagios and polled by Orion agent for Linux, you need to enter a script as follows. The argument would be `python $(SCRIPT)` with a body of:

```
from random import randint
STAT PAIRS_COUNT = 10

for stat_id in range(STAT PAIRS_COUNT):
    print 'Statistic.random%d: %d
Message.random%d: %s' % (stat_id, randint(1,100), stat_id, 'random number: ' + str(randint(1,100)))
```

⚠️ To use scripts with Nagios formats, we recommend using the [Nagios Script monitor](#).
Windows Script monitor

This component monitor runs a Windows script on the SolarWinds SAM server and then processes the script's exit code and text output. This monitor has the ability to return up to ten pairs, i.e.: 10 statistic values + 10 [optional] messages. This is best used in conjunction with the Multiple Statistic Chart. To create this monitor, see Create a Windows Script Monitor.

A maximum of 10 output pairs can be returned. If you exceed the maximum allowed, remove the excess output pairs or they will simply be ignored.

Statistic

The statistic for this component monitor is the value returned by the script.

Script Monitor Formatting

At least one message and statistic is required. The statistic must be a valid integer and be able to be converted to double, otherwise it is handled as Not as Number (NaN). There is no maximum length for the message; however, only alphanumeric characters and the underscore are allowed.

Field Descriptions

Description

This field provides a default description of the monitor. You have the ability to override the default description by adding to or replacing the text, which will then be automatically saved. The variable to access this field is ${UserDescription}.

Component Type

This describes the type of monitor you are using.

Enable Component

This option determines whether or not the component is enabled. Disabling this component leaves it in the application as deactivated and does not influence application availability or status.

Credential for Monitoring

Select a Windows credential that is both a user who can log on to the SolarWinds SAM server, and has sufficient rights on the target node (which may be the SAM server itself, depending upon your application) to do whatever the script needs to do. For example, if the script does something with WMI, the credentials also need WMI rights on the target node. If the credential you need is not already present in the credentials list, use the Quick Credentials section to add a new credential.
Script Arguments

This field is in the script editing window and allows you to specify arguments to pass to the script. You may include the variables ${IP}, ${USER}, and ${PASSWORD}, which are replaced respectively by the IP address of the target node, the credential user name, and the credential password.

Script Engine

This field allows you to specify the scripting language to be used. The default value is vbscript. Below is a list of scripting engines that the Windows Script Host supports:

<table>
<thead>
<tr>
<th>NAME</th>
<th>FILE EXTENSIONS</th>
<th>AVAILABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>VBScript</td>
<td>.vbs</td>
<td>Installed by default</td>
</tr>
<tr>
<td>JScript</td>
<td>.js</td>
<td>Installed by default</td>
</tr>
<tr>
<td>PerlScript</td>
<td>.pls</td>
<td>Freeware</td>
</tr>
<tr>
<td>ooRexxScript</td>
<td>.rxs</td>
<td>Freeware</td>
</tr>
<tr>
<td>PythonScript</td>
<td>.pys</td>
<td>Freeware</td>
</tr>
<tr>
<td>TclScript</td>
<td>.tcl</td>
<td>Freeware</td>
</tr>
<tr>
<td>ActivePHPScript</td>
<td>.phps</td>
<td>Freeware</td>
</tr>
<tr>
<td>RubyScript</td>
<td>.rbs</td>
<td>Freeware</td>
</tr>
<tr>
<td>Object Rexx engine</td>
<td></td>
<td>Commercial</td>
</tr>
<tr>
<td>Delphi scripting engine</td>
<td></td>
<td>Commercial</td>
</tr>
</tbody>
</table>

1. VBscript runs locally on the SAM server only. PowerShell uses WINRM that runs over TCP ports 5985 and 5986. All Linux, Unix, and Nagios script monitors use SSH over TCP Port 22.

Script Body

This field is in the script editing window and allows you to enter your script via typing or pasting. To enter your script, click the Edit button that reveals the script editing window.

Status Roll-Up

This option allows you to choose how you would like the monitor to report the returned results based on the output provided by the script. With the ability to have multiple values returned, selecting how your scripts report back to you offers more flexibility. The default selection is “Show worst status.”
User Notes

This field allows you to add notes for easy reference. You can access this field by using the variable, `${UserNotes}`.

Create a Windows Script Monitor

You can create a Windows Script monitor to have SolarWinds SAM run a script using Windows Script Host. Windows Script Host comes with VBScript and Jscript, but can be extended with other scripting languages.

Scripts run on the SolarWinds SAM server and use the credentials you specify. The script must both return an exit code and output a text string containing a statistic value conforming to the specifications described later in this section.

Format the Statistic value to use the same decimal separator as the SolarWinds SAM server. The SolarWinds SAM server uses the decimal separator set by its Microsoft Windows regional settings. You may need to log in with an administrator account to perform this action.

Adapt an existing Visual Basic script to a Windows Script Monitor in a new template

1. On the Web Console, click Settings > SAM Settings > Create a New Template, then name the template.
2. Click Add Component Monitor, then expand the Custom Component Monitors group, and then check Windows Script Monitor.
3. Click Submit, and then select credentials with the appropriate permissions to run the script on the SolarWinds SAM server, and that also has appropriate permissions to do whatever else the script requires.
4. Copy the Visual Basic script into the Script Body field.
5. Type any script arguments into the Script Arguments field.
6. Specify the critical and warning thresholds, then click Submit.

Macros for Script Arguments

Specify script arguments in the Script Arguments field if needed. You can use the following variables as script arguments:

${IP}

This is replaced with the target node's IP Address.

${USER}

This is replaced with the user name from the credential set.

${PASSWORD}

This is replaced with the password from the credential set.
Scripts Must Report Status Through Exit Codes

Scripts must report their status by exiting with the appropriate exit code.

To correctly create this component monitor, you must first return an exit code which results in an Up (0), Warning (2), or Critical (3) status. When one of these exit codes is received the appropriate dynamic evidence table structure is created and all further exit codes are handled correctly. If the component only returns Down (1) or Unknown (4) on first use, the appropriate dynamic evidence table structure is not created appropriately.

<table>
<thead>
<tr>
<th>EXIT CODE</th>
<th>MEANING</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>1</td>
<td>Down</td>
</tr>
<tr>
<td>2</td>
<td>Warning</td>
</tr>
<tr>
<td>3</td>
<td>Critical</td>
</tr>
<tr>
<td>Any other value</td>
<td>Unknown, for example 4</td>
</tr>
</tbody>
</table>

For example, if you want to inform SolarWinds SAM that a VBScript reports Up status, you would exit the script using code similar to the following, where 0 reports Up: `Wscript.quit(0)`

Scripts with Text Output

Scripts report additional details by sending text to the script's standard output. SAM supports multiple values returned by a script using the following format.

Statistic.Name1: xMessage.Name1: abc

Statistic.Name2: yMessage.Name2: abc

<table>
<thead>
<tr>
<th>DETAIL TYPE</th>
<th>REQUIRED</th>
<th>MEANING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistic</td>
<td>Yes</td>
<td>A numeric value used to determine how the monitor compares to its set thresholds. This must be an integer value, (negative numbers are supported). Statistic.Name1: 123Statistic.Name2: 456</td>
</tr>
<tr>
<td>Message</td>
<td>No</td>
<td>An error or information message to be displayed in the monitor status details. Note: Multi-line messages are supported. To use this functionality print each line using a separate command. For example: Message.Name1: abc Message.Name2: def</td>
</tr>
</tbody>
</table>
There is a limit of ten Statistic and Message pairs for the script. These can be placed anywhere in the script output. The Statistic and Message names you give must contain valid letters and/or numbers.

Sample output:

```plaintext
# Script comment: This shows two pairs. Ten pairs are possible.
Statistic.CPU: 31.08Message.CPU: svchost.exe cpu usage
Statistic.RAM: 1234.56Message.RAM: svchost.exe ram usage
```

Example Scripts

Below is a sample vbscript that returns two values:

- The total number of files in a folder
- Twice the total number of files in the same folder

The code that represents these two values are bold. To use this script, copy and paste the following code into the Script Body field. In the Scripts Arguments field, type in C:\Windows, or any other folder you want to monitor.

```vbs
Option Explicit
On Error Resume Next
Dim lstArgs, path, fso, objDir, objFiles, objFiles2
Set lstArgs = WScript.Arguments
If lstArgs.Count = 1 Then
    path = Trim( lstArgs( 0 ) )
Else
    WScript.Echo "Message: Usage: wscript.exe filelist.vbs [pathToFiles]\n    &amp;" & vbCRLF & "[pathToFiles] Local or UNC Path"
    WScript.Echo "Statistic: 0"
    WScript.Quit( 1 )
End If
Set fso = Wscript.CreateObject( "Scripting.FileSystemObject" )
If fso.FolderExists( path ) Then
    Set objDir = fso.GetFolder( path )
    If( IsEmpty( objDir ) = True ) Then
        WScript.Echo "Message: Object Not Initialized"
        WScript.Echo "Statistic: 0" WScript.Quit( 1 )
    End If
    Set objFiles = objDir.Files
    If( IsEmpty( objFiles ) = true ) Then
        WScript.Echo "Message: Object Not Initialized"
        WScript.Echo "Statistic: 0"
        WScript.Quit( 1 )
    End If
End If
```
WScript.Echo "Message.Total: " &amp; CInt( objFiles.Count ) &amp; " files in this folder."
WScript.Echo "Statistic.Total: " &amp; CInt( objFiles.Count )
WScript.Echo "Message.Twice: " &amp; CInt( objFiles.Count*2 ) &amp; " = twice the number of files in this folder."
WScript.Echo "Statistic.Twice: " &amp; CInt( objFiles.Count*2 )
WScript.Quit( 0 )
Else
WScript.Echo("Message: Folder Not Found")
WScript.Echo("Statistic: 0")
WScript.Quit( 1 )
End If

There are several examples of Windows Script component monitors included in templates. These include: File Count, File Modified, LDAP Connection Monitor, Run 3rd Party Application, and Windows Event Log Count.

Sample scripts are installed on your SolarWinds SAM server, in the folder: C:\Program Files\SolarWinds\Orion\APM\SampleScriptMonitors\WindowsScripts
Nagios Script monitor

This component uses SSH to upload a Nagios script to a Linux/Unix server, runs the Nagios script on the server and then processes the script's exit code and text output. This monitor has the ability to return multiple values.

**Statistic**

The statistic for this component monitor is the value returned by the script. This component monitor has the ability to return multiple results and has the ability to process Nagios resulting output. For more information, see [http://nagios.sourceforge.net/docs/3_0/pluginapi.html](http://nagios.sourceforge.net/docs/3_0/pluginapi.html).

1. A maximum of 10 output pairs can be returned. If you exceed the maximum allowed, remove the excess output pairs or they are ignored.

**Prerequisites for Orion agent for Linux**

You need to include credentials that can run scripts on the monitored Linux-based computer. Agentless monitoring does not require these credentials.

If you are using this component monitor with Nagios and polled by Orion agent for Linux, you need to enter a script as follows. The argument would be `python $(SCRIPT)` with a body of:

```python
from random import randint
STAT_PAIRS_COUNT = 10

for stat_id in range(STAT_PAIRS_COUNT):
    print 'Statistic.random%d: %d\nMessage.random%d: %s' % (stat_id, randint(1,100), stat_id, 'random number: ' + str(randint(1,100)))
```

**Troubleshooting high CPU usage**

This component monitor uses SSH for connecting to target machines. Due to supported key exchange algorithms, the JobWorker process used by SAM may encounter high CPU usage. If the issue is due to the algorithm, you can modify the order of supported algorithms. If you have concerns making these changes, contact Support.

1. Locate the file `c:\Program Files (x86)\SolarWinds\Orion\APM\SolarWinds.APM.Probes.dll.config`.
2. Edit the text file and locate `<LinuxScriptSettings PromptWait="2" ColumnCount="200" TemporaryScriptFileNamePrefix="APM_" />`.
3. Modify the order of algorithms, such as: `<LinuxScriptSettings PromptWait="2" ColumnCount="200" TemporaryScriptFileNamePrefix="APM_"
KeyExchangeList="diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1,diffie-hellman-group14-sha1" />
4. Save changes.
Field Descriptions

Description
This field provides a default description of the monitor. You have the ability to override the default description by adding to or replacing the text, which is automatically saved. The variable to access this field is ${UserDescription}.

Component Type
This describes the type of monitor you are using.

Enable Component
This option determines whether or not the component is enabled. Disabling this component leaves it in the application as deactivated and does not influence application availability or status.

Authentication Type
Choose either User name and Password or User name and Private Key. The second option allows you to use certificates for authentication.

Credential for Monitoring
Select a Windows credential that is both a user who can log on to the SolarWinds SAM server, and has sufficient rights on the target node to do whatever the script needs to do. For example, if the script does something with WMI, the credentials also need WMI rights on the target node. If the credential you need is not already present in the credentials list, use the Quick Credentials section to add a new credential.

Port Number
This field allows you to specify the port number used for the SSH connection. The default value is 22.

Script Working Directory
This field allows you to specify the working directory of the script process.

Check Type
Set the check type to Service or Host. To prevent false positives, Nagios allows you to define how many times a service or host should be (re)checked before alerting for an issue. Depending on the select, the monitor checks using the configured value on the server for \texttt{max\_check\_attempts} option in the host and service definitions.

Count Statistic as Difference
Changes the statistic to be the difference in query values between polling cycles.
Command Line

This field is in the script editing window and allows you to specify the script you want to run on the target node followed by the arguments. To enter your script, click the Edit button that reveals the script editing window. For more information, see [http://nagios.sourceforge.net/docs/3_0/pluginapi.html](http://nagios.sourceforge.net/docs/3_0/pluginapi.html).

1. The length of the Command Line field is limited to 266 characters for Solaris systems, minus the length of the ${SCRIPT} variable after being resolved to a file name such as the following: APM_937467589.pl. Since the length of the file name will typically be around 16 characters, this means that the actual user Command Line input cannot be longer than 266 - 16, or 250 characters (not including the length of the 9 characters for the "${SCRIPT}" variable itself). If you need to pass a longer command line to the target node, you can create a shell script on the target node (for example: myscript.sh) that contains the long command line and place the call to this script in the Command Line field, for example: /opt/sw/myscript.sh

Script Body

This field is in the script editing window and allows you to enter your script via typing or pasting. You can test the script to receive output definitions. You can save these definitions to the component monitor for further configurations. Every saved definition is listed as Script Output with an assigned number and name. See Test script output for details.

Status Roll-Up

This option allows you to choose how you would like the monitor to report based on the output provided by the script. The default selection is “Show worst status.”

User Notes

This field allows you to add notes for easy reference. You can access this field by using the variable, ${UserNotes}.

Scripts must report status through return codes

Nagios determines the status of a host or service by evaluating the return code. The following table shows a list of valid return codes, along with their corresponding service or host states.

<table>
<thead>
<tr>
<th>Return Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>1</td>
<td>Down</td>
</tr>
<tr>
<td>2</td>
<td>Warning</td>
</tr>
<tr>
<td>3</td>
<td>Critical</td>
</tr>
<tr>
<td>4</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

To correctly create this component monitor, you must first return an exit code which results in an Up (0), Warning (2), or Critical (3) status. When one of these exit codes is received the appropriate dynamic evidence table structure is created and all further exit codes are handled correctly. If the component only returns Down (1) or Unknown (4) on first use, the appropriate dynamic evidence table structure is not created appropriately.
### RETURN CODES

<table>
<thead>
<tr>
<th>RETURN CODE</th>
<th>SERVICE STATE</th>
<th>HOST STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>OK</td>
<td>Up</td>
</tr>
<tr>
<td>1</td>
<td>Warning</td>
<td>Up or Down/Unreachable†</td>
</tr>
<tr>
<td>2</td>
<td>Critical</td>
<td>Down/Unreachable</td>
</tr>
<tr>
<td>3</td>
<td>Unknown</td>
<td>Down/Unreachable</td>
</tr>
</tbody>
</table>

†If the Use Aggressive Host Checking option is enabled, return codes of 1 will result in a host state of Down, otherwise return codes of 1 will result in a host state of Up.

Nagios scripts must exit with a valid return code and a line of text output. The exit code determines the status of the component. If the exit code is 0 (OK), the component status may be further modified by thresholds from the optional statistics. To return up to ten optional statistics, separate the statistics from the status message with the pipe (|) symbol using the following syntax:

```
statusMessage [|'statisticName'=value]
```

Below is an example of valid output with a status message and two statistics:

The script ran. | 'CPU%'=75.2 'MemoryRemainingInKB'=600784

### Test script output

You should test the script output while editing the script prior to testing the script in the template or application component pages. If the output formatting or values are not correctly defined or missing, you may receive an error: "Script output values are not defined or improperly defined." This error displays if the named fields could not be located in the script output.

To test the script and save output definitions:

1. Open the template or application monitor using the Nagios Script monitor. To open, click Settings > All Settings > SAM Settings > Manage Application Monitors. Locate and edit the application monitor or template with the Nagios Script monitor.
2. Locate and expand the component using the Nagios Script monitor type in the template.
3. Locate the Script Body field and click Edit Script.
4. On the Edit Script dialog, click Get Script Output. You may be prompted to specify a test node and credentials.
5. Wait for the Output Result. The results should populate with values returned by the script. Review the results to ensure all formatting is correct and fields properly load.

If you receive an error, you may have an issue in the script. For more information on formatting and outputs, see [http://nagios.sourceforge.net/docs/3_0/pluginapi.html](http://nagios.sourceforge.net/docs/3_0/pluginapi.html).
6. You can store the output definitions returned by the script test as Script Output in the component monitor. Click Save to add the output definitions. The component monitor will display the definitions with a unique ID, display name, and additional configuration options.

7. To save changes to the template or application monitor, click Submit.
Windows PowerShell monitor

This component monitor runs a Windows PowerShell script on the SolarWinds SAM server or a remote target node and then processes the script's exit code and text output. To create this monitor, see Create a Windows PowerShell monitor.

A maximum of 10 output pairs can be returned. If you exceed the maximum allowed, remove the excess output pairs; the system will ignore them.

Statistic

The statistic for this component monitor is the Statistic value returned by the script.

Configure Windows Remote Management (WinRM)

You need WinRM configured on the Orion server and remote target server.

1. Install WinRM on the Orion server and remote target servers.
2. On the Orion server, open a command prompt as an Administrator.
   Go to the Start menu, right-click the cmd.exe, and select Run as Administrator.
3. Enter the following in the command prompt:
   
   ```
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="*"}
   ```
4. On the target server, open a command prompt as an Administrator.
   Go to the Start menu, right-click the cmd.exe, and select Run as Administrator.
5. Enter the following in the command prompt:
   
   ```
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="IP_ADDRESS"}
   ```
   For IP_ADDRESS enter the IP address of your Orion server.

Field Descriptions

Description

This field provides a default description of the monitor. You have the ability to override the default description by adding to or replacing the text, which will then be automatically saved. The variable to access this field is `${UserDescription}`.

Enable Component

Determines whether the component is enabled. Disabling the component leaves it in the application in a deactivated state not influencing either SolarWinds SAM application availability or status.
Credential for Monitoring

Select a Windows credential that is both a user who can log on to the SolarWinds SAM server, and has sufficient rights on the target node to do whatever the script needs to do. For example, if the script does something with WMI, the credentials also need WMI rights on the target node. If the credential you need is not already present in the credentials list, use the Quick Credentials section to add a new credential.

The PowerShell monitor handles requests from PowerShell for the credentials to run the script and resolves them using the selected Credential for Monitoring. However some PowerShell commands used in scripts require the use of the \${CRENDENTIAL} variable. See the note in the Script Body section below regarding the use of the \${CRENDENTIAL} variable.

Execution Mode

This field allows you to specify where to run the PowerShell script:

Count Statistic as Difference

Changes the statistic to be the difference in query values between polling cycles.

Run the script under specified account

Select this option to enable impersonation with the component's credentials. (This works only in local script execution mode.)

- Local Host can run scripts only locally, that is, on the SolarWinds SAM server. This is the default value.
- Remote Host can execute scripts remotely (on the selected target node) using the Windows Remote Management (WRM) system component. WRM should be configured separately to get it working with the Windows PowerShell monitor.
- If Remote Host is selected, the following options are available:
  - Use HTTPS Protocol - if checked, specifies that the secure HTTPS protocol should be used to send and receive WS-Management protocol requests and responses. Otherwise the HTTP protocol is used.
  - URL Prefix - specifies a URL prefix on which to accept HTTP or HTTPS requests. The default is wsman.
  - Port Number - specifies the TCP port for which this listener is created. For WinRM 1.1 and earlier, the default HTTP port is 80. For WinRM 2.0, the default HTTP port is 5985.

Script Body

This field allows you to specify the PowerShell script you want to run.

Use the \${CRENDENTIAL} variable in the script where the credentials are required, as shown in the following example:
```powershell
$avg = Get-WmiObject win32_process -ComputerName '${IP}' -Credential '${CREDENTIAL}' | Where-Object {$_ -Name eq "lsass.exe"} | Measure-Object -property ReadOperationCount -Average;
```

Some PowerShell commands (such as `Get-WmiObject` as shown in the example above) require the `$CREDENTIAL` variable. The user name from the specified Credential for Monitoring is stored automatically in the `$CREDENTIAL` variable for you by the monitor. As a result, the `$CREDENTIAL` variable should not be placed in the Script Arguments field, since it is set automatically. When the script is run by PowerShell, it prompts for a password. The monitor automatically provides the password from the specified Credential for Monitoring.

Custom Properties can be passed by using the following format: `$Node.Custom.XXX` where `xxx` is the name of the custom property.

**Script Arguments**

This field allows you to specify arguments to pass to the script. You may include the variable `$IP`, which is replaced by the IP address of the target node. You should not include variables that are stored automatically, such as the `$CREDENTIAL` variable.

**User Notes**

This field allows you to add notes for easy reference. You can access this field by using the variable, `${UserNotes}`.

### Create a Windows PowerShell monitor

You can create a monitor that runs a Windows PowerShell script to monitor specific performance information for troubleshooting a Windows process that may be having issues.

A maximum of 10 output pairs can be returned. If you exceed the maximum allowed, remove the excess output pairs or they will simply be ignored. You may need to log in with an administrator account to perform this action.

What needs to be monitored

The process you want to monitor is `lsass.exe`, which enforces security on the system for users who are logging on, changing passwords, and so forth. In particular, you want to monitor the average number of read operations performed to check for spikes.

To use the Windows PowerShell monitor to run a PowerShell script with a `Get-WmiObject` call to measure the average `ReadOperationCount` for the `lsass.exe` process and monitor its value:

1. On the Web Console, click Settings > All Settings > SAM Settings > Create a New Template
2. Name the template, for example, `Lsass.exe PowerShell Monitor`.
3. Click Add Component Monitor, then expand the Custom Component Monitors group, and then select Windows PowerShell Monitor and click Add.
4. Select the Credential for Monitoring with appropriate permissions to run the script on the SolarWinds SAM server, and that also has appropriate permissions to do whatever else the script requires (in this case, to get the average number of read operations performed on the target node).

5. Select the Execution Mode to use:
   - Local Host can run scripts only locally, that is, on the SolarWinds SAM server.
   - Remote Host can execute scripts remotely (on the remote target node to which the Windows PowerShell monitor is assigned) using the Windows Remote Management (WRM) system component. WRM should be configured separately to get it working with the Windows PowerShell monitor.

6. Copy the following PowerShell script, which uses the Get-WmiObject call to measure the average ReadOperationCount for the lsass.exe process, into the Script Body field:

   ```powershell
   $avg = Get-WmiObject win32_process -ComputerName '${IP}' -Credential '${CREDENTIAL}' | Where-Object {$_ .Name -eq 'lsass.exe' } | Measure-Object -Property ReadOperationCount -Average; Write-Host 'Statistic: ' $avg.Averageexit(0)
   ```

   The PowerShell code does the following:
   a. Reads the average `ReadOperationCount` information for the process `lsass.exe` from the computer whose IP address is specified by the variable `$IP` using the credential specified by the variable `$CREDENTIAL`.

   i. The user name from the Credential for Monitoring that is specified is stored automatically in the `$CREDENTIAL` variable by the monitor. Do not add the `$CREDENTIAL` variable in the Script Arguments field. When the script is run by PowerShell, it prompts for a password. The monitor automatically provides the password from the Credential for Monitoring.

   b. Writes the statistic information gathered by the script.

   c. Exits the script.

   i. The script does not perform error checking.

7. Enter the following Script Arguments:
   Use the token `$IP` and the IP address will be filled in with the IP address of the target node. You can then access the value in the script body using the variable `$IP`.
   For example, if you type `$IP` for Script Arguments the PowerShell script will be able to access the IP address for the target node using the variable `$IP` in the script body.

8. Select Run the script under specified account to enable impersonation with the component's credentials. This works only in local script execution mode.

9. Select Count Statistic as Difference to change the statistic to be the difference in query values between polling cycles.

10. Change the Statistic Warning Threshold to, greater than 800.
11. Change the Statistic Critical Threshold to greater than 1000.

12. Click Set test node. Browse the tree view, select the desired target node for the PowerShell script, and then click Select.

13. Click Test, and then click Submit.

14. Click All in the Select tag to filter by list, and then locate the Lsass.exe PowerShell Monitor.

15. Select Lsass.exe PowerShell Monitor and then click Assign to Node.

16. Expand the tree view and select the target node, and then click Next.

17. Select Inherit credentials from template, and then click Test to confirm the credentials and component monitor against the test node.

18. Click Assign Application Monitors and then click Done.

Report status through exit codes

Scripts must report their status by exiting with the appropriate exit code. The exit code is used to report the status of the monitor, which is seen by the user through the interface.

To correctly create this component monitor, you must first return an exit code which results in an Up (0), Warning (2), or Critical (3) status. When one of these exit codes is received the appropriate dynamic evidence table structure is created and all further exit codes are handled correctly. If the component only returns Down (1) or Unknown (4) on first use, the appropriate dynamic evidence table structure is not created appropriately.

<table>
<thead>
<tr>
<th>EXIT CODE</th>
<th>SERVICE STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>1</td>
<td>Down</td>
</tr>
<tr>
<td>2</td>
<td>Warning</td>
</tr>
<tr>
<td>3</td>
<td>Critical</td>
</tr>
<tr>
<td>Any other value</td>
<td>Unknown, for example 4</td>
</tr>
</tbody>
</table>

Troubleshooting the Lsass.exe PowerShell Monitor

Verify that you are entering the user name and password of an administrator-level account. If you think you have entered an incorrect credential, correct the mistake and then retest.

Make sure that the RPC server is available and that the Windows PowerShell execution policy is not set to Restricted (the default setting). You can check the execution policy by entering the following command at the PowerShell command prompt: Get-ExecutionPolicy

If you encounter issues using the Windows PowerShell Monitor, visit the SolarWinds Success Center and see the following article for tips: https://support.solarwinds.com/success_center/Server_%26_Application_Monitor_(SAM)/Problems_using_the_Orion_APM_Windows_PowerShell_Monitor
Application Monitor Thresholds

Thresholds are markers that indicate certain levels have been reached. Many component monitors used in SAM applications have thresholds that can be adjusted and set.

Once set, thresholds can act as trigger points. For example, if you are monitoring CPU usage, a Critical threshold set at 90% would be typical. You can use this threshold as a trigger to send an email alert to inform you of the Critical status once that threshold has been breached.

Normally, an administrator would need to monitor applications for several weeks in order to collect enough data to be used as a baseline. Once a baseline has been established, the administrator can make an educated guess how to set Warning and Critical thresholds for the component monitors.

If thresholds are set too low, the administrator would be getting alerts all the time. If set too high, problems can occur without the administrator’s knowledge.

Baseline data, as well as Warning and Critical thresholds for application monitors, can be gathered and calculated automatically. The option to enter thresholds manually remains available.

By default, I/O thresholds of Windows Service Monitors are not set.

For more information, refer to the following sections:

- Inheriting Thresholds
- Adjust threshold settings and apply baseline data
- Multi-Value scripts and thresholds
- Apply baseline thresholds at the template level
- Apply baseline thresholds at the application level
- View latest baseline details
Inheriting Thresholds

Thresholds can be adjusted at the template level or on the individual component monitor level of an application.

Threshold Adjustments at the Template Level

If adjusting thresholds on the template level, either manually entered or calculated using baseline data, any changes made trickles down to the component monitor level for applications based on this template. This means the component monitors within the application inherit the changes made in the template.

Threshold Adjustments at the Component Monitor Level

If you change thresholds at the component monitor level, only thresholds of the individual component monitor are affected. Thresholds on the parent template, or other applications based on that parent template, are not be affected.
Multi-Value scripts and thresholds

Each component monitor includes a number of thresholds for pulling and saving data. To use these values in multi-value scripts, you need to use the following threshold macros:

- `$(Threshold.Warning.DisplayName)` - Macro for using the display name for a warning threshold
- `$(Threshold.Critical.DisplayName)` - Macro for using the display name for a critical threshold

The following screenshot displays the use of the macros in a script.

![Screenshot of script using threshold macros](image)

The following screenshots display the multiple display names used in a script for the thresholds values for warning and critical.

![Screenshot of multiple display names](image)
Apply baseline thresholds at the template level

Applying and editing thresholds at the template level affect all applications that are based on that template. Thresholds can be used based on calculated baseline data or you can create your own thresholds based on your needs.

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

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Select a template and click Edit from the toolbar.
3. Select a component monitor, click [+] to expand the monitor details.
4. Select Use thresholds calculated from baseline data:

Once this box is checked, the Warning and Critical fields automatically populate with the macro, ${USE_BASELINE}. This macro can be used when configuring alerts.

5. Select the options for sustained thresholds, and then click Submit.
You can edit multiple component monitors and their thresholds if the monitors are the same type and thresholds are available. Multi Edit only become available when the selected component monitors are the same type, as shown. After you click Multi Edit, select Statistic Threshold > Use thresholds calculated from baseline data. Edit thresholds, click Save > Submit.

By default, I/O thresholds of Windows Service Monitors are not set.
Apply baseline thresholds at the application level

To customize your monitoring, you can apply baseline thresholds at the application level. The Orion Web Console has a set of global thresholds that apply to all monitored nodes. Using the following instructions, you can modify those thresholds per specific node.

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

1. On the Web Console, click My Dashboards > Applications > SAM Summary.
2. From the All Applications resource, expand the tree and then click an application.
3. From the Application Details resource, click Edit Application Monitor.
4. If selecting only one Component Monitor, click [+] to expand the monitor details.
   a. Click Override Template.
      - The current values for the thresholds appear in the Warning and Critical fields.
   b. Click Use Latest Baseline Thresholds, as shown:

   ![Response Time Threshold](image)

   c. When applied, the values change and a blue icon appears indicating that baseline thresholds are being used.

   ![Statistic Threshold](image)
5. If selecting more than one component monitor, use the check boxes to select the monitors you want to edit, and then click Multi-Edit.
   a. Click Multi-Edit.

   Multi-Edit only becomes available when the selected component monitors are of the same type.

   ![Component Monitor Table]

   b. Check the Statistic Threshold check box on the pop-up window, then check the Use thresholds calculated from baseline data.

   Once the second box is checked, the Warning and Critical fields automatically populate with the macro, `${USE_BASELINE}`.

6. Click Save > Submit.
Adjust threshold settings and apply baseline data

In general, baseline data is calculated on demand; however, seven days of data is the recommended minimum amount of data needed for baseline calculations to be considered accurate. Baseline data for macros, such as \${USE_BASELINE}, are automatically calculated during nightly database maintenance.

After thresholds are calculated and applied to component monitors, the thresholds remain static until manually re-applied. This is not a moving baseline that is calculated nightly based on the last seven days of data. A moving baseline would mask data spikes and other anomalies that need to be highlighted.

Thresholds set manually to meet the needs of your environment may yield more desirable results.

How SAM calculates the baseline

SolarWinds SAM uses the following macros to calculate the baseline:

<table>
<thead>
<tr>
<th>Macro</th>
<th>Description</th>
</tr>
</thead>
</table>
| \${USE_BASELINE} | Currently used baseline in SAM, used in threshold fields of SAM component monitors. Recommended baseline values are calculated using the following formulas:  
                    **Warning:** \${MEAN} + 2 * \${STD_DEV} (or \${MEAN} - 2 * \${STD_DEV})  
                    **Critical:** \${MEAN} + 3 * \${STD_DEV} (or \${MEAN} - 3 * \${STD_DEV})  
                    Baseline thresholds are not suitable for all metrics. If calculated values do not meet expectations, consider setting the thresholds manually.  
                    \${USE_BASELINE} does not support math functions. To adjust the baseline calculation, replace \${USE_BASELINE} with the formulas above and change the calculation as necessary. |
| \${MEAN}        | Current Mean or Average. You can use this macro with math functions in threshold fields. |
| \${STD_DEV}     | Standard Deviation. You can use this macro with math functions in threshold fields. |
Change the amount of data used in baseline calculations

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

1. In the Orion Web Console, click Settings > All Settings > SAM Settings > Data & Database Settings.

2. Enter a number of days, and then click Submit.

The value for the Baseline Data Collection Duration field cannot exceed the value defined for the Detail Statistics Retention field, as displayed at the top of the Data & Database Settings section.

Apply baseline thresholds at the template level

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

1. In the Orion Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Check a template and click Edit from the toolbar.
3. If selecting only one component monitor, click [+] to expand monitor details.
   a. Click Use Latest Baseline Thresholds to display the \( \texttt{USE\_BASELINE} \) macro in the Warning and Critical fields.
   b. Select options for sustained thresholds as needed.
4. If selecting more than one component monitor, select monitors by checking the boxes next to their names.
   a. Click Multi-Edit.
   
   *Multi-Edit is only available if selected component monitors are the same type.*
   
   b. Review Statistic Threshold data that on the pop-up window, then check the Use thresholds calculated from baseline data.

   *The Use thresholds calculated from baseline data check box is not available until Statistic Threshold is checked. After Use thresholds calculated from baseline data is checked, the Warning and Critical fields automatically populate with the macro, `USE_BASELINE`.*

5. Click Save, then click Submit.

**Apply baseline thresholds at the application level**

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

1. In the Orion Web Console, click My Dashboards > Applications > Summary.
2. From the All Applications resource, expand the tree and then click an application.
3. From the Application Details resource, click Edit Application Monitor.
4. If selecting only one Component Monitor, click `+` to expand the monitor details.
   a. Click Override Template.

   *The current values for the thresholds appear in the Warning and Critical fields.*

   b. Click Use Latest Baseline Thresholds, as shown:

   ![Response Time Threshold](image)

   ![Statistical Threshold](image)

   c. When applied, values change and a blue icon indicates that baseline thresholds are used.
5. If selecting more than one component monitor, use the check boxes to select the monitors you want to edit.
   a. Click Multi-Edit. 

   ![Component Monitors](image)

   Multi-Edit is only available if selected component monitors are the same type.

   b. Check the Statistic Threshold check box on the pop-up window, then check the Use thresholds calculated from baseline data.

   ![Once the second box is checked, the Warning and Critical fields automatically populate with the macro, \$\{USE_BASELINE\}.](image)

6. Click Save, then click Submit.

Use latest baseline details

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

2. From the All Applications resource, expand the tree and then click an application.
3. From the Application Details resource, click Edit Application Monitor.
4. Find a component monitor in the list and click [+] to expand the monitor details.
5. Click Override Template, then click Latest Baseline Details.

Edit capacity planning thresholds

You may need to log in with an administrator account to perform this action.
1. On the Web Console, click a node to navigate to the Node Details page for that node.
2. In the Management resource, click Edit Node.
3. Click Manage Orion General Thresholds to display Capacity Planning options appear under each object:

<table>
<thead>
<tr>
<th>Avg CPU Load</th>
<th>Critical Level</th>
<th>1% to 10%</th>
<th>Nodes with CPU Load above this level will...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>90</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning Level</td>
<td>80</td>
<td>1% to 10%</td>
<td>Nodes with CPU Load above this level will...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capacity Planning</td>
<td>Calculate exhaustion using average daily values</td>
<td>Calculate exhaustion using peak daily values</td>
<td></td>
</tr>
</tbody>
</table>

4. Make your selections, then click Submit on both the Orion General Thresholds screen and the Edit Properties screen.
View latest baseline details

Details about how baseline data, as well as Warning and Critical thresholds are calculated, can be found on the Latest Baseline Details page. This page details the data collection and calculation process using several graphs and tables.

View the Latest Baseline Details Page

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

1. On the Web Console, click My Dashboards > Applications > SAM Summary.
2. In the All Applications resource, expand the tree and then click an application.
3. From the Application Details resource, click Edit Application Monitor.
4. Find a component monitor in the list and click [+] to expand the monitor details.
5. Click Override Template click Latest Baseline Details.
Example tasks for application monitors

These are scenarios for monitoring with SAM.

- Create your first application and alert
- Scan for applications to monitor
- Monitor a specific URL
- Monitor VMware performance counters using an application monitor
- Monitor and restart stopped Windows services
- Monitor large directories
- Monitor IIS application pools
- Use the JMX component monitor wizard
- Configure the SOAP monitor
Create your first application and alert

After applied to a node, a template becomes an application, which is comprised of component monitors, also known as performance counters. Applications created from templates are used to report metrics based on your needs. This example provides steps for creating a template for monitoring WMI.

You will create a template with added monitors, configure the monitors, then apply the template to nodes for monitoring. We also provide information for creating an alert for the WMI application to send email notices based on monitored thresholds.

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

Create a WMI monitor

1. On the Web Console, click Settings > All Settings > SAM Settings > Create a New Template.
2. Name the template and click Add Component Monitor.
3. Select WMI Monitor, click Add.
4. Select credentials or Inherit Credentials from Node.
5. In the Query field, enter a WQL query to return a statistic to be reported.
6. Enter thresholds or select Use thresholds calculated from baseline data.
7. Click Submit.

Apply the WMI monitor template

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

1. On the Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Locate your template and click Assign to Node.
3. Select the Windows node from the left pane, click the green arrow to move it to the right pane, and click Next.
4. Choose the credentials, click Assign Application Monitor, then click Done.

Alert on the WMI application via email

2. Click Add New Alert and name the alert.
3. On the Properties tab, enter required information, and click Next.
4. For the Trigger Conditions, complete the section as shown:

```
I want to alert on:
Application
```

![Trigger Conditions](image)

**Important:** Add the second trigger condition by clicking [+]. The first trigger condition tests for Status (Down), the second for the specific application instance (indicated by 1 Object).

5. For Trigger Actions, click Add Action, select Send an Email/Page, then click Configure Action.
6. Enter the required information, click Next and complete the wizard as instructed, then click Submit.
7. Review and edit the Reset Actions and the Summary, then click Submit.
8. The Manage Alerts page indicates the alert was created successfully.
Scan for applications to monitor

You can scan for applications to monitor as added nodes through the Scan Nodes for Applications page. SAM scans your network for applications. Select applications from the displayed list to add as monitored nodes.

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

1. On the Web Console, click Settings > All Settings > SAM Settings > Scan Nodes for Applications.
2. Select nodes by clicking [+] to expand the node groups, then select the nodes you want to scan, and then click Next.
3. Select applications to find, and then click Next.
4. Enter the credentials for the servers you are scanning, and then click Start Scan.
5. Click View SAM Summary Page, then click View results after the SAM scan is complete.
Monitor a specific URL

You can add a specific URL as a monitored node. All usage and performance displays as a node with details pages of collected data.

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

1. On the Web Console, click Settings > All Settings > Add a Node.
2. Enter the Hostname or IP Address you want to monitor (for example, www.google.com).
3. Select External Node: No Status, and then click Next.
4. From the Show only: drop-down, select Web Pages.
5. Check Web Link and select Inherit credentials from Template.

6. Click Test, and then click Next.
7. On the Change Properties page, make any changes, and then click OK, Add Node.
8. Navigate to the Node Details page to review the results. To do this, click My Dashboards > Home, and then drill down to your specific node in the All Nodes resource.
Monitor VMware performance counters using an application monitor

Learn more about monitoring VMware performance counters, used by application monitor templates and component monitors.

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

1. On the Web Console, click Settings > All Settings > SAM Settings > Component Monitor Wizard.
2. Select a VMware performance counter, then click Next.
3. Enter the IP address of the VMware node you want to browse, or click Browse, select the node from the list, and then click Select.
4. Select or enter the appropriate credentials, then click Next.
5. Select whether you want to monitor A single system or Multiple systems.
6. Choosing A single system provides specific counters that apply to the target system only, choosing Multiple systems provides more generic counters that can be applied to multiple systems. Choosing Multiple systems provides only aggregate performance counters (without instances). Therefore, the Application Monitor created based on them can be considered as generic and assigned to different ESX/vCenter target hosts. In this case, monitors in the application created contain the special `${VMWARE_ENTITY_NAME}` variable in the Entity Name field of the monitor. When the monitor runs, this variable is resolved to the first available entity on a target host with the desired Entity Type (for example, the first Host System).

7. Select the desired VMware Entity to monitor, then select the desired Performance Object (group) to monitor.
8. Select the counters to monitor for the selected Performance Object, then click Next.
9. From the Edit Properties page you can modify settings as desired. When done, click Next.

Add components to the application monitor

1. Click [+] next to Component list to expand the list of counters or counters to be added.
2. Select New Application Monitor. Then enter a name for the new Application Monitor, then click Next, then OK, Create.
3. Click View SAM Summary Page. Your new VMware monitor appears in the tree view for the All Applications resource. The polling results for the new monitor are updated after a few minutes.

- **Cluster Compute Resource** (only available if the VMware vCenter Performance Counter Monitor type is selected) – Data object that aggregates the computation resources of its associated Host System objects into one single computation resource for use by virtual machines. The cluster services such as HA (High Availability), DRS (Distributed Resource Scheduling), and EVC (Enhanced vMotion Compatibility), enhance the usefulness of this single computation resource. This Entity Type is specific to vCenter systems.

- **Host System** – Managed object type that provides access to a virtualization host platform.

- **Resource Pool** – Represents a set of physical resources which may be a single host, a subset of a host's resources, or resources spanning multiple hosts. You can subdivide Resource pools by creating child resource pools. In order to run, a virtual machine must be associated as a child of a resource pool. In a parent/child hierarchy of resource pools and virtual machines, the root resource pool is the single resource pool that has no parent pool.

- **Virtual Machine** – Managed object type for manipulating virtual machines, including templates that can be repeatedly deployed as new virtual machines. This object type provides methods for configuring and controlling a virtual machine.
Monitor and restart stopped Windows services

Learn more about monitoring and restarting stopped Windows services.

ℹ️ You may need to log in with an administrator account to perform these actions.

Create the monitor

1. On the Web Console, click Settings > All Settings > SAM Settings > Component Monitor Wizard.
2. Select Windows Service Monitor, and then click Next.
3. Enter the IP address of the Windows node you want to browse, or click Browse, select the node from the list, then click Select.
4. Enter or select the appropriate credentials, then click Next.
5. Check the services to monitor, adjust thresholds as needed, then click Next.
6. Ensure that New Application Monitor Template Name is selected and then enter a name for your new template, then click Next.
7. Select the desired nodes to monitor and then click Next.
8. Click OK, Create, to create the assigned Application Monitor.

Create an alert that restarts any stopped Windows services and sends an email

2. Click Add New Alert > Configure Alerts.
3. Scroll to the bottom of the list in the Manage Alerts dialog, and check the box for Restart a service.
4. To send an e-mail notification for the service restart:
   a. Highlight Restart a Service and click Edit.
   b. Select the Trigger Actions tab and then click Add New Action.
   c. Select Send an E-Mail / Page and click OK.
   d. Complete the e-mail info and click OK.
   e. Click OK.
5. Click Done.
Monitor large directories

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

1. On the Web Console, click Settings > All Settings > SAMSettings > Create a New Template.
2. Name the template, click Add Component Monitor, then expand the Custom Component Monitors group, select Windows Script Monitor, then click Submit.
3. Select credentials with appropriate permissions to run the script on the SolarWinds SAM server.
4. Copy the following Visual Basic script to get the directory size into the Script Body field:

```vbnet
Dim folderPath
folderPath = WScript.Arguments(0)
Set fs=WScript.CreateObject("Scripting.FileSystemObject")
Set folder= fs.GetFolder(folderPath)
WScript.Echo "Message: Folder " &folderPath & " is " & folder.Size & " bytes large"
WScript.Echo "Statistic: " & folder.Size
```
5. Enter the UNC path name for the directory to monitor into the Script Arguments field.

6. Enter the UNC path name for the directory to monitor into the Script Arguments field.

7. Use the variable `${IP}` for the IP address of the target node to which the monitor is assigned when the Windows Script monitor runs.

8. Specify the critical and warning thresholds for the desired directory size, then click Submit.
9. Create an assigned Application Monitor by assigning the Large Directory Monitor template to the node.
   a. On the Web Console, click Settings > All Settings > SAM Settings > Manually Assign Application Monitors.
   b. Select All in the Show only list, click Large Directory Monitor and then click Next.
   c. Click Manually Assign Application Monitors and Select All in the Show only list.
   d. Click Large Directory Monitor and then click Next.
   e. Locate and select the desired node and then click Next.
   f. Enter itadmin in the Credential Name field and then enter your credentials.
   g. Click Test, click Assign Application Monitors, and then click Done.

The Visual Basic code does the following:

a. Reads the first argument passed to the UNC path name for the directory to monitor and stores it in FolderPath.

Creates the `Scripting.FileSystemObject` and stores it in `fs`. 
a. Retrieves the folder name from the saved command line argument and stores it in folder.
b. Displays the message with the folder name and the folder size.
c. Displays the statistic (folder size in bytes).

ℹ️ The script does no error checking.
Monitor IIS application pools

SolarWinds SAM can monitor five instances, for example, of w3wp.exe, differentiated by application pools separately if you specify the application pool names in the component monitors.

1. From the SolarWinds Web Console, click Settings.
2. Add the web server to the Orion database.
   a. Click Add a Node then enter the hostname or IP address of the Intranet web server.
   b. Check the ICMP (Ping only) check box and then click Next.
   c. From the Add Application Monitors page, click Next.
   d. From the Change Properties page, Click OK, Add Node.
3. Find the w3wp.exe process on the web server.
   a. From the SolarWinds Web Console, click Settings > All Settings > SAM Settings > Component Monitor Wizard.
   b. Select Process Monitor - WMI as the monitor type, and then click Next.
   c. Click Browse, select the web server, and then click Select.
   d. Enter WebServerAdmin in the Credential Name field.
   e. Enter your credentials in the fields provided, then click Next.
   f. Click the last page button to view the last page, then check the check box next to w3wp.exe, and then click Next.
   g. Change Monitor Name to Webpool1, then enter webpool1 in the Command Line Filter field.
   h. Change the CPU Warning Threshold to greater than 40, then Change the CPU Critical Threshold to greater than 50.
   i. Click Add Another Component. After creating the monitors for all five w3wp.exe instances, click Next.
   j. Select New Application Monitor and enter Web Server Application Pools as the Application Monitor Name, and then click Next.
   k. Select the web server node, and then click Next, then click OK, Create.
Use the JMX component monitor wizard

Creating a standard template for this monitor is not practical because of the amount of variables in any one specific environment. However, adding this monitor to your environment has been made simple with the use of a wizard driven interface. For details, see the JMX monitor.

Only values that return numerical data can be monitored. String data is not supported at this time. Non-numerical data is shown without a check box.

Add a JMX component monitor

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

1. On the Web Console, click Settings > All Settings > SAM Settings > Component Monitor Wizard.
2. Select JMX Monitor from the drop down list and then click Next.
3. For Server IP Address, click Browse, then select the node you want to monitor.
4. Add the Port number, Protocol type, URL path, and Credentials for the remaining fields.
5. Click Next. The following MBean selection screen appears:

6. Expand the folders by clicking the arrows (or [+] ) to expand the tree view folder structure. From here you can drill down to select the attributes you want by checking them.
7. Click Next.
Configure the SOAP monitor

The are two ways to configure the SOAP monitor:

- Loading a WSDL file.
- Manually entering XML.

Load WSDL Files

The SOAP monitor within SAM currently supports the WSDL schema, which must be exposed on a URL. After the WSDL file is successfully loaded, the file is parsed automatically, the fields populate (as shown next), and you can specify values for the available arguments. There are two types of arguments: simple and complex.

A simple argument is one where you define the value directly. A complex argument (for example, one that includes structures, classes, and lists) must be user-defined in the XML format. SolarWinds recommends that only experienced users compose complex arguments.

**Advanced Settings are read-only and display additional information. Because the SOAP envelope is based on the WSDL schema, the Advanced Settings values should not be changed.**

The SOAP XML field contains the SOAP envelope which is generated by the WSDL and dynamically changes as you change the SOAP settings. Use this field to confirm what will be sent to the web service.
Important: If changes are made to any of the base SOAP settings, the content of the SOAP XML is re-generated and your changes become lost.

Manually Enter XML

The following is an example of a Complex argument and would be placed in the Parameters field. SAM automatically takes the code and place it where it belongs in the envelope:

```xml
<tempPhoneNumber xmlns:ns2="http://schemas.xmlsoap.org/soap/encoding/
 xsi:type="ns2:Array" ns2:arrayType="ns1:TemporaryPhoneNumber[3]">
  <item xsi:type="ns1:TemporaryPhoneNumber">
    <startDate xsi:type="xsd:int">37060</startDate>
    <endDate xsi:type="xsd:int">37064</endDate>
  </item>
</tempPhoneNumber>
```
<phoneNumber xsi:type="xsd:string">+1-212-5551234</phoneNumber>
</item>
<item xsi:type="ns1:TemporaryPhoneNumber">
  <startDate xsi:type="xsd:int">37074</startDate>
  <endDate xsi:type="xsd:int">37078</endDate>
  <phoneNumber xsi:type="xsd:string">+1-212-5554321</phoneNumber>
</item>
<item xsi:type="ns1:TemporaryPhoneNumber">
  <startDate xsi:type="xsd:int">37088</startDate>
  <endDate xsi:type="xsd:int">37092</endDate>
  <phoneNumber xsi:type="xsd:string">+1-212-5557890</phoneNumber>
</item>
</tempPhoneNumber>

XML can also be entered manually by typing or pasting XML.

![SOAP Settings](image)

**SOAP Settings**

**SOAP XML Request:** Manually enter SOAP XML Request

**Web Service Server URL:**

**SOAP Action:**

**SOAP Version:** 1.1

**SOAP XML:**

```xml
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:query="http://2007/08/informationsservice">
  <query>select co</query>
  <soap:Body/>
</soap:Envelope>
```
Assign an application template to a group

Assigning an application template to a group is more efficient than applying the template to individual nodes one at a time. Before you begin, a group must be created. To create a group, see Create groups.

![Tip]
The process may take about 10 minutes for templates to be assigned to the group. If the templates do not assign, you may need to restart services to verify.

![Note]
Nested groups are not supported. AppInsight applications cannot be assigned to groups. Application assignment to a group happens in the background and can take some time to be created depending on the size of the application.

1. On the web console, click Settings > All Settings > SAM Settings > Manage Templates > Application Monitor Templates.
2. Select an application template and then click, Assign to Group.

![Image]
Manage Application Monitor Templates

Listed below are application monitor templates. Application monitor templates are a group of component monitors that have not been assigned yet. Application monitor templates will inherit the changes.

- Select tag to filter by:
  - All (227)
  - Active Directory (4)
  - Apache (4)

- Actions:
  - CREATE NEW TEMPLATE
  - ASSIGN TO NODE
  - ASSIGN TO GROUP
  - Assign to Group
  - Unassign from Group

page 477
3. Select a group from the Available Groups column, click the green arrow, and then click Next.

   By default, the template is assigned to those nodes in the group that are running a server operating system. This can be changed in the Advanced section at the bottom of the page. When a node is removed from a group, the application is deleted from the node by default. You can override this by selecting No under the Advanced section.

4. Select your credentials and then click, Assign Groups.

5. Click Done.

Your application templates are now assigned to a group.

To view the applications within a group, in the web console, click My Dashboards > SAM Summary and then click a group in the Application Templates Assigned to Group resource.
You can create dynamic groups and assign templates to these groups. For example, a dynamic group can be created for all Windows computers and the Windows Update template can be applied to the nodes of the group dynamically.
Use alerts to monitor your environment

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
- Best practices and tips for alerting
- Navigate to the Alert Manager
- Create new alerts to monitor your environment
- Alert me when a server goes down

You can also view our Alert Lab on THWACK for community-based alert information.

Alert preconfiguration tasks

Some alerts require extra configuration, separate software installations, or 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
- Dial a paging or SMS service
- Play a sound when an alert is triggered
- Send an SNMP trap
- Use the speech synthesizer to read alerts

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

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

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

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

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.
SAM alert variables

SAM supplements the alerting abilities of the Orion Platform with a number of SAM-specific configurable alerts and variables.

- Component Monitor properties for alerts
- Component Monitor variables for alerts
- Application Monitor properties for alerts
- Application Monitor variables for alerts

Component Monitor properties for alerts

The following alert possibilities for component monitors.

**Component Name**

This allows you to base your alert criteria on component names.

**Component Type**

This allows you to base your alert criteria on component types. Specify the component monitor type by value using the following table.

<table>
<thead>
<tr>
<th>COMPONENT MONITOR TYPE</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>DHCP User Experience Monitor</td>
<td>35</td>
</tr>
<tr>
<td>Directory Size Monitor</td>
<td>38</td>
</tr>
<tr>
<td>DNS Monitor - TCP</td>
<td>4</td>
</tr>
<tr>
<td>DNS Monitor - UDP</td>
<td>5</td>
</tr>
<tr>
<td>DNS User Experience Monitor</td>
<td>15</td>
</tr>
<tr>
<td>Download Speed Monitor</td>
<td>25</td>
</tr>
<tr>
<td>File Age Monitor</td>
<td>36</td>
</tr>
<tr>
<td>File Change Monitor</td>
<td>23</td>
</tr>
<tr>
<td>File Count Monitor</td>
<td>39</td>
</tr>
<tr>
<td>File Existence Monitor</td>
<td>28</td>
</tr>
<tr>
<td>File Size Monitor</td>
<td>22</td>
</tr>
<tr>
<td>COMPONENT MONITOR TYPE</td>
<td>VALUE</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>FTP Monitor</td>
<td>7</td>
</tr>
<tr>
<td>FTP User Experience Monitor</td>
<td>24</td>
</tr>
<tr>
<td>HTTP Form Login Monitor</td>
<td>27</td>
</tr>
<tr>
<td>HTTP Monitor</td>
<td>6</td>
</tr>
<tr>
<td>HTTPS Monitor</td>
<td>14</td>
</tr>
<tr>
<td>IMAP4 Monitor</td>
<td>13</td>
</tr>
<tr>
<td>IMAP4 User Experience Monitor</td>
<td>30</td>
</tr>
<tr>
<td>JMX Monitor</td>
<td>49</td>
</tr>
<tr>
<td>LDAP User Experience Monitor</td>
<td>34</td>
</tr>
<tr>
<td>Linux/Unix Script Monitor</td>
<td>21</td>
</tr>
<tr>
<td>MAPI User Experience Monitor</td>
<td>31</td>
</tr>
<tr>
<td>Nagios Script Monitor</td>
<td>50</td>
</tr>
<tr>
<td>NNTP Monitor</td>
<td>11</td>
</tr>
<tr>
<td>ODBC User Experience Monitor</td>
<td>16</td>
</tr>
<tr>
<td>Oracle User Experience Monitor</td>
<td>18</td>
</tr>
<tr>
<td>Performance Counter Monitor</td>
<td>37</td>
</tr>
<tr>
<td>POP3 Monitor</td>
<td>12</td>
</tr>
<tr>
<td>POP3 User Experience Monitor</td>
<td>29</td>
</tr>
<tr>
<td>Process Monitor – SNMP</td>
<td>8</td>
</tr>
<tr>
<td>Process Monitor - WMI</td>
<td>1</td>
</tr>
<tr>
<td>RADIUS User Experience Monitor</td>
<td>40</td>
</tr>
<tr>
<td>SMTP Monitor</td>
<td>10</td>
</tr>
<tr>
<td>SNMP Monitor</td>
<td>32</td>
</tr>
<tr>
<td>SQL User Experience Monitor</td>
<td>17</td>
</tr>
<tr>
<td>TACACS+ User Experience Monitor</td>
<td>41</td>
</tr>
<tr>
<td>COMPONENT MONITOR TYPE</td>
<td>VALUE</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>TCP Port Monitor</td>
<td>2</td>
</tr>
<tr>
<td>Tomcat Server Monitor</td>
<td>33</td>
</tr>
<tr>
<td>Web Link Monitor</td>
<td>26</td>
</tr>
<tr>
<td>Windows Event Monitor</td>
<td>42</td>
</tr>
<tr>
<td>Windows PowerShell Monitor</td>
<td>45</td>
</tr>
<tr>
<td>Windows Script Monitor</td>
<td>20</td>
</tr>
<tr>
<td>Windows Service Monitor</td>
<td>9</td>
</tr>
<tr>
<td>WMI Monitor</td>
<td>19</td>
</tr>
</tbody>
</table>

**Component Status**

This allows you to alert on Critical, Down, Unknown, Up, and Warning status.

**Response Time**

This allows you to alert on response time.

**Statistic Data**

This allows you to alert on statistic data.

**Process (Service) Name**

This allows you to alert on the process or service name. For example: dns.exe, or AlertingEngine.

**Process Instance Count**

This allows you to alert on the instance count of a process.

**Percent CPU**

This allows you to alert on the percentage of CPU in use of a monitored process or service.

**Percent Physical Memory**

This allows you to alert on the percentage of physical memory in use of a monitored process or service.

**Percent Memory Used**

This allows you to alert on the percentage of total memory in use of a monitored process or service.
Percent Virtual Memory

This allows you to alert on the percentage of virtual memory in use of a monitored process or service.

Virtual Memory Used

This allows you to alert on the amount of virtual memory in use, in bytes, of a monitored process or service.

Component Monitor variables for alerts

The following variables are available when selecting APM-Component as the property type.

<table>
<thead>
<tr>
<th>COMPONENT MONITOR VARIABLE</th>
<th>MACRO</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>${APM:ComponentDetailsURL}</td>
<td>${N=SwisEntity;M=DetailsUrl}</td>
<td>Hyperlink to the Component Details page that triggered the alert.</td>
</tr>
<tr>
<td>${ApplicationId}</td>
<td>${N=SwisEntity;M=Application.ApplicationID}</td>
<td>Provides the unique numeric identifier of the application. This value is analogous to the node ID.</td>
</tr>
<tr>
<td>${ApplicationName}</td>
<td>${N=SwisEntity;M=Application.ApplicationAlert.ApplicationName}</td>
<td>Provides the name of the monitored application.</td>
</tr>
<tr>
<td>${ApplicationStatus}</td>
<td>${N=SwisEntity;M=Application.Status}</td>
<td>Provides the status</td>
</tr>
<tr>
<td>COMPONENT MONITOR VARIABLE</td>
<td>MACRO</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td>${ComponentId}</td>
<td>${N=SwisEntity;M=ComponentAlert.ComponentID}</td>
<td>Provides the numeric component ID of the specific application.</td>
</tr>
<tr>
<td>${ComponentMessage}</td>
<td>${N=SwisEntity;M=ComponentAlert.ComponentMessage}</td>
<td>Message sent when alerting on component status.</td>
</tr>
<tr>
<td>${ComponentName}</td>
<td>${N=SwisEntity;M=ComponentAlert.ComponentName}</td>
<td>Provides the name of the component, for example, SW Module Engine.</td>
</tr>
<tr>
<td>${ComponentStatus}</td>
<td>${N=SwisEntity;M=Status}</td>
<td>Provides the status of the specific component.</td>
</tr>
<tr>
<td>${ComponentType}</td>
<td>${N=SwisEntity;M=ComponentAlert.ComponentType}</td>
<td>Provides the numeric component type.</td>
</tr>
<tr>
<td>COMPONENT MONITOR VARIABLE</td>
<td>MACRO</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td><code>${DisplayType}</code></td>
<td><code>${N=SwisEntity;M=ComponentAlert.DisplayType}</code></td>
<td>Provides the display type for the specific monitor. For example, Windows Service.</td>
</tr>
<tr>
<td><code>${LastTimeUp}</code></td>
<td><code>${N=SwisEntity;M=ComponentAlert.LastTimeUp}</code></td>
<td>Provides the date and time the component was last seen in the Up state.</td>
</tr>
<tr>
<td><code>${MemoryUsed}</code></td>
<td><code>${N=SwisEntity;M=ComponentAlert.MemoryUsed}</code></td>
<td>Provides the memory used by a component, in bytes.</td>
</tr>
<tr>
<td><code>${MultiValueMessages}</code></td>
<td><code>${N=SwisEntity;M=ComponentAlert.MultiValueMessages}</code></td>
<td>Message sent when alerting on the Multiple Value Chart.</td>
</tr>
<tr>
<td><code>${MultiValueStatistics}</code></td>
<td><code>${N=SwisEntity;M=ComponentAlert.MultiValueStatistics}</code></td>
<td>Statistics sent when alerting on the Multiple Value</td>
</tr>
<tr>
<td>COMPONENT MONITOR VARIABLE</td>
<td>MACRO</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td>${NodeID}</td>
<td>${N=SwisEntity;M=ComponentAlert.NodeId}</td>
<td>Provides the numeric node ID of the server on which the application is monitored.</td>
</tr>
<tr>
<td>${PercentApplicationAvailability}</td>
<td>${N=SwisEntity;M=ComponentAlert.PercentApplicationAvailability}</td>
<td>Provides the availability of an application as a percentage.</td>
</tr>
<tr>
<td>${PercentComponentAvailability}</td>
<td>${N=SwisEntity;M=ComponentAlert.PercentComponentAvailability}</td>
<td>Provides the availability of a component as a percentage.</td>
</tr>
<tr>
<td>${PercentCPU}</td>
<td>${N=SwisEntity;M=ComponentAlert.PercentCPU}</td>
<td>Provides the amount of CPU used by a component as a percentage.</td>
</tr>
<tr>
<td>COMPONENT MONITOR VARIABLE</td>
<td>MACRO</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>${PercentMemory}</code></td>
<td><code>${N=SwisEntity;M=ComponentAlert.PercentMemory}</code></td>
<td>Provides the memory used by a component as a percentage.</td>
</tr>
<tr>
<td><code>${PercentVirtualMemory}</code></td>
<td><code>${N=SwisEntity;M=ComponentAlert.PercentVirtualMemory}</code></td>
<td>Provides the virtual memory used by a component as a percentage.</td>
</tr>
<tr>
<td><code>${ProcessInstanceCount}</code></td>
<td><code>${N=SwisEntity;M=ComponentAlert.ProcessInstanceCount}</code></td>
<td>Provides the instance count of a process.</td>
</tr>
<tr>
<td><code>${ProcessName}</code></td>
<td><code>${N=SwisEntity;M=ComponentAlert.ProcessName}</code></td>
<td>Provides the process name.</td>
</tr>
<tr>
<td><code>${ResponseTime}</code></td>
<td><code>${N=SwisEntity;M=ComponentAlert.ResponseTime}</code></td>
<td>Provides the response time of a component.</td>
</tr>
<tr>
<td><code>${StatisticData}</code></td>
<td><code>${N=SwisEntity;M=ComponentAlert.StatisticData}</code></td>
<td>Provides the statistics data value of a</td>
</tr>
<tr>
<td>COMPONENT MONITOR VARIABLE</td>
<td>MACRO</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>${StatusOrErrorDescription}</td>
<td>${N=SwisEntity;M=ComponentAlert.StatusOrErrorDescription}</td>
<td>Provides the status of the component, including the full text of any error messages.</td>
</tr>
<tr>
<td>${Threshold-CPU-Critical}</td>
<td>${N=SwisEntity;M=ComponentAlertThresholds.ThresholdCPU Critical}</td>
<td>Provides the critical threshold for CPU.</td>
</tr>
<tr>
<td>${Threshold-CPU-Warning}</td>
<td>${N=SwisEntity;M=ComponentAlertThresholds.ThresholdCPU Warning}</td>
<td>Provides the Warning threshold for the CPU.</td>
</tr>
<tr>
<td>${Threshold-PhysicalMemory-Critical}</td>
<td>${N=SwisEntity;M=ComponentAlertThresholds.ThresholdPhysicalMemory Critical}</td>
<td>Provides the Critical threshold for physical memory.</td>
</tr>
<tr>
<td>${Threshold-PhysicalMemory-Warning}</td>
<td>${N=SwisEntity;M=ComponentAlertThresholds.ThresholdPhysicalMemory Warning}</td>
<td>Provides the Warning threshold for physical memory.</td>
</tr>
<tr>
<td>${Threshold-ResponseTime-Critical}</td>
<td>${N=SwisEntity;M=ComponentAlertThresholds.ThresholdResponseTime Critical}</td>
<td>Provides the Critical threshold for response time.</td>
</tr>
<tr>
<td>COMPONENT MONITOR VARIABLE</td>
<td>MACRO</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td>${Threshold-ResponseTime-Warning}</td>
<td>${N=SwisEntity;M=ComponentAlertThresholds.ThresholdResponseTimeWarning}</td>
<td>Provides the Warning threshold for response time.</td>
</tr>
<tr>
<td>${Threshold-Statistic-Critical}</td>
<td>${N=SwisEntity;M=ComponentAlertThresholds.ThresholdStatisticCritical}</td>
<td>Provides the Critical threshold for statistics.</td>
</tr>
<tr>
<td>${Threshold-Statistic-Warning}</td>
<td>${N=SwisEntity;M=ComponentAlertThresholds.ThresholdStatisticWarning}</td>
<td>Provides the Warning threshold for statistics.</td>
</tr>
<tr>
<td>${Threshold-VirtualMemory-Critical}</td>
<td>${N=SwisEntity;M=ComponentAlertThresholds.ThresholdVirtualMemoryCritical}</td>
<td>Provides the Critical threshold for virtual memory.</td>
</tr>
<tr>
<td>${Threshold-VirtualMemory-Warning}</td>
<td>${N=SwisEntity;M=ComponentAlertThresholds.ThresholdVirtualMemoryWarning}</td>
<td>Provides the Warning threshold for virtual memory.</td>
</tr>
<tr>
<td>${TimeStamp}</td>
<td>${N=SwisEntity;M=CurrentStatus.ObservationTimestamp}</td>
<td>Provides</td>
</tr>
<tr>
<td>COMPONENT MONITOR VARIABLE</td>
<td>MACRO</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the last polling date and time of a component.</td>
</tr>
<tr>
<td>${UserDescription}</td>
<td>${N=SwisEntity;M=ComponentAlert.UserDescription}</td>
<td>Provides a description of the component. Note: A default description is given by SolarWinds. Any changes you make will override the default description and be automatically saved.</td>
</tr>
<tr>
<td>${UserNotes}</td>
<td>${N=SwisEntity;M=ComponentAlert.UserNotes}</td>
<td>Provides notes from the user about a component. Changes you make will automatically be saved.</td>
</tr>
</tbody>
</table>
### COMPONENT MONITOR VARIABLE | MACRO | DEFINITION
--- | --- | ---
${WindowsEventMessages} | ${N=SwisEntity;M=ComponentAlert.WindowsEventMessages} | Full details of the corresponding event.

<table>
<thead>
<tr>
<th>COMPONENT MONITOR VARIABLE</th>
<th>MACRO</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>${VirtualMemoryUsed}</td>
<td>${N=SwisEntity;M=ComponentAlert.VirtualMemoryUsed}</td>
<td>Provides the virtual memory used by a component, in bytes.</td>
</tr>
</tbody>
</table>

### Application Monitor properties for alerts

You can use the following properties in alerts for application monitors.

- **Application Name**
  
  This allows you to select the names of currently configured application templates as values.

- **Application Status**
  
  This allows you to select whether the application is in a Critical, Down, Unknown, Up, or Warning status.

### Application Monitor variables for alerts

The following variables are available when selecting APM-Application as the property type.

<table>
<thead>
<tr>
<th>APPLICATION VARIABLE</th>
<th>MACRO</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>${APM:ApplicationDetailsURL}</td>
<td>${N=SwisEntity;M=DetailsUrl}</td>
<td>Hyperlink to the Application Details page that</td>
</tr>
<tr>
<td><strong>APPLICATION VARIABLE</strong></td>
<td><strong>MACRO</strong></td>
<td><strong>DEFINITION</strong></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------</td>
<td>----------------</td>
</tr>
<tr>
<td>${Availability}$</td>
<td>${N=SwisEntity;M=ApplicationAlert.ApplicationAvailability}$</td>
<td>Provides the status of the application.</td>
</tr>
<tr>
<td>${ComponentsWithProblems}$</td>
<td>${N=SwisEntity;M=ApplicationAlert.ComponentsWithProblems}$</td>
<td>Provides a comma-delimited list of components in a Down, Unknown, Warning, or Critical state.</td>
</tr>
<tr>
<td>${ComponentsWithProblemsFormatted}$</td>
<td>${N=SwisEntity;M=ApplicationAlert.ComponentsWithProblemsFormatted}$</td>
<td>List of components that</td>
</tr>
<tr>
<td>APPLICATION VARIABLE</td>
<td>MACRO</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td>${ComponentsWithProblemsFormattedHtml}$</td>
<td>${N=SwisEntity;M=ApplicationAlert.ComponentsWithProblemsFormattedHtml}$</td>
<td>List of components that are not Up along with the component status. Formatted with HTML tags for the Send e-mail action to provide an improved appearance of the listed components.</td>
</tr>
<tr>
<td>APPLICATION VARIABLE</td>
<td>MACRO</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td>${\text{ComponentsWithStatus}}$</td>
<td>${N=\text{SwisEntity}; \text{M=ApplicationAlert.ComponentsWithStatus}}$</td>
<td>Provides a comma-delimited list of all components and their current status.</td>
</tr>
<tr>
<td>${\text{ComponentsWithStatusFormatted}}$</td>
<td>${N=\text{SwisEntity}; \text{M=ApplicationAlert.ComponentsWithStatusFormatted}}$</td>
<td>List of components with component status included formatted with HTML tags. HTML formatting is used for send e-mail action to provide improved</td>
</tr>
<tr>
<td>APPLICATION VARIABLE</td>
<td>MACRO</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td>${ComponentsWithStatusFormattedHtml}</td>
<td>${N=SwisEntity;M=ApplicationAlert.ComponentsWithStatusFormattedHtml}</td>
<td>List of components with the component status. Formatted with HTML tags for events that appear in the web console.</td>
</tr>
<tr>
<td>${ID}</td>
<td>${N=SwisEntity;M=Application.ApplicationID}</td>
<td>Provides the numeric application ID of the specific application.</td>
</tr>
<tr>
<td>${LastTimeUp}</td>
<td>${N=SwisEntity;M=CurrentStatus.LastTimeUp}</td>
<td>Provides the date and time the application was</td>
</tr>
<tr>
<td>APPLICATION VARIABLE</td>
<td>MACRO</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>-------</td>
<td></td>
</tr>
<tr>
<td>${Name}</td>
<td>${N=SwisEntity;M=Application.ApplicationAlert.ApplicationName}</td>
<td></td>
</tr>
<tr>
<td>Last seen in an Up state.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provides the name of the application that is triggering the alert.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>${NodeID}</td>
<td>${N=SwisEntity;M=Application.Node.NodeID}</td>
<td></td>
</tr>
<tr>
<td>Provides the numeric node ID of the server on which the application is monitored.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>${SystemSummaryFormatted}</td>
<td>${N=SwisEntity;M=Application.ApplicationAlert.SystemSummaryFormatted}</td>
<td></td>
</tr>
<tr>
<td>System summary. HTML formatting is used for the Send e-mail action to provide an improve</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>APPLICATION VARIABLE</strong></td>
<td><strong>MACRO</strong></td>
<td><strong>DEFINITION</strong></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------</td>
<td>----------------</td>
</tr>
<tr>
<td><code>${SystemSummaryFormattedHtml}</code></td>
<td><code>${N=SwisEntity;M=ApplicationAlert.SystemSummaryFormattedHtml}</code></td>
<td>System summary. Formatted with HTML tags for events that appear in the web console.</td>
</tr>
<tr>
<td><code>${TimeStamp}</code></td>
<td><code>${N=SwisEntity;M=Application.CurrentStatus.ObservationTimestamp}</code></td>
<td>Provides the last polling date and time of an application.</td>
</tr>
</tbody>
</table>

Create new alerts to monitor your environment

Navigate to the Alert Manager 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

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

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. To see an example of completed trigger conditions, see the Alert me when a server goes down topic.

Trigger conditions are built using child conditions that are evaluated in order. Child conditions are represented as a line item under the Actual Trigger Condition. You can have multiple trigger condition blocks with multiple child conditions.

Filter your environment to 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.

   - All objects in my environment (Show List)
   - Only following set of objects

   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

   i. 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

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](#) or [Build complex conditions](#) 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**

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.
   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

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

The Summary tab allows you to check your alert definition before you save any changes.

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.

Commonly created alerts

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

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.
   - Select and enter a value for Condition must exist for more than to prevent being alerted when a node enters the down state frequently within a set amount of time. This prevents you from receiving alerts until the node has been in the down state for longer than the time you have selected.
   - 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.
    - Enter the location of the log. For example, enter C:\ExampleAlertLog.txt in the Alert Log Filename Field.
    - In the Message text box, type Node ${N=SwisEntity;M=Caption} is currently down.
    - 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
      \( \text{${N=Alerting;M=AcknowledgUrl}$} \).

   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

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.

You can use variables to customize your message. You can also use a variable that allows you to acknowledge an alert from email
\( \text{${N=Alerting;M=AcknowledgUrl}$} \).

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:
      Node \( \text{${N=SwisEntity;M=Caption}$} \) is currently down.
   c. Click Add Action.
7. Click Add Action, and select Send a Syslog Message. Click Configure Action.
   a. Type 127.0.0.1 as the Hostname or IP Address of the Syslog Server, and then type the following in the Message field:
      Node ${N=SwisEntity;M=Caption} is currently down.
   b. Click Add Action.

8. Click Add Action, and select Send SNMP Trap. Click Configure Action.
   a. Type 127.0.0.1 as the SNMP Trap Destination, and then type the following in the Alert Message field:
      Node ${N=SwisEntity;M=Caption} is currently down.
   b. Click Next.
   c. Click Add Action.

9. Click Summary 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 > Syslog and SNMP Traps > Trap Viewer.

**View triggered 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 resource to any view.

**Remove alerts from the Active Alerts list**

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.

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

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.

The Send Email/Page, Play a Sound, and Text to Speech Output actions do not have to fire. You can view what the message will look like when the trigger or reset action fires without performing the action.

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 and SNMP Traps > Syslog Viewer.
- To view the results of your Syslog message action, click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer.

Modify multiple alerts or share alerts

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.

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

SolarWinds customers share their customized alerts in the SolarWinds THWACK community. Visit 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, and delete before making it public. Also review your company policy on sharing this type of file.

# Build complex conditions

Complex conditions are generally enabled by users who are comfortable with building normal trigger conditions, or who have trialed alerts using the normal trigger conditions and require more control over the trigger conditions to better refine the environmental conditions that trigger an alert.

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

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: \( (\text{Node Status} = \text{Up}) \ \text{AND} \ (\text{Percent Loss} \geq 75) \ \text{AND} \ (\text{CPU Load} \geq 85) \)

**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**

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**

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.

![Drop-down menu](image)

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.

\[(\text{Condition A}) \& (\text{Condition B}) \& (\text{Condition C})\]

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

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

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.

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.

Available alert actions

Orion Platform products provide a variety of actions to signal an alert condition on your network.

Change a custom property

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

This alert management 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.

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®.

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>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.

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. Then you will be able to use the properties as reference fields.

5. Under State Management, define the status of the incident when the incident is reset, reopened, acknowledged, and closed. 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.

Dial a paging or SMS service

This action forwards alerts to a paging or SMS service. You must download and install NotePager Pro from Notepage.net to your Orion server to use this action.


Email a web page to users

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.
   > Multiple addresses must be separated with commas.
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.
   > Use variables to make the message dynamic.
   - You can create a dynamic URL to send information about the object that triggered the alert.
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**

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.

   **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 external program runs.
Execute an external Visual Basic script

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.

   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 VB script runs.

Log the alert message to a file

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

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.

      This option is only available if the alert is built to trigger for virtual machines.

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.

      This is often used to prevent an action from occurring during specific windows.

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

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

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**

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.
   
   🔄 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.  

   ! 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**

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.  
      ! 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.  

   ! 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

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.
      
      ![Info icon] 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.
   
   ![Info 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 powered off.

Power on a virtual machine

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.
      
      ![Info icon] 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.
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

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.
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

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

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

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.
Send a Windows Net message

If a computer is experiencing issues, you can have an alert trigger a Windows Net Message to be sent to a specific computer or to all computers.

Alerts can be configured to display a pop-up Windows Net Message either on a specific computer or on all computers in a selected domain or workgroup. The following steps configure Windows Net messaging for triggered or reset alerts.

The only operating systems supporting Windows Net Messaging are Windows Server 2003 and Windows XP or earlier.

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 Net Message option, then click Configure Action.
3. Under Send a Net Message settings:
   a. Enter Computer Name or IP address in the field provided.
      You can enter multiple computers or IP addresses by separating them with commas.
   b. 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 message is sent to the selected computers.

Restart IIS sites or application pools

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

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.
      ! Multiple IP Addresses should be separated by commas or semicolons.
   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.
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

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.
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

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.

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 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

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.

   - You must provide at least one email address in the To field, and multiple addresses must be separated by commas. Some pager systems require a valid reply address to complete the page.
   - Messaging is disabled if both the Subject and Message fields are empty.

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

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 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

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

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.

**Changes in the alerting engine**

As of Orion Platform version 2015.1, alerts are no longer created with the desktop-based, Advanced Alerts Manager or Basic Alerts Manager. Alerts are instead created and managed in the SolarWinds Orion Web Console.

Alerts that you created in the desktop-based Alert Manager are migrated to the web-based alerting engine when upgrading to Core version 2015.1 or later. Some alerts may not be successfully migrated and include information about why they were not migrated in the migration log. You can view the alert migration logs in the informational banners displayed after you update your installation.

**Changed or removed functionality**

The suppression section has not been carried over to web-based alerting. Use options, such as Condition must exist for more than, in the trigger conditions to accomplish similar tasks.

**Database changes**

The following are a list of tables that have been changed that you may be using in custom SQL queries:

- Engines has been renamed to AllEngines.
- Nodes has been split into NodesCustomProperties, NodesData, and NodesStatistics.
- History has been split into table-specific history tables, such as the AlertHistory table.

The new alerting engine also includes the following new alerting tables:

- Actions
- ActionsAssignments
- ActionsProperties
- AlertActive
- AlertActiveObjects
- AlertConditionState
Macro or variable changes

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.

Alert migration to the web

The Advanced Alert Manager and the Basic Alert Manager are deprecated in SolarWinds Orion Core 2015.1 and later. A web-based alerting engine replaces the previous alerting engine and includes new alerting variables.

To facilitate using the web-based alerting engine, part of the upgrade process migrates alerts created with the desktop-based alerting engine to the web-based alerting engine. All alerts are migrated, including alerts that are disabled.

Migration issues

Some alerts may not be successfully migrated. The migration log records all alerts that are migrated and includes error messages for alerts that either cannot be migrated or that are not migrated successfully.

Common reasons that migration may not be successful include:

- **Invalid alert variables or macros** - Some variables are no longer supported.
- Invalid conditions - Some conditions are no longer supported.
- Large alert scope - The number of objects that are relevant to an alert may be too large to migrate.
Limitations to migrated alerts

After an alert has been migrated, you can only view the alert definition through the web-based Alert Manager. You can no longer click the alert in the views.

General alert variables

The following are valid, general alert variables.

<table>
<thead>
<tr>
<th>General Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${N=Alerting;M=AlertID}</td>
<td>The ID of the alert</td>
</tr>
<tr>
<td>${N=Alerting;M=AlertName}</td>
<td>The name of the alert from the alert field Name of alert definition in Alert Properties</td>
</tr>
<tr>
<td>${N=Alerting;M=AlertDescription}</td>
<td>The description of the alert from the alert field Description of alert definition in Alert Properties</td>
</tr>
<tr>
<td>${N=Alerting;M=AlertDetailsURL}</td>
<td>The URL used to get more information about the triggered alert</td>
</tr>
<tr>
<td>${N=Alerting;M=AlertMessage}</td>
<td>The alert message from the alert field Message displayed when this alert is triggered in Trigger Actions</td>
</tr>
<tr>
<td>${N=Alerting;M=DownTime}</td>
<td>The amount of time the alert has been active</td>
</tr>
<tr>
<td>${N=Alerting;M=ObjectType}</td>
<td>The object type that the alert is monitoring</td>
</tr>
<tr>
<td>${N=Alerting;M=Severity}</td>
<td>The severity of the alert from the alert field Severity of Alert in Alert Properties</td>
</tr>
<tr>
<td>${N=Alerting;M=LastEdit}</td>
<td>The last time the alert definition has been edited</td>
</tr>
<tr>
<td>${N=Alerting;M=Acknowledged}</td>
<td>Acknowledged status</td>
</tr>
<tr>
<td>${N=Alerting;M=AcknowledgedBy}</td>
<td>Who the alert was acknowledged by</td>
</tr>
<tr>
<td>${N=Alerting;M=AcknowledgedTime}</td>
<td>Time the alert was acknowledged</td>
</tr>
<tr>
<td>${N=Alerting;M=Notes}</td>
<td>Information from the Notes field when you acknowledge alerts through the Web Console</td>
</tr>
<tr>
<td>${N=Alerting;M=AlertTriggerCount}</td>
<td>Count of triggers</td>
</tr>
<tr>
<td>${N=Alerting;M=AlertTriggerTime}</td>
<td>Date and time of the last event for this alert. (Windows control panel defined “Short Date” and “Short Time”)</td>
</tr>
<tr>
<td>${N=Generic;M=Application}</td>
<td>SolarWinds application information</td>
</tr>
</tbody>
</table>
It is possible to use previous generation variables, for example \${NodeName}. However, when using the variable picker, the new format is displayed by default. Previous generation variables can only be entered manually.

Some variables are no longer valid.

### Defunct alert variables

The following variables are no longer valid:

- \${Property} - The property the alert is monitoring. You can select a new variable with the specific property you want to view.
- \${TriggeredValue} - The value that triggered the alert. You can select a new variable with the specific property you want to view.
- \${AlertStartTime} - When the alert active. You can use the Time of Day scheduler to control when the alert is active.
- \${AlertEndTime} - When the alert is no longer active. You can use the Time of Day scheduler to control when the alert is not active.
- \${ObjectSubType} - Determines if the node supports SNMP or is ICMP only. You can use Node.ObjectSubType as the macro name.

### Share 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.

- This 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 reports in the Orion Web Console

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

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

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

Predefined reports

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

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

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.

![Edit Resource: Availability of Each Node]

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**

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

You can include any Orion Web Console resource, 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 resource.
2. Use the Group by field to filter the available resources or search for a specific resource.

   ! The Classic category grouping provides the most comprehensive list of available resources.

3. Select the resource 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.

4. Click Select and Continue.
5. If the resource 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 resource 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

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.
     1. Filter or search for the objects you want to include.
     2. Select the objects' check boxes.
   - Dynamic Query Builder - use to select objects based on object properties.
     1. Select Basic Selector to create and/or queries or select Advanced Selector to create complex queries.
     2. Choose the object type you want to include.
     3. Enter your conditions.
   - Advanced DataBase Query (SQL, SWQL) - only use if you are comfortable querying your SolarWinds database directly using SQL or SWQL.
     1. Select SQL or SWQL, and enter your query.
     2. 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.

   The groups available and the data series within these groups will depend on the object selected.

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.

   It is possible to select a sample interval that is longer than the reporting period.

9. Choose how you want to filter your report.

   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**

Use report limitation categories to limit access to any SolarWinds report created on SolarWinds Orion Platform versions 2013.1 and later. Users with a report limitation category set can only see reports that are in the same report limitation category.

- The No Reports limitation is a special report limitation category that removes all access to reports when applied to a user account. You do not need to add No Reports as a limitation in the report properties.

- If you are running SolarWinds Orion Platform versions 2012.2.X or earlier, reports are stored in a folder on the primary SolarWinds server (default location C:\Program Files\SolarWinds\Orion\Reports). Place reports into subfolders and restrict user access to the file system to limit user access.
- If you are running SolarWinds Orion Platform version 2013.1.X or later, reports are stored in the SolarWinds database, and both users and reports may be assigned a report limitation category to restrict who can access the report.
Create or add a report limitation category

When you create or edit a report, expand Report Limitation on the Properties page to add a report limitation. Choose an existing limitation or enter a new one.

- Each report can have only one limitation.

After the report limitation is created and the report saved, the limitation is available in the user settings.

Restrict user access to the report

After the report limitation is saved, it is available in the user account's Define Settings page.

In the Report Limitation Category, select the limitation, and save your changes.

Generate reports 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

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.
   - 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 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.

   ```markdown
   [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.

   ```markdown
   [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 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

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>
</tbody>
</table>
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.
Manage the Orion Web Console

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.

Manage Orion Polling Engines

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

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.
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.
## 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.

View a polling engine status

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.

Update polling settings

Click Settings > All Settings, and in the Thresholds & Polling group, click Polling Settings to configure your polling engine.

Configure polling interval settings

You can improve your Orion server performance by entering longer polling intervals.

Configure how frequently the polling engine requests information from devices.

Default Node Poll Interval

The interval for polling the status and response time of monitored devices. By default, this interval is 120 seconds.

Default Volume Poll Interval

The interval for polling the status and response time of volumes. By default, this interval is 120 seconds.
Default Rediscovery Interval

The interval for polling the entire network to detect any re-indexed interfaces. Monitored network devices are also checked for IOS upgrades for EnergyWise support. By default, this interval is 30 minutes.

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.

1. 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.

Lock Custom Values

Select this option to store the configured custom ICMP polling interval settings.

Re-Apply Polling Intervals

Apply the settings specified in this section to all objects in the database by clicking Re-Apply Polling Intervals. Click Submit to use the current settings for new objects.

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. For objects added to the database in the future, the saved 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

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

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

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 reduce retention periods or otherwise change the default settings, 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.
Archive Time

Configure the time of day when the maintenance of the SolarWinds Orion database runs.

Auditing Trails Retention

Specify the number of days until the audit trails statistics are deleted from the database.

Detailed Statistics Retention

Specify the time period in which all statistics collected in the SolarWinds Orion database are summarized into hourly statistics. By default, this period is seven days.

Hourly Statistics Retention

Specify the time period in which all statistics collected in the SolarWinds Orion database are summarized into daily statistics. By default, this period is 30 days.

Daily Statistics Retention

Specify how long daily statistics are kept in the SolarWinds Orion database. After the specified time, the daily statistics are deleted. By default, this period is 365 days.

Container Detailed Statistics Retention

Specify when group statistics are summarized into hourly statistics. The default is seven days.

Container Hourly Statistics Retention

Specify when hourly group statistics are summarized into daily statistics. The default is 30 days.

Container Daily Statistics Retention

Specify how long group statistics are kept in the SolarWinds Orion database. The default is 365 days.

Baseline Data Collection Duration

Specify the number of days that are included into the baseline.

Detailed Wireless Statistics Retention

Specify the number of days until the detailed wireless statistics in the SolarWinds Orion database are summarized into hourly statistics. By default, this period is three days.

Hourly Wireless Statistics Retention

Specify the number of days until the hourly wireless statistics are summarized into daily statistics. By default, this period is 14 days.

Daily Wireless Statistics Retention

Specify the number of days until the daily wireless statistics are deleted from the database. By default, this period is 180 days.
Events Retention

Specify the number of days until the all network events data are deleted from the SolarWinds Orion database. By default, this period is 30 days.

Syslog Messages Retention

Specify the number of days until all data related to received Syslog messages are deleted from the SolarWinds Orion database. By default, this period is seven days.

Trap Messages Retention

Specify the number of days until all data related to received trap messages are deleted from the SolarWinds Orion database. By default, this period is 30 days.

Max Alert Execution Time

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.

Alert Acknowledge URL Text

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.

Allow alert actions for unmanaged objects

Select this option if you want the SolarWinds Alerting Engine to execute configured alert actions for unmanaged objects.

⚠️ Enabling this option increases the processing load on both the SolarWinds server and the database server.

Discovery Retention

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. By default, this period is 60 days.

Downtime History Retention

Specify the number of days until the downtime history is deleted from the database. By default, this period is seven days.

Configure network settings

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 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

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.

Calculate node availability

Determine the availability under Orion Polling Settings > Calculations & Thresholds > Availability Calculation by using one of the following methods.

Tip 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.

The Percent Packet Loss method introduces a historical dependency into each availability node record. It is best practice to leave calculations based on Node Status unless you specifically need node availability based on packet loss.

Define baselines for nodes

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.
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.

Assign credentials to virtual servers

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 general thresholds

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.

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.

Set how many retries are necessary before packet loss is reported

Configure the Response Time Retry Count for your polling engine to manage the amount of network-wide packet loss reported by Orion Platform products. This setting specifies the number of times Orion retries ICMP pings on a monitored device before packet loss is reported.
This configuration change requires an insertion into your SolarWinds Orion database. SolarWinds recommends installing and using the SQL Server Management Studio to perform this insertion.

To configure the Response Time Retry Count for your polling engine:

1. Create a full backup of the SolarWinds Orion database.
2. To start the Orion Service Manager, click SolarWinds Orion > Advanced Features program folder.
3. Click Shutdown Everything.
4. On your SolarWinds Orion database server, execute the following query on the SolarWinds Orion database.

   ```sql
   INSERT INTO [OrionDatabaseName].[dbo].[Settings] (SettingID, Name, Description, Units, Minimum, Maximum, CurrentValue, DefaultValue) VALUES ('SWNetPerfMon-Settings-Response Time Retry Count', 'Response Time Retry Count', 'Number of times Orion retries ICMP pings on a monitored device before reporting packet loss', '', 1, Maximum, CurrentValue, DefaultValue)
   ```

5. To start the Orion Service Manager, click SolarWinds Orion > Advanced Features program folder.
6. Click Start Everything.

Set the node warning level

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.

- Some of the events or alerts for down nodes you are receiving can inform you about nodes that are not actually down. Their status can be caused by intermittent packet loss on the network.

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.

   ```
   The default Node Warning Level interval is 120 seconds.
   ```

5. Click Submit.
Delete polling engines

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.

Thresholds

Many Orion Web Console resources can display error and warning 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). Dynamic baseline thresholds are the most accurate way to define thresholds for a specific device.
Baselines are calculated once, after data has been collected for a week. You can recalculate baselines on demand.

**Set general thresholds**

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.

![](percent_packet_loss.png)

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.

**Customize thresholds for single objects**

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.

> If you want to use dynamic thresholds, click Use Dynamic Baseline Thresholds. The integer values will be replaced with macros for dynamic thresholds ($\{USE_BASELINE_WARNING\}, $\{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.

General threshold types

**Avg CPU Load**

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

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

You can choose to calculate exhaustion using average daily values or peak daily values.

**Disk Usage**

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

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

You can choose to calculate exhaustion using average daily values or peak daily values.

**Percent Memory Used**

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

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

You can choose to calculate exhaustion using average daily values or peak daily values.

**Percent Packet Loss**

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

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

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

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

Orion 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.

Baselines and baseline calculations

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.

**Manage Orion Web Console user accounts**

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 users accounts if they only need to review reports or access views. See [Share 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.

**Create users**

Before you begin, consider what tasks the user must perform, and what views and menu bars are most suitable.
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.

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. Provide the account credentials, and click Next.
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

When you log in to the Orion Web Console for the first time, SolarWinds recommends that you change the password for the Admin account.

Only users with administrator rights can change the password.

1. Log in to the Orion Web Console, and click Settings > All Settings.
2. Click Manage Accounts in the User Accounts grouping.
3. Select a user, and click Change Password.

4. Enter and confirm the new password, and click Change Password.

Enable 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.

Define what users can access and do

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</td>
<td>Select Yes for the Disable Session Timeout option. Session timeouts are</td>
</tr>
<tr>
<td>is closed?</td>
<td>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 (Select Yes for this option or do as instructed)</th>
</tr>
</thead>
</table>
| Add and edit user accounts and reset passwords.                      | Allow Administrator Rights  
Granting administrator rights does not assign the Admin menu bar to a user. |
|                                                                      | **SolarWinds recommends that you do not allow users to change their own Orion Web Console account passwords.**            |
| Add, edit, and delete nodes.                                         | Allow Node Management Rights                                                                                           |
| Create, edit, and delete maps in the Network Atlas.                  | Allow Map Management Rights                                                                                           |
| Add, edit, schedule, and delete reports.                            | Allow Report Management Rights  
To only allow access to some reports, select the report category the user can access. |
| 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 elements.                                 | Allow Account to Unmanage Objects                                                                                       |
| 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.

Set default menu bars and views for users

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.

5. Select Yes for the items the user will 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.

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

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.

Restrict user access to network areas by applying limitations

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

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

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

- 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.
   1. Click Add Limitation in the Account Limitations section.
   2. Select the type of limitation to apply, and click Continue.
   3. Define the limitation, and click Submit.
      The limitation will be added to the Edit Account page.
5. Click Submit.

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

Patterns for limitations

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

Patterns are not case sensitive.

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

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

Create limitations based on custom properties

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

Before you start, plan how you want to limit the user access, and create custom properties.

This procedure requires access to the computer that hosts the Orion server.

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

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

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

6. Click OK.

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

### Delete account limitations

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.

ℹ️ 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.

ℹ️ 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.

### Configure automatic login

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](#).

ℹ️ Windows authentication must be enabled in the Configuration Wizard and the Web Console Settings. See [Enable Windows Authentication with Active Directory](#).

**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 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 views with non-Orion Web Console users.

Pass-through user credentials in a URL

See Automatically login by passing your credentials through the URL.

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

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 (NTFS) 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. Enable the Orion Web Console to use automatic Windows Authentication.
   1. Start the Configuration Wizard in the SolarWinds Orion > Configuration and Auto-Discovery program folder.
   2. Select Website, and click Next.
   3. Provide the appropriate IP Address, Port, and Website Root Directory, and select Yes - Enable Automatic Login Using Windows Authentication.
   4. Click Next, and complete the Configuration Wizard.
2. Log in to the Orion Web Console using the appropriate domain and user, providing Domain\Username or Username@Domain as the User Name.
3. Run the Configuration Wizard and enable Windows authentication.
4. 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

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></td>
<td>LogonFallback must be enabled.</td>
<td></td>
</tr>
</tbody>
</table>
**SCENARIO** | **WEB CONSOLE LOGIN SUPPORTED?** | **LOCAL LOGIN REQUIRED?** | **NETWORK ATLAS AND UNMANAGE UTILITY LOGIN SUPPORTED?**
---|---|---|---
Login with trusted domain AD user |  |  | No
Login with trusted domain AD Group User |  |  |  
Login with "Orion Server" domain Group AD account (group user belongs to trusted domain)\(^1\) | No | N/A | 
Login with trusted domain Group AD account (group user belongs to "Orion Server" domain)\(^2\) | No |  | 
Login with AD user or Group user from a foreign AD forest | Yes, when LDAP is enabled  
No, without an Additional Website\(^3\) |  |  

**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 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 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.
8. Click Submit.

Users can now look at views without an account on the Orion Web Console.

Automatically login 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.

**Administrative functions of the Orion Web Console**

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

**View secure data**

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).

ℹ️ This setting does not affect the display of custom reports that you export to the web.

**Handle counter rollovers**

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**

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](https://thwack.com)
- Access the product blog
- Check for maintenance updates

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.

Orion Web Console and chart settings

The Web Console Settings page allows an Orion Web Console administrator to 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.

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.

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

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

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

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.

Show Data Points on Lines

The actual data points that are used to create a chart may be shown by checking Show Data Points on Lines.

Font Size

Font Size sets the default relative size, Small, Medium, or Large, of the text that is displayed within charts in the Orion Web Console. This setting is independent of your browser settings. The font settings in your browser will affect resource headers and some resource contents.
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.

Web Console settings

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

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

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

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

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.

Show Data Points on Lines

The actual data points that are used to create a chart may be shown by checking Show Data Points on Lines.

Font Size

Font Size sets the default relative size, Small, Medium, or Large, of the text that is displayed within charts in the Orion Web Console. This setting is independent of your browser settings. The font settings in your browser will affect resource headers and some resource contents.
Discovery, Worldwide Map, and Active Alerts 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.

**Automatic Geolocation**

Select the box to place nodes automatically on worldwide maps.

**Active Alerts Refresh**

Specify how often the active alerts grid page is refreshed.

Active Alerts settings

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

**Custom properties**

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 properties must use the Latin1 character set.

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.
When you create, edit or remove a custom property, an event is logged. These events are audited, and you can display them in Audit Events resources.

Create a custom property

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.

1. 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.

2. 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.

3. 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.
4. If you want to limit how the custom property for nodes should be used, clear boxes in the Usage section.

![Warning]

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 [for 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.

   ![Tip]

   To add a value for properties with restricted values, select Add New Value from the drop-down 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.

You can now use the custom property for sorting objects of the type in Group By lists.

Remove a custom property

⚠️ 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**

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.

- Your data must be formatted as a table, and at least one column title should match an existing object property such as IP Address.

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. Browse to the custom property data file, and click Open.
6. Select the object type you want in the Import Values For drop-down, and click Next.
7. For each detected Spreadsheet Column in your data, select the corresponding Orion Database 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.
8. 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

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.

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

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.

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.
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

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.
Customize the Orion Web Console look, views, settings, charts, and maps

You need the Allow Administrator Rights privilege.

My Dashboards

My Dashboards provide menu bars with 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 views and labels offered in default menus for individual users.
If you do not need to see 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.

   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.

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.

```
<table>
<thead>
<tr>
<th>DEFAULT MENU BAR AND VIEWS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the menu bar for this account. To view the contents of each</td>
</tr>
<tr>
<td>HomeTab Menu Bar: New York</td>
</tr>
<tr>
<td>NetworkTab Menu Bar: Network.TabMenu</td>
</tr>
</tbody>
</table>
```

5. Select Yes for the items the user will see in the Alerts & Activity menu bar.

```
<table>
<thead>
<tr>
<th>Show Alerts Menu</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Events Menu</td>
<td>Yes</td>
</tr>
<tr>
<td>Show Syslog Menu</td>
<td>Yes</td>
</tr>
<tr>
<td>Show Traps Menu</td>
<td>Yes</td>
</tr>
<tr>
<td>Show Message Center Menu</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

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.

```
<table>
<thead>
<tr>
<th>Tabs ordering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home</td>
</tr>
<tr>
<td>Network</td>
</tr>
<tr>
<td>Applications</td>
</tr>
<tr>
<td>Storage</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Home Page View</th>
</tr>
</thead>
<tbody>
<tr>
<td>New York IT Summary</td>
</tr>
</tbody>
</table>
```

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.

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

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

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\.
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.

6. Click Submit.

Use Orion Web Console breadcrumbs

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.

Customize resources in the Orion Web Console

The following sections explain how to customize resources (also called "widgets") in the Orion Web Console. Available options depend on the resource type and may include:
Filter nodes in resources using SQL queries

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

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 resource.
2. Provide an appropriate SQL query in the Filter Nodes (SQL) field, and click Submit.

SQL query examples

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.

The following are valid status levels:

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

Specify what a Custom Object resource displays

Custom Object resources can display performance data for any monitored objects.

You can graph data for multiple objects on the same chart, such as memory usage on all storage devices. The resource can include a sum of all the series.
1. Click Edit in the resource.
2. Edit the resource Title and Subtitle.
3. Select an object type in Choose Object Type.
4. Select objects to be displayed in the resource:
   a. Click Select Object.
   b. In the Group By field, select a grouping criterion.
   
```
   Defined custom properties are listed for all grouping types.
   ```
   c. Select objects (either a group, or expand a group and select individual child objects), and click the arrow to move the objects into the pane on the right.
   d. Click Submit.
   The selected objects will appear on the Edit Custom Object Resource page, together with appropriate options.
5. Select a Chart to include in your custom object resource.
6. If you want to automatically display nodes related to the current view, select the option in Select Object.
7. To limit the number of data series in the resource, select Limit Series, and select the number of series to allow.
8. Select whether or not you want to Show Sum in Data Series.
9. Select the Time Period and Sample Interval.
10. To automatically hide the resource when there is no data for it to report, select Yes for the Auto-Hide Resource option.
11. Click Submit.

**Widget configuration examples**

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

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.
   - Https 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.

**Customize views**

Create, delete, modify, or restrict views

Orion Web Console views are configurable presentations of network information that can include maps, charts, summary lists, reports, events, and links to other resources. Edit views directly or through the Manage Views page.

Customized views can be assigned to menu bars. With NOC View Mode enabled, views may be optimized for display in Network Operations Centers.

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

Create new views

You can customize the Orion Web Console for individual users by creating views.

You need Administrator Rights to create views.

Plan what should be on a view before you create it.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify objects to see on the view.</td>
<td>Select the appropriate object type, such as nodes, interfaces, groups, applications, and so on.</td>
</tr>
<tr>
<td>View information for all objects of the selected object type.</td>
<td>Select a Summary view.</td>
</tr>
<tr>
<td>OPTION</td>
<td>ACTION</td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>View details for a selected object.</td>
<td>Select a Details view.</td>
</tr>
<tr>
<td>Select information about the objects you want to see.</td>
<td>Select resources.</td>
</tr>
<tr>
<td>Divide the information into several tabs.</td>
<td>Enable Left Navigation.</td>
</tr>
<tr>
<td>Optimize the view for large screens or mobile devices.</td>
<td>Create a Network Operations Center (NOC) view.</td>
</tr>
<tr>
<td>Limit what devices should be displayed on the view.</td>
<td>Add a limitation.</td>
</tr>
<tr>
<td>Access the view from the Menu Bar.</td>
<td>Add the view into the menu bar.</td>
</tr>
</tbody>
</table>

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.

   ![Add New View](image)

4. Click Submit.

You have now created an empty view. The Customize view page opens automatically. Add resources that contain the information you want to see or immediately add the view to a dashboard.

After you have created a new view, you can customize which widgets are on the page.

Add resources and columns to views, and define subviews

Administrators can edit views directly on the page by clicking the pencil icon or through the Customize Views page.

1. Click Settings > All Settings in the menu bar.
2. In the Views grouping, click Manage Views.
3. Select the view, and click Edit.
Add widgets to the view from the Customize Page

Widgets are a new way to refer to resources in your SolarWinds installation.

1. Go to the view you created.
2. Click the pencil icon on the upper left.

3. Click the Add Widgets button in the upper right.
4. Search for widgets, or resources, and drag and drop widgets directly on the page where you want them to be, including in new columns.
   - You can limit offered resources by criteria in the Group by list, or search for a resource or widget in the Search box.

5. When complete, click Done adding widgets, and then Done editing.

The view is populated with the widgets you selected.

Add resources to the view from the Customize Views page

1. On the Customize page, click + next to the column that you want to add the resources, also known as widgets.

   To open the Customize view page, click Settings > All Settings > Manage Views. Select the view, and click Edit.
2. Select resources in the middle pane, and click Add Selected Resources.

   You can limit offered resources by criteria in the Group by list, or search for a resource, or widget, in the Search box.

3. Use the arrow icons next to the columns to move resources between columns.

4. Click Done.

The view is now populated with the widgets you selected.

   Resources already in your view are not marked in the list. You can add a resource on a view more than once.
Some resources may require additional configuration.
Several options on the Add Resources page are added to the list of resources for a page, but the actual configuration of a given map, link, or code is not added until the page is previewed.

Divide content into subviews from the Customize Page

1. Hover over the side menu and click Add tab.
2. Type a name for the new tab, and click Update.
3. Select an icon.
4. Click Done.
5. Add resources by opening the Customize Page.

Divide content into subviews from the Customize Views page

1. On the view, click the Customize Page icon.
2. Click Add tab.
3. Enter the tab name, and click Update.
4. Select an icon, add resources, and click Done.

To drag and drop widgets, click Preview, and then add the widgets.

You can access the subview with the resources from the view menu.
Add subviews using Enable Navigation

1. On the Customize view, select Enable Left Navigation.

To open the Customize view page, click Settings > All Settings > Manage Views. Select the view, and click Edit. You can also click Customize Page > Page Settings on the view.

2. Click Add Tab.

3. Type a name for the new tab, and click Update.

4. Select an icon, and add resources.

5. Click Done.

You can access the subview with the resources from the view menu.

When you are done with your changes, click Preview, and then click Submit.

Create custom summary views

The Custom Summary view enables you to create a fully customized object-based view.

You need the Allow Account to Customize Views right enabled.

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.

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.

The fields displayed and information required depend upon the object type selected.
Enable NOC View Mode

Network Operations Center (NOC) View Mode enables you to customize web console views for optimal display on large network operations center screens. With NOC View enabled, a web console view cycle through its network monitoring resources for continually updated, shared viewing.

1. Click Customize Page in the top right of the view for which you want to enable NOC View Mode.
2. Select Enable NOC view mode.
3. Click Done & Go To NOC to display the view in the NOC mode.

Optimize 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 resources.

Enable NOC Views

You can configure any Orion Web Console view to appear in the NOC view form.
1. Log in to the Orion Web Console as an administrator.
2. Open a view, and click Customize Page in the top right 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. You have created a NOC version of your view with a compressed header and footer, and without the left navigation area.

Customize NOC Views

To add resources, remove resources, or add subviews on a NOC view, click the top-right icon, and select Customize Page.

Exit NOC Views

Click the NOC Settings icon, and select Exit NOC Mode.

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

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.

Display subviews

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

To display a subview, click the circle.

Move resources in NOC Views

If you want to move resources within a NOC view, you turn on the drag&drop mode.
1. Click the Settings icon in the top right corner of the NOC view, and select Pause Rotation.
2. Drag and drop resources within the selected pane.
3. When you have finished repositioning the resources, click the Settings icon again, and select Resume Rotation.

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

As a security feature, administrators can limit which devices are displayed on a view.

You can open the Customize View page from the view by clicking the pencil icon on the left, and then Page Settings.

1. Click Settings > All Settings in the menu bar, and click Manage Views in the Views grouping.
2. Select a view, and click Edit.
3. On the Customize View page, click Edit in the View Limitation area.
4. Select the type of view limitation you want to apply, and click Continue.
5. 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

When you want to create multiple views, create one view, and use it as a template to create other new views.

If you copy a view with a view limitation applied, that view limitation is carried over to the copied view and any change you make applies to both views. You can delete the view limitation to remove it from all views, and then create a view limitation for each view.

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

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 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

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

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. (Note: HTTPS 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

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.
   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.
Maintain the SolarWinds Orion database

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.

**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

**Database maintenance**

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>Detailed Statistics Retention</th>
<th>7 days</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hourly Statistics Retention</td>
<td>30 days</td>
</tr>
<tr>
<td>Daily Statistics Retention</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.

Back up and restore the database

Use the SQL Server Management Studio to create and restore backups on your servers. The application should be installed with the Microsoft SQL Server. You typically will manage backups when performing SolarWinds product upgrades, migrating to a new server, or as part of a maintenance schedule.
See the Microsoft Support page for information about creating backups with your version of the MS SQL Studio.

After performing a restore, you will need to update the database location through the console.

- While restoring the database, use the Restore with Recovery option.
  
  For more information, search for "restore a database backup" on the Microsoft TechNet web portal at https://technet.microsoft.com, and consult the help for the appropriate SQL Server Management Studio version.

### 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.

- If you need to backup or restore a database, you should use the SQL Server Management Studio. For details, see Creating a Database Backup.

### Add a server to Database Manager

If you have not already designated a backup or supplementary database for use with your Orion Platform product, add a SQL server.

1. Start the Database Manager in the SolarWinds Orion > Advanced Features program folder.
2. To add a default server, click Add Default Server.
3. To select a server:
   a. Click Add Server.
   b. Select or enter the SQL Server instance you want to use in the server/instance format.
   c. Select the appropriate authentication method, enter your credentials, and click Connect.

You can now see the server and associated databases in the tree structure of the Database Manager.

### View database details

The Database Manager provides details per database to review current information. If the SQL server hosting your database is not listed, you should add the database.

1. Start the Database Manager in the SolarWinds Orion > Advanced Features program folder.
2. If the SQL Server hosting your SolarWinds Orion database is not listed in the left pane, add the SQL Server hosting your Orion database.
3. Click + in the left pane to expand the SQL Server hosting your SolarWinds Orion database, and right-click the database.

   The default database name is **SolarWindsOrion**.

4. Click Database Details.
   - The Properties tab shows general statistics and descriptions of the selected database.
   - The Tables tab lists the tables and their respective sizes.
   - If you have not yet made a backup of the database, the Last Backup field on the Properties tab is blank.

**View table details**

You can view the Table details for a selected database including the property, column, and index information through the Database Manager. You can also query the selected table directly from the Table Details window for specific or additional data.

1. Start the Database Manager in the SolarWinds Orion > Advanced Features program folder.
2. If the SQL Server hosting your SolarWinds Orion database is not listed in the left pane, [add the SQL Server](#) hosting the database.
3. Expand the SQL Server hosting your SolarWinds Orion database in the left pane, and expand the SolarWinds Orion database.

   The default database name is **SolarWinds Orion**.

4. From the tables displayed for the database, right-click any table to view the Table Details.
   - The Properties tab includes general statistics relating to the selected table size and creation date.
   - The Columns tab lists keys, column names, size and data types in the selected table.
   - The Indexes tab shows indexes used in the table.
5. To execute a query:
   a. Right-click the table name, and click Query Table.
   b. Adjust the default SQL query or create a new one, and click Execute.
      - The default SQL query lists the contents of the table.
6. To export a table, right-click the table name, and click Export to CSV. You will be asked to enter a name for the comma separated value file created.

**Update Orion Platform products to use the new database**

After you have restored your SolarWinds Orion database backup file on the new server, you must update the database location for the Orion server to access the restored database on the new database server.
SolarWinds recommends that you use SQL Server Authentication with the sa login and password to ensure that Orion can always access the SolarWinds Orion database, even if it is hosted remotely on a separate server.

1. Log in to your Orion server.
2. Start the Configuration Wizard in the SolarWinds Orion > Configuration and Auto-Discovery program folder.
3. Select Database, and click Next.
4. Specify your new database server in the SQL Server field.
5. To use SQL authentication, select Use SQL Server Authentication, provide the credentials, and click Next.
6. Select Use an Existing Database, select or type the existing database name, and click Next.
7. If you are prompted to use the existing database, click Yes.
8. Select Create a New Account, and provide a New Account name.

- Creating a new account ensures that Orion has required access to your migrated database.
- The New Account must be a member of the securityadmin server role.
- The sysadmin role and the sa user account are always members of securityadmin.

9. Provide and confirm an account Password, and click Next.
10. Click Finish to exit the Configuration Wizard.
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.

**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><strong>Single Subnet</strong></th>
<th><strong>Multiple Subnets</strong></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.

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.

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.
## 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.

Visit [SolarWinds KB MT6886](https://kb.solarwinds.com/) to build an upgrade path.

### 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>IP Address Manager 4.3.2 and later</td>
<td>IP Address Manager 4.5 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>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
- Firewall Security Manager 6.6.8
- 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

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.

<table>
<thead>
<tr>
<th>HARDWARE/SOFTWARE</th>
<th>REQUIREMENTS FOR BOTH SERVERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016</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.
## Hardware/Software Requirements for Both Servers

- The primary and secondary server can be joined to a Windows domain.

### 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>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

- SolarWinds High Availability does not support IPv6 addresses.
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.

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.

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.

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.

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.

![High Availability Deployment Summary](image)

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.

```
High Availability
- Backup Server for Main Server Protection
- Backup Server for Additional Polling Engine(s) Protection
```

   - 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.

> 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

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**
     1. Enter the IP address of the DNS server that manages the pool members' DNS Zone.
     2. Enter the DNS Zone.
     3. 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**
     1. Enter the IP address of the DNS server that manages the pool members' DNS Zone.
     2. Enter the DNS Zone.
     3. 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.
        SolarWinds cannot validate the DNS server IP address or DNS zone for this selection.
     1. Enter the IP address of the DNS server that manages the pool members' DNS Zone.
     2. 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.

Choose the server you want to be active

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**

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.

**Disable or delete HA pools, force a failover, or update an HA pool**

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.
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.

Which IP address is used as the source?

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.

Choose an IP address close to the default gateway's IP address so outbound communication comes from the VIP address. You can also modify the converted bits to be the IP address with the longest match and convert it back to an IP address.

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>
</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.

### 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.

- **TSIG shared secret key name**: The name you gave the key in the configuration file.
- **TSIG shared key value**: 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 <keysize> -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
   ```
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. Reconfigure 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. Reconfigure BIND using the following command:
   \texttt{rndc reconfig}

## 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.

\begin{itemize}
\item SolarWinds does not support other DNS server options. However, we have provided an out-of-the-box alert, \textit{Update High Availability Active Member DNS Record on AWS Route53 When Failover Occurs}, that you can use as an example.
\end{itemize}

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.
   \begin{itemize}
   \item We recommend duplicating \textit{Update High Availability Active Member DNS Record on AWS Route53 When Failover Occurs} as a base.
   \end{itemize}

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.

\begin{itemize}
\item Reset the alert automatically after a period of time, such as one to five minutes.
\item Add an Execute an External Program or External VB Script alert action.
\item Create a DNS host entry update script. You can use following values in your alert actions to pass as parameters to your script.
   \begin{itemize}
   \item Active member primary IP address = \texttt{$\{N=SwisEntity;M=PrimaryIpAddress\}$}
   \item DNS server IP Address = \texttt{$\{N=SwisEntity;M=Pool.DnsIpAddress\}$}
   \item DNS Zone = \texttt{$\{N=SwisEntity;M=Pool.DnsZone\}$}
   \item Virtual HostName = \texttt{$\{N=SwisEntity;M=Pool.VirtualHostName\}$}
   \end{itemize}
\item Do not add a reset action.
\end{itemize}

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.